Vol 25, No. 2
Fall 2016

The Journal of the Antitrust, UCL and Privacy Section of the State Bar of California

The Journal of the
Antitrust, UCL and Privacy Section
of the State Bar of California

Chair's Column
Paul Riehle

Editor's Column
Heather S. Tewksbury

Recent Developments in Antitrust, Competition, and Privacy Law

Vol. 25, No. 2 Fall 2016

Recent Developments in Antitrust, Competition, and Privacy Law

Editor-in-Chief

HEATHER S. TEWKSBURY
Partner
Wilmer Cutler Pickering Hale and Dorr LLP
Palo Alto, CA

Deputy Vice Chair

PETER K. HUSTON
Sidley & Austin LLP
San Francisco, CA

AARON SHEANIN
Of Counsel
Pearson Simon and Warshaw, LLP
San Francisco, CA

Article Editors

EVAN DAVIS

LAURA GOODALL
Wilmer Cutler Pickering Hale and Dorr LLP
Palo Alto, CA

NICOLE CALLAN
LAUREN IGE
CHRIS MEGAW
Wilmer Cutler Pickering Hale and Dorr LLP
Washington, DC

competition

The Journal of the Antitrust, UCL and Privacy Section of the State Bar of California

ANTITRUST, UCL AND PRIVACY SECTION EXECUTIVE COMMITTEE 2016-2017

OFFICERS

Niall E. Lynch, **Chair**, San Francisco
Lee F. Berger, **Vice Chair**, Washington DC
Jill M. Manning, **Vice Chair**, San Francisco
Robert E. Freitas, **Vice Chair**, Publications, Redwood City
Heather S. Tewksbury, **Vice Chair**, Publications (Competition), Palo Alto
Eric P. Enson, **Vice Chair**, Programs, Los Angeles
Steven N. Williams, **Vice Chair**, Programs, Burlingame
Anna Fabish, **Deputy Vice Chair**, Treatise, Los Angeles
Qianwei Fu, **Deputy Vice Chair**, Treatise, San Francisco
Courtney A. Palko, **Deputy Vice Chair**, Treatise, Los Angeles
E. Kate Patchen, **Deputy Vice Chair**, Programs, San Francisco
Elizabeth C. Pritzker, **Deputy Vice Chair**, Oakland
Dominique-Chantale Alepin, **Secretary**, Palo Alto
Peter K. Huston, **Treasurer**/Competition, San Francisco
Paul J. Riehle, **Immediate Past Chair**, San Francisco
Rafey Balabanian, **Public Member**, San Francisco

MEMBERS

Jason M. Bussey, Palo Alto
Abiel Garcia, Los Angeles

ADVISORS

Aton Arbisser, Los Angeles
Asim M. Bhansali, San Francisco
Maxwell M. Blecher, Los Angeles
Albert J. Boro, Jr., San Francisco
Terrence A. Callan, San Francisco
Craig C. Corbitt, San Francisco
John F. Cove, Jr., Oakland
Thomas N. Dahdouh, San Francisco
Kathleen E. Foote, San Francisco
Elaine F. Foreman, San Francisco
J. Thomas Greene, San Francisco
Paul R. Griffin, San Francisco
Don T. Hibner, Jr., Los Angeles
Thomas S. Hixson, San Francisco
Geoffrey T. Holtz, San Francisco
Holly A. House, San Francisco
Cheryl L. Johnson, Los Angeles
David Kesselman, Los Angeles
Kim A. Kralowec, San Francisco
Susan Kupfer, San Francisco
John M. Landry, Los Angeles
Jesse W. Markham, San Francisco
Sarretta C. McDonough, Los Angeles
Daniel J. Mogin, San Diego
Kenneth R. O'Rourke, Los Angeles
Thomas A. Papageorge, Laguna Niguel
Roxane A. Polidora, San Francisco
Robert B. Pringle, San Francisco
J. Thomas Rosch, Washington DC
Lisa M. Saveri, San Francisco
Francis O. Scarpulla, San Francisco
Aaron M. Sheanin, San Francisco
Karen Silverman, San Francisco
Bruce L. Simon, San Francisco
Gary R. Spratling, San Francisco
William L. Stern, San Francisco
Anita F. Stork, San Francisco
Bonny E. Sweeney, San Francisco
Kevin Y. Teruya, Los Angeles
Kathleen J. Tuttle, Los Angeles
Howard M. Ullman, San Francisco
Craig A. Waldman, San Francisco

Mitch Wood, Section Coordinator
Ana Castillo, Administrative Support

CHAIR'S COLUMN

Paul Riehle
Sedgwick LLP
San Francisco, CA

With many thanks to all who contributed, particularly the authors and editors, the Antitrust, Unfair Competition Law and Privacy Section is pleased to provide you with another edition of *Competition*. Special thanks to **Heather Tewksbury** our Editor-in-Chief, who provides an overview of this edition in her Editor's Column.

This issue is being distributed contemporaneous with our flagship program, the **Golden State Institute**, being held November 3, 2016. For the fifth year in a row, we will have presentations on "Big Stakes" Antitrust Trials, this year with counsel from *United States vs. AB Electrolux & General Electric Co.*, a successful merger challenge filed by the United States Department of Justice, Antitrust Division, and *In re Cox Enterprises, Inc. Set-Top Cable Television Box Antitrust Litigation*, a Section 1 claim of illegal tying by forcing consumers to rent a Cox set-top box in order to gain full access to Cox's premium cable service. For the fourth year in a row, the luncheon program will involve a sitting California Supreme Court Justice, this year **Associate Justice Carol Corrigan**. We are also pleased to present programs on assessing damages in privacy cases, a distinguished panel of federal judges—**Judge Denise Cote** from the Southern District of New York and **Northern District Judges Lucy Koh** and **James Donato**—and views from the **Department of Justice Antitrust Division**, featuring **Renata Hesse** (the acting head of the Antitrust Division), **Brent Snyder** (Deputy Assistant Attorney General for Criminal Enforcement) and our Section's own **Kate Patchen** (Chief of the DOJ's San Francisco Office). In the evening, we honor **Paul Griffin** of Winston & Strawn LLP as our **2016 Antitrust Lawyer of the Year**.

Please join us on November 30, 2016 at the Los Angeles County Library, for a **Privacy Law Symposium**, which will provide insider views on emerging trends in privacy law litigation and enforcement actions in California. The panel will be moderated by **Orange County Complex Litigation Judge Kim G. Dunning** and will feature **Tina Wolfson** on the plaintiffs' side, **Lori Chang** providing the defense perspective, economic consultant **Henry Fishkind**, **Lisa Kim**, Deputy Attorney General, California Department of Justice, Privacy Enforcement and Protection Unit, and **Tom Dahdough**, Federal Trade Commission Western Region Director and 2014-15 Section Chair. Thank you to **Jill Manning**, our Privacy Vice Chair, for organizing this event and many Section webinars over the last year.

The State Bar's Annual Meeting in October marked the end of my term as Chair of the Section. It has been an honor and a privilege to serve as Chair over the last year, and as a member of the Executive Committee since 2010. Notwithstanding a tumultuous year for the State Bar politically, our Section's membership increased substantially as a result of the excellent live educational programs, treatise, e-briefs and this journal. What I appreciate the most about my years on the Committee are the friendships formed with and the collegiality displayed by all sides of our profession: government enforcers, the plaintiffs' bar, and defense counsel. Thank you to everyone on the Committee for making this a successful year, and particular thanks to **Sarretta McDonough** and **Aaron Sheanin**, who are cycling off the Committee as members and who will continue to participate as advisors.

Congratulations to **Niall Lynch** as the Chair of our Section for 2016-17. Niall is a partner in the San Francisco office of Latham & Watkins LLP and previously spent 15 years as a prosecutor in the Antitrust Division of the DOJ. Niall has been a member of our Section's Executive Committee since 2011, most recently serving as Vice Chair responsible for the Golden State Institute.

Congratulations also to new members of the Executive Committee **Rafey Balabanian**, **Abiel Garcia** and **Jason Bussey**. With them, Niall, and the returning Vice Chairs, Deputy Vice Chairs and other Committee members, I am confident that our Section will continue to be favored with outstanding educational offerings and collegiality for many years in the future.

EDITOR'S COLUMN

Heather S. Tewksbury
Wilmer Cutler Pickering Hale & Dorr LLP
Palo Alto, CA

I want to thank all of the authors and editors who put a tremendous amount of work into this edition of *Competition*. I also want to give special thanks to **Paul Riehle**, who did a tremendous job leading our Section this past year! Please enjoy this edition of *Competition*!

Vol 25, No. 2 Fall 2016

The Journal of the Antitrust, UCL and Privacy Section of the State Bar of California

TABLE OF CONTENTS

THE RAPIDLY CHANGING LANDSCAPE OF PRIVATE GLOBAL ANTITRUST LITIGATION: INCREASINGLY SERIOUS IMPLICATIONS FOR U.S. PRACTITIONERS

By James L. McGinnis, Oliver Heinisch, and Nadezhda Nikonova[1]

I. INTRODUCTION

The center of gravity when it comes to private litigation of international antitrust disputes is still in the United States, but two trends affecting the legal landscape in the U.S., U.K., and EU are shifting it across the Atlantic. In this article, we address these trends and further discuss their implications for lawyers handling major antitrust disputes that have global footprints. Much of the discussion will focus on cartel litigation because those cases often involve global issues and present the most obvious examples for our discussion.

The first trend is the evolving jurisprudence of the Foreign Trade Antitrust Improvements Act ("FTAIA"). The FTAIA governs the scope of U.S. antitrust law over sales that implicate foreign comity concerns. While the FTAIA remains among the more baffling statutes to apply, circuit court decisions are multiplying and foreign jurisdictions are adding their own views in support of their own remedies. Complete clarity is likely to remain elusive, but there are categories of commerce involving foreign entities that are increasingly likely to be ruled out of bounds for U.S. courts with the result that foreign courts may be the only venues with jurisdiction over large amounts of sales.

The second key development is that, after many years of discussion, foreign remedies and procedures in the U.K. and other EU member states are finally being defined in ways that can be attractive for plaintiffs.[2] In 2013, the European Commission ("Commission") adopted non-binding recommendations on collective redress.[3] On November 26, 2014, the Commission also mandated additions to national laws ensuring uniform rules across the EU's 28 member states for private damage actions. These revisions must be implemented by December 27, 2016. National law modifications consequently are underway. There will be changes even in those jurisdictions that already have advanced systems and attract most private antitrust actions, such as the U.K., the Netherlands, and Germany.

Last year, the U.K. adopted rules in the Consumer Rights Act of 2015 that include for the first time an opt-out collective redress mechanism that is similar to a U.S.-style class action system. This law goes far beyond both the Commission's recommendations

---

1 Mr. McGinnis is a partner and Ms. Nikonova is an associate in the San Francisco office of Sheppard Mullin Richter & Hampton LLP. Mr. Heinisch is a partner in the London office of Sheppard Mullin. All practice in the firm's Antitrust and Competition Group.

2 The changes in Europe resulted from a protracted process of consultation. In 2005 the Commission adopted a Green Paper on antitrust damages actions and a White Paper in 2008 which dealt among other things with collective redress. A subsequent public consultation on the proposed European framework for collective redress highlighted the divergence of views among the stakeholders across Europe and the difficulty to reach consensus on a Directive.

3 Recommendation of 11 June 2013 on common principles for injunctive and compensatory collective redress mechanisms in the Member States concerning violations of rights granted under Union Law, 11.6.2013 COM(2013) 401 final.

and what was required under the Directive. No other European Union Member State has followed suit so far.

In short, until recently, private cases were focused on U.S. remedies with few companion cases across the Atlantic. This dynamic has dramatically changed over recent years as cartels investigated in both the U.S. and the EU now routinely trigger private damages actions on both sides of the Atlantic. Many practitioners now assume that international cartel matters will prompt significant private cases filed by large customers either in the U.K., Germany, or the Netherlands. In the future, more European national courts are likely to be involved, especially if Brexit further shifts the balance toward continental Europe. International cartels already have attracted private actions across Europe including: auto glass, DRAM, CRT, LCD, batteries, and air cargo. Representative cases have started to emerge—despite predictions to the contrary. If there are any early successes, those cases are likely to proliferate soon.

We will begin with a brief overview of how we got to where we are now, move to an analysis of the current situation in the U.K. and the EU, and conclude with a discussion of what all of this may mean for practitioners. Specifically, we focus on the exponentially increasing complexity of decisions concerning arbitration, discovery, settlement, and case coordination.

II. EVOLVING LIMITS ON THE SCOPE OF U.S. LAW AND EMERGING FOREIGN REMEDIES

A. Limits on the Scope of U.S. Law

Traditionally, global cases were litigated almost exclusively in the U.S. Plaintiffs were inclined to pursue all of their damage claims in U.S. courts based on the availability of treble damages and attorney's fees. And the American rule on attorney's fees made this a no risk proposition. Moreover, the FTAIA case law was much less developed.

Now, maturing FTAIA jurisprudence has begun to clarify what sales may or may not be addressed in U.S. courts. While parties will continue to disagree about the scope of the U.S. Sherman Act, most would acknowledge that there is a serious risk that a U.S. court will not adjudicate disputes involving foreign sales of components to foreign subsidiaries of U.S. companies. If finished products then are made by those overseas subsidiaries and sold abroad, almost certainly U.S. law will not reach those sales.

The FTAIA was signed into law in 1982, but has not been applied and litigated in earnest until the last fifteen years. The entirety of the surprisingly short statute reads as follows:

> Sections 1 to 7 of [the Sherman Act] shall not apply to conduct involving trade or commerce (other than import trade or import commerce) with foreign nations unless—
>
> 1. such conduct has a direct, substantial, and reasonably foreseeable effect—
>
> (A) on trade or commerce which is not trade or commerce with foreign nations, or on import trade or import commerce with foreign nations; or

(B) on export trade or export commerce with foreign nations, of a person engaged in such trade or commerce in the United States; and

2. such effect gives rise to a claim under the provisions of sections 1 to 7 of this title, other than this section.

If sections 1 to 7 of this title apply to such conduct only because of the operation of paragraph (1)(B), then sections 1 to 7 of this title shall apply to such conduct only for injury to export business in the United States.[4]

The FTAIA has two fundamental purposes. First, the statute codifies principles of international comity by limiting the reach of U.S. antitrust laws in order to avoid "interference with other nations' prerogative to safeguard their own citizens from anti-competitive activity within their own borders."[5] Second, the FTAIA promotes "certainty in assessing the applicability of American antitrust law to international business transactions and proposed transactions" by articulating a "single, objective test" for "determining whether American antitrust law is to be applied to a particular transaction."[6]

The FTAIA establishes a general rule that the Sherman Act does not apply to conduct involving foreign commerce.[7] The FTAIA then articulates two exceptions. First, under the "import commerce" exclusion, the statute provides that the Sherman Act does apply to conduct involving U.S. import commerce, which courts have defined to mean "transactions that are directly between [U.S.] plaintiff purchasers and [foreign] defendant cartel members."[8] Second, the "domestic effects" exception applies only where (1) the foreign conduct at issue had a "direct, substantial, and reasonably foreseeable effect" on U.S. commerce, and (2) that domestic effect "gives rise to" the claim.[9]

Courts have had a remarkably difficult time applying the FTAIA to business situations that have become common in an increasingly global economy. Although there is still little consensus regarding the exact boundaries of the FTAIA, recent circuit court decisions have given practitioners some clarity over which sales may be out of bounds for U.S. courts.

For example, the FTAIA excludes anticompetitive conduct by foreign companies that only causes a foreign injury. In its first major ruling on the issue, the Supreme Court recognized that the purpose of the FTAIA is to "exclude from the Sherman Act's reach much anticompetitive conduct that causes only foreign injury."[10] In *Empagran I*, a foreign purchaser brought claims in U.S. court for vitamins that were sold into foreign commerce. It was not disputed that the global Vitamins cartel had affected domestic

---

4 15 U.S.C. § 6a.

5 *Empagran S.A. v. F. Hoffmann-LaRoche, Ltd.*, 417 F.3d 1267, 1271 (D.C. Cir. 2005) ("*Empagran II*").

6 H.R. Rep. No. 97-686 at 2, 5, 8 (reprinted in 1982 U.S.C.C.A.N. 2487, 2488, 2490, 2493).

7 *Empagran S.A. v. F. Hoffmann-LaRoche, Ltd.*, 542 U.S. 155, 158 (2004) ("*Empagran I*"); *United States v. Hsiung,* 778 F.3d 738, 757 (9th Cir. 2015).

8 *Minn-Chem, Inc. v. Agrium Inc.,* 683 F.3d 845, 855 (7th Cir. 2012).

9 15 U.S.C. § 6a(1)-(2).

10 *Empagran I*, 542 U.S. at 158.

commerce, but defendants argued that the foreign plaintiff's purchases did not give rise to a Sherman Act claim in the same way that a domestic plaintiff satisfied the "domestic injury" exception. The Supreme Court held that U.S. antitrust laws do not apply where "price-fixing conduct significantly and adversely affects both customers outside the United States and customers within the United States, but the foreign effect is independent of any adverse domestic effect."[11] This case made clear that U.S. antitrust laws do not extend to *independent* foreign injuries, even if they were caused by an alleged global cartel that also caused domestic injuries.

The FTAIA also implicates foreign purchases made pursuant to a global purchasing agreement. In *Motorola Mobility, LLC v. AU Optronic Corp.*, three sets of purchases of TFT-LCD panels (the major component of LCD screens) were at issue.[12] The first set of purchases consisted of LCD panels that were sold directly to Motorola's U.S. parent. These purchases were "import commerce" subject to the Sherman Act, but they comprised only 1% of Motorola's claimed damages. The rest of the LCDs were purchased outside of the U.S. by Motorola's foreign subsidiaries and incorporated into cellphones that were either resold in the U.S. by the parent company ("Category 2" purchases) or sold abroad to foreign purchasers ("Category 3" purchases). The court ruled that Category 3 purchases—which were the majority of Motorola's claimed damages—"can't possibly support a Sherman Act claim" because "neither those cellphones nor their panel components entered the United States." The court also barred Motorola's Category 2 purchases because the added layer of a foreign subsidiary selling the cellphones back to Motorola for resale to U.S. consumers was too tenuous to "give rise" to Motorola's claim under the FTAIA. That the foreign purchases were subject to a master price agreement negotiated between Motorola and LCD manufacturers in the U.S. was not enough, on its own, to bring these purchases under the Sherman Act. Motorola's foreign subsidiaries were thus treated as the foreign purchaser in *Empagran*, rather than a single enterprise.

The law is still developing as to indirect sales of foreign sourced goods that are sold in the U.S. Take *United States v. Hsiung et al.*,[13] which arose from the same LCD cartel as *Motorola*, as an example. In *Hsiung*, AU Optronics sold LCDs to foreign OEMs which then sold "substantial volume of goods" to U.S. consumers. In this criminal case, the Ninth Circuit determined that AUO's conduct, which "targeted" the LCDs "for sale or delivery in the United States," constituted "import commerce" that fell under the purview of the Sherman Act. The Ninth Circuit held that although the guilty verdict could be sustained under the domestic effects exception, there was no need to apply that exception because the DOJ had proved U.S. import commerce. The Supreme Court refused to hear the *Hsiung* and *Motorola* appeals, even though some argued that the decisions were in conflict.

As the FTAIA jurisprudence was evolving, many foreign nations were simultaneously developing more robust antitrust regimes that did not exist when the statute was first enacted in 1982. The FTAIA, of course, was explicitly enacted to embrace principles of international comity by limiting the reach of U.S. antitrust laws. U.S. courts have

---

11 *Id.* at 164.

12 775 F.3d 816 (7th Cir. 2015).

13 778 F.3d 738 (9th Cir. 2015).

interpreted "interference" to apply to leniency programs, state enforcement actions, and private remedies.

Though not explicitly stated in the decisions, U.S. courts may be giving more deference to comity principles as they begin to understand the remedies that are available abroad. The Governments of Germany, the U.K. and Northern Ireland, Japan, Switzerland and the Netherlands submitted a joint brief as amicus curiae in the *Empagran* case arguing that "fundamental principles of international law and prescriptive comity limit U.S. court jurisdiction over foreign injuries" and that unrestricted U.S. jurisdiction "would shift private claims to U.S. courts and interfere with the policy choices made by other jurisdictions."[14] They explained that the differences in private damages remedies—or lack thereof—should be treated as deliberate policy choices that should be respected by the United States' commitment to international comity."[15] The Supreme Court recognized that "the comity concerns remain real as other nations have not in all areas adopted antitrust laws similar to this country's and, in any event, disagree dramatically about appropriate remedies."[16]

In the *Motorola* case, the Belgian Competition Authority and the Ministry of Economy, Trade and Industry of Japan ("METI") submitted amicus curiae briefs making even stronger comity arguments. The Belgian Competition Authority[17] specifically highlighted changes in Belgium's competition regime since *Empagran* was decided, including adopting a leniency program, new rules on collective redress, the establishment of a new procedure for early settlement of investigations, and its directive to "build consensus . . . across the global antitrust community" through participation in the International Competition Network ("ICN"). The Belgian Competition Authority urged the U.S. not to interfere with its competition regime.

METI[18] argued that allowing Motorola to pursue its Category 2 and 3 claims in the U.S. would have "international public policy implications which would adversely affect the ability of the government of Japan to regulate its own economy and govern its own society." One of METI's concerns was that "the applicability of treble damages, which are not common outside US, will be expanded through excessive extraterritorial application of US competition law, and that, as a result, Japan's ability to regulate its own commercial affairs will be interfered." METI added: in civil lawsuits based on injuries alleged to have been incurred as a result of foreign anticompetitive activities, plaintiffs often tend to insist on the remarkably enlarged scope of extraterritorial application." The Seventh Circuit seemed to agree:

---

14 Brief of the Federal Republic of Germany, United Kingdom of Great Britain and Northern Ireland, Japan, the Swiss Confederation, and the Kingdom of the Netherlands as Amici Curiae in Support of Defendants-Appellees, *Empagran, S.A. et al., v. F. Hoffman-La Roche Ltd.*, 2005 WL 3873712 (D.C. Cir. March 9, 2005).

15 *Id.*

16 *Empagran I*, 542 U.S. at 155.

17 Brief of the Belgian Competition Authority as Amicus Curiae in Support of Appellees, *Motorola Mobility v. AU Optronics,* 775 F.3d 816, Case No. 14-8003 Dkt. 113 (Oct. 16, 2014).

18 Brief of the Ministry of Economy, Trade and Industry of Japan as Amicus Curiae in Support of Appellees, *Motorola Mobility v. AU Optronics,* 775 F.3d 816, Case No. 14-8003 Dkt. 119 (Oct. 17, 2014).

> Of course Motorola wants damages for its subsidiaries, rather than just a cessation of the cartel activities that are hurting them. And foreign antitrust laws rarely authorize private damages actions. But . . . Motorola is asserting a right to forum shop; that if some foreign country in which one of its subsidiaries operates happened to provide a more generous private damages remedy than American antitrust law provides, Motorola would direct that subsidiary to seek that remedy in that country.[19]

No doubt the emerging case law will continue to refine the analysis of the FTAIA.

B. EU and U.K. Developments

At the same time that the scope of U.S. Sherman Act was being defined, U.K. and EU statutes began to make those jurisdictions more attractive for private cases both in terms of procedure and available damages.

1. Basic European Level Provisions

In 2001, the European Court made clear that any person can claim compensation for harm suffered where there is a causal relationship between that harm and an infringement of competition law.[20] While this landmark judgment definitely added momentum to private enforcement in the U.K. in particular, U.K. courts had established for many years that damages were available for harm caused by infringements of competition law. To some extent, that history explains the prominent position of the U.K. courts in private damages actions within Europe.

While it is now well established that anyone who suffered harm can claim compensation for actual loss, lost profit and interest, additional compensation in the form of punitive, multiple or penalty damages is not currently allowed. While the right to compensation stems from the *aquis communautaire*[21] the exercise of this right in the form of damages actions has remained subject to individual national laws of 28 EU members states. The diversity of those regimes was a contributing factor to the slow overall growth of private remedies in Europe.

European Regulation 1/2003/EC[22] was the first important legislative step toward facilitating private damages action across Europe. This regulation made European Commission decisions binding on national courts, consequently promoting cooperation with national courts and the Commission. Since then, national cases have shed more light on questions including standing, standard of proof, interim relief, pass-on and damages—still with a significant degree of diversity across the EU 28.

The European Commission's 2014 Directive was intended to promote private remedies by harmonizing the member states' substantive rights and procedures. While

---

19 *Motorola,* 775 F.3d at 826.

20 Case C-453/99 *Courage Ltd v Crehan* [2001] ECR I-6297, see also C-295/04 *Vincenzo Manfredi* [2006] ECR I-6619.

21 The accumulated body of European Union law.

22 Official Journal L 001, 04/01/2003 P. 0001—0025.

the Directive explicitly did not address collective actions, it mandated that member states ensure the right to claim and obtain full compensation for competition infringements. The Directive sets minimum requirements in several key areas that must be reflected in 28 national laws by the end of 2016:

Disclosure of Evidence[23]

Following a reasoned request based on evidence supporting the plausibility of a claim, national courts will be empowered to order proportionate disclosure of relevant evidence. Evidence will be available to the claimant, defendants, third parties or competition authorities. The resulting rules must ensure that disclosure is limited and proportionate, and can be challenged by the responding party. Both leniency statements and settlement submissions will be protected from disclosure. But it remains to be seen how this new procedure will be implemented and applied in practice. Most European jurisdictions do not have experience with disclosure, nor any precedents and inconsistent practices across the EU may be the result. The U.K.'s longstanding tradition of disclosure likely will offer more legal certainty in this area. The availability of discovery, while likely far less expansive than under U.S. procedures, will be a major change in European jurisdictions.

Joint and Several Liability[24]

New rules will require that companies jointly responsible for a breach of competition law will be jointly and severally liable. Plaintiffs will have the option to sue one or several infringers for the entire damage, regardless of each company's contribution. Joint infringers may recover any overpayment of liability through contribution claims against other infringers. However, an immunity applicant's liability will be limited to the damages caused to its direct or indirect customers or providers unless recovery from other infringers is unavailable. Small and Medium-sized Enterprises[25] can also be protected from overpayment if (1) their market share is less than 5%, (2) joint and several liability would jeopardize their economic viability and (3) they were not ringleader of the cartel or (4) recidivists.

Defenses[26]

The pass-on defense claiming that overcharge was in whole or part passed on can be invoked by defendants as a defense to a damages claim. Defendants must bear the

---

23 Directive 2014/104/EU Of The European Parliament And Of The Council of 26 November 2014, Recitals 15-33, Chapter II.

24 *Id.* Recitals 37, 38, Chapter III, Article 11.

25 As defined in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises: The main factors determining whether an enterprise is an SME are: staff headcount and either turnover or balance sheet total.

Company category	**Staff headcount**	**Turnover**	or	**Balance sheet total**
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

These ceilings apply to the figures for individual firms only. A firm that is part of larger group may need to include staff headcount/turnover/balance sheet data from that group too.

26 Directive 2014/104/EU Of The European Parliament And Of The Council of 26 November 2014, Recitals 39-44, Chapter IV.

burden of proof and may require disclosure from the claimant and third parties. Indirect purchasers can claim antitrust damages if they can show that that direct purchasers of the cartelist passed on the overcharge to them. This theory may be facilitated by the introduction of a rebuttable presumption if (1) there is an infringement, (2) an overcharge to the direct purchaser, and (3) the plaintiff purchased the cartelized products or their derivatives. Courts will assess the pass on rate.

Standing for Indirect Customers[27]

Indirect customers can also claim antitrust damages on the basis of a rebuttable presumption that their suppliers have passed on the cartel overcharge to them if it can be shown that (1) the defendant committed an infringement, (2) the infringement resulted in an overcharge for the direct purchaser, and (3) the indirect purchaser purchased the good or services that were the object of the infringement.

Quantification of Harm[28]

The quantification of damages remains subject to national rules and the Directive only establishes that the burden of proof shall not render the exercise of the right to damages practically impossible or excessively difficult. The courts will be empowered to estimate the amount of damage, and there will be a rebuttable presumption that the infringement of antitrust law caused the harm.

While the objective of fines imposed by the European Commission is deterrence, the purpose of damages claims in Europe is to repair the harm suffered as a result of an infringement. The Court of Justice of the European Union has described the concept of compensation as placing the injured party in the position it would have been in had there been no infringement. Therefore, compensation includes reparation not only for actual loss suffered (*damnum emergens*), but also for loss of profit (*lucrum cessans*) and the payment of pre-judgment interest (which is not available in the U.S.). Actual loss means a reduction in a person's assets. Loss of profit means that growth of those assets, which would have occurred without the infringement, was stifled.[29]

The Commission also adopted a non-binding Communication[30] on the quantification of damages, including a practical guide,[31] in order to address the perceived difficulty courts, tribunals and parties have in quantifying the loss suffered. The guide sets out various techniques available to identify the amount of the damage and addresses how they can be applied. The Commission does not favor one method over another and

---

27 *Id*. Recital 44, Article 14.

28 *Id*. Recitals 45-46, Article 17.

29 Commission Staff Working Document Practical Guide Quantifying Harm in Actions for Damages Based on Breaches of Article 101 or 102 of the Treaty on the Functioning of the European Union, June 11, 2013, SWD (2013) 2015, {C(2013) 3440}, *available at* http://ec.europa.eu/competition/antitrust/actionsdamages/quantification_guide_en.pdf.

30 *Communication from the Commission on quantifying harm in actions for damages based on breaches of Article 101 or 102 of the Treaty on the Functioning of the European Union*, Official Journal of the European Union (2013/C 167/07), p. 19, June 23, 2013.

31 *Id*.

leaves this decision to a case-by-case analysis of the court. The first step in the analysis is to establish the counterfactual, *i.e.*, the situation the injured parties would have been in but for the infringement. The favored counterfactual technique is the comparator-based method where actual market outcomes are defined in order to compare them with what would have likely happened in the market but for the infringement. In doing so, a comparison can be drawn with the time before the infringement in the same market and what happened in same product but different geographic or similar product markets. Other methods mentioned are simulation models, cost-based and finance-based methods.

Importantly, the Directive also mandates that "Member States shall lay down procedural rules appropriate to ensure that compensation for actual loss at any level of the supply chain does not exceed the overcharge harm suffered at that level."[32]

Implementation of the Directive

Although the Directive will not lead to complete harmonization, there should be real progress toward common ground across the EU 28. The result will likely make it easier and safer for plaintiffs to launch proceedings.

Indeed, the process of complying with the Directive has begun. On July 16, 2016, the German authorities issued a draft set of rules intended to comply with the Directive. Germany has been a pioneer in private antitrust actions so its laws already are broadly similar to what the Directive requires. Nonetheless, the new draft Section 33 of the German Act Against Restraints of Competition details the right to full compensation for victims of competition infringements. Also, the draft law includes an express, though rebuttable, presumption of harm from cartel activity. As required by the Directive, the German statute provides for indirect purchaser standing and a presumption that direct purchasers passed on the overcharge. Courts will be permitted to evaluate the pass on rate. As is the case in the U.S., pass on cannot be used defensively against the direct purchaser.

As could be the case when other member states comply with the Directive, parts of the German law exceed what the Directive requires. The Directive leaves to national courts the decision whether or not to permit discovery. The draft, by contrast, grants the parties a substantive right to discover documents and obtain information, with the exception of leniency documents and settlement agreements. In this instance, Germany's implementation of the Directive effectively will result in important changes in German discovery practice. Discovery has never been allowed before in cartel damages cases in Germany.

Germany's implementation of the Directive is likely to build on the current momentum for private antitrust litigation in German courts. While discovery is likely to remain more limited than in the U.S., other aspects of German procedure will be increasingly familiar to U.S. practitioners. The new rules will no doubt further increase the attractiveness of German courts for businesses to claim damages. However, the lack of detailed rules on collective redress will continue to be a significant hurdle for consumers.

---

32 {C(2013) 3440}, Article 12 (2).

2. The Developing U.K. and EU Private Remedies

While not all EU national parliaments have implemented required changes to facilitate antitrust damages actions, there has been a surge of cases across Europe. Perhaps the most notable development has been the promulgation of a true U.S.-style collective action mechanism in the U.K. While other EU nations have flirted with the collection action concept, none of the resulting procedures resemble U.S. class actions.

U.K.

The U.K. collective action mechanism was enacted in the Consumer Rights Act 2015.[33] The Competition Appeal Tribunal ("CAT"), a specialized court in London, has exclusive jurisdiction over collective action proceedings.[34] The CAT will serve as a gateway by granting a collective proceedings order ("CPO") and certifying the claims that may be brought.[35] In order to grant a CPO, there must be an "identifiable class",[36] claims must raise common issues,[37] and claims must be "suitable" for collective proceedings.[38] Although the CAT has wide discretion, there is still not clear guidance on two fundamental questions that have been at the heart of U.S. class action litigation and certification: what will the standards be for granting a CPO and how will they be analyzed?

The CAT, not the claimants, also will determine whether a collective action will proceed as "opt-in" (each class member must affirmatively opt into the class) or "opt-out" (class members are automatically in the class unless they choose to opt out). In deciding whether the collective action will proceed as opt-in or opt-out, the CAT will determine the strength of the claim, the degree of commonality, and whether opt-in would be practical given the amount of damages an individual class member is estimated to recover.[39] Indeed, the class representative is required to provide an estimate of the damages and a proposal for how they would be distributed among class members.[40] But it is ultimately up to the CAT to determine how each class member's damages will be calculated.[41]

The CAT can calculate damages in the aggregate, via sub-classes, or individually.[42] When dealing with a "large class with largely identical individual claims", the CAT "may calculate the damages on a class-wide basis" by either calculating "a lump sum award against the defendant" or by "using a formula to determine each represented person's claim."[43] One area where the U.K. rules are more flexible than the U.S. is the

---

33 CRA15.

34 *See* CAT Guide to Proceedings 2015.

35 CAT rule 79.

36 CAT guide section 6.37.

37 CAT rule 73(2).

38 CAT rule 79(2)(a)-(g).

39 *See* rule 79(2)(a)-(g).

40 CAT guide, section 6.30 and CAT rule 75(3)(i).

41 CAT guide, section 6.82.

42 *See* CAT rules 73(2), 88(2).

43 CAT guide, section 6.78.

CAT's ability to grant a CPO for the liability portion of the case and then "direct that the quantification of damages proceed as individual issues."[44] If the CAT cannot specify a formula, it may appoint an "independent third party to determine the claims or any disputes regarding quantification."[45]

A major difference between the U.K. and U.S. systems is the extent of class action incentives. The new U.K. rules do not allow for punitive or treble damages.[46] The U.K. rules also limit compensation for class representatives and the use of unclaimed damages,[47] and the CAT has greater control over certifying the class representative based on policy grounds.[48] Finally, the U.K. allows fee-shifting, which puts plaintiffs at greater exposure for bringing unsuccessful claims.[49] Although the incentives to bring collective actions may not be as strong in the U.K. as they are in the U.S., the introduction of opt-out actions clearly has the potential to increase the overall exposure for defendants.

Indeed, on September 8, 2016, U.K. consumers filed an $18.7 billion collective action against MasterCard. The claim is that 46 million U.K. customers overpaid interchange fees from 1992 to 2008. This case will be closely watched and is likely to generate precedents that impact the future of collective actions in the U.K. Procedural successes in this case, or any of the others, will add to the current momentum for these collective actions in the U.K.

The U.K. CAT recently issued a judgment[50] in a single plaintiff MasterCard case that was its first stand-alone action since it was empowered to hear them by the new rules on antitrust damages action. [51] This case is important in several ways. It was not only the first case of many multilateral interchange fee cases but also the first in which the CAT awarded damages in a case under Article 101 of the Treaty of the Functioning of the European Union TFEU and Chapter I of the Competition Act of 1998, both of which prohibit anticompetitive agreements. In determining damages, the CAT admittedly used a "broad axe".[52] The CAT first calculated the overcharge by comparing the actual interchange fee paid by plaintiff Sainsbury with the highest lawful interchange fee it could have been charged in the but-for world. It then turned to pass on and mitigation defenses both of which failed. The result was an award of £68.8 million plus interest.

The MasterCard case was the first decision of a U.K. court explicitly dealing with pass-on.[53] The CAT defined pass-on as an aspect of the process of the assessment of

---

44 CAT guide, section 6.4, 6.79 and CAT rule 88(2)(c).

45 CAT guide, section 6.82 and CAT rule 92(1).

46 CRA15 Schedule 8.

47 CAT Rule 97.

48 CAT Rule 78(2)-(3).

49 CAT Rules 94, 98.

50 *Sainsbury's Supermarket Ltd v. MasterCard Inc.*, Case 1241/5/7/15 (T), 14 July 2016, [2016] CAT 11.

51 *See* Section II.B.2, *supra*.

52 *Supra*, note 10, ¶ 424 (3).

53 Pass-on was recognized by European Courts in cases such as *Courage v Crehan* and *Manfredi*, see footnote 3 and many subsequent cases. It is a well-known concept in many civil law jurisdictions.

damage rather than a defense.[54] It also established strict conditions that must be satisfied for pass-on to be established and reduce a damages award. First, there must be identifiable increases in prices by a firm to its customers. Second, the increase in price must be causally connected with the overcharge. Third, on the balance of probability, another class of claimant, downstream of the claimant must exist to whom the overcharge was passed on. The last condition was included in order to address the risk that any potential claim might become either so fragmented or impossible to prove that the end result would be that the defendant retained the overcharge instead of a successful claimant.[55] The court also perceived this as necessary in order not to render recovery of compensation "impossible or excessively difficult" as stipulated by the Directive[56]. These conditions may constitute the U.K.'s implementation of the Directive which explicitly deals with the concept of pass-on. MasterCard has asked for permission to appeal the judgment.

A significant number of other antitrust cases are pending before judges in England and Wales.[57] Most of them concern cartel damages actions but there are also an increasing number of damages cases relating to abuse of dominance. As noted earlier, class actions have been filed. In December 2016, the CAT will hold its first hearing in a case brought by the National Pensioners Convention against the maker of scooters for elderly people.[58] The first issue to be decided is whether the Convention can represent the class and whether the CAT can issue a collective proceedings order.

Outside the U.K., there are many different kinds of cases in EU national courts. The diversity of approaches taken by national judges in those cases has been a major factor driving the perceived need for harmonization. In particular, there are a growing number of cases in German and Dutch courts. There have also been attempts to launch collective actions but so far only with mixed success.

Germany

In 2015, a case brought by a Cartel Damage Claims Consulting SCRL[59] ("CDC"), an antitrust claims aggregation vehicle established under the laws of Belgium, was dismissed on the basis that (1) the Belgian litigation vehicle did not have sufficient funds to cover the legal costs of its opponents, (2) the transfer was against public morals, and (3) certain claims were transferred to CDC before it was registered to give legal advice.[60] The CDC had obtained claims of 36 cement customers against six cement manufacturers which the German competition authority had fined for cartel activity. The value of the

---

54 *See supra* note 10, ¶ 484. Similar position taken by the German Federal Court in 2011: BGH, judgment of 28 June 2011—KZR 75/10).

55 *Supra* note 18, ¶ 484 (4).

56 *See supra* note 10.

57 Private litigation is pending in front of U.K. courts in relation to cartels, including in CRT, bearings, polyurethane foam, car glass, power cable, smart chips, batteries, LCD, and air cargo.

58 In the Competition Appeal Tribunal: *Dorothy Gibson v. Pride Mobility Products Ltd.*, Case No. 1257/7/7/16.

59 Société coopérative à responsabilité limitée.

60 Landgericht Duesseldorf, Urteil vom 17. Dezember 2013 37 O 200/09 and Oberlandesgericht Duesseldorf.

claims was in excess of 130 million Euros. The CDC has since relaunched proceedings in a different regional court in Mannheim.[61]

The Netherlands

Dutch courts have also been active in attracting antitrust damages litigation, including collective actions. The Netherlands so far is the only EU member state where a collective settlement of mass claims can be declared binding on an entire class on an opt-out basis.

Recent cases in the Netherlands also have confirmed the availability of the pass-on defense in antitrust damages action[62] and that parent companies are not liable for damages arising from antitrust infringement committed by their subsidiaries which stands in contrast to other case law in Europe.

In a case following on from the European Commission's Paraffin Wax cartel decision,[63] the CDC asserted claims that were assigned to it from customers of companies fined by the Commission in a court in the Hague. The CDC so far has shown that it is able to cover potential litigation costs, a hurdle it faced in the German cement litigation.[64] Although different CDC entities are acting, this result shows the possible divergent views on collective actions between EU member states.

Two similar proceedings are pending following European Commission decisions relating to the Sodium Chlorate[65] and the Air Cargo[66] cartels.

3. Brexit Impacts

Because the U.K. is now the most sophisticated jurisdiction for antitrust damages actions, an obvious question arises: What impact will Brexit have? Assuming a hard Brexit (withdrawal from the EU with no application of EU law), the impact could be significant though it will not likely be felt until the parameters of Brexit are known. Rules for antitrust damages, however, will not be on the agenda anytime soon.[67] This uncertainty alone is likely to impact forum choices.

Post Brexit, plaintiffs may be more inclined to choose the EU over the U.K. for litigation unless the rules are similar to what they are now. For example, if European Commission decisions are no longer binding on U.K. judges, there would be an incentive to litigate where they are. The same would be true if European law and rules on the

---

61 Landgericht Mannheim, 2 O 195/15.

62 July 8, 2016, the Dutch Supreme Court, *TenneT v. ABB*.

63 Case COMP/39181—Candle Waxes.

64 C-09-414499-HA ZA 12-293.

65 C-13-500953-HA ZA 11-2560.

66 C-13-553534-HA RK 13-353 (Claim was brought by Claims Funding Europe Limited (CFE) a special purpose vehicle).

67 The Article 50 negotiations will only deal with the parameters of the exit. Competition law is likely not even on this agenda and will be discussed once Brexit has occurred.

allocation of jurisdiction and the enforcement of judgments (*e.g.*, Brussels Regulation[68]) no longer apply. The Brussels Regulation successfully regulates and facilitates the cross-border enforcement of judgments in relation to civil and commercial matters. The Regulation also deals with jurisdiction of courts including over claims relating to defendants not domiciled in their jurisdiction.

Brexit might also affect U.K. courts' willingness to assert jurisdiction over all of the worldwide parties in a cartel case. Recent cartel damages claims have proceeded in the U.K. without a strong connection of the cartel to the U.K. Companies not domiciled in the U.K. (or the EU) have been brought into the jurisdiction on the basis of a so-called "anchor defendant"—the primary defendant domiciled in the U.K. chosen for the ostensible purpose of bringing the claim before a U.K. court. Even if U.K. common law rules would allow jurisdiction in the absence of the Brussels Regulation, the question will be whether the U.K. courts continue to provide the one-stop-shop a plaintiff might desire. It is unclear whether these differences would discourage so called stand-alone actions which do not rely on prior infringement findings.

While foreign jurisdictions are still catching up, the bottom line is that the U.S. is no longer the only important forum. There are still no treble damages, no contingent fee arrangements, and the English rule for attorney's fees still prevails. However, the ability to recover for worldwide sales and more user-friendly procedural rules are healthy incentives for sophisticated plaintiffs.

III. ISSUES FOR PRACTITIONERS

So if it is clear that cases are likely to be filed both in the U.S. and elsewhere, what does that mean for decisions and strategies in litigation?

A. Arbitration

To arbitrate, or not, is an early and critical question in any case for which that course is at least arguably available. Not infrequently, supplier contracts have arbitration clauses in them. Does the availability of foreign remedies change the calculus as to whether arbitration is desirable? Of course, the facts of the case matter as do the arbitration forum and its procedural rules. At a minimum, though, a close examination of the possible legal jurisdictions is necessary, followed by an equally close comparison of the available arbitral forums, processes and remedies.

At the very least, the following new questions must be answered:

(1) Where is there jurisdiction? How would a foreign court's analysis of jurisdiction impact the timing of its decision and relate to key events in litigation elsewhere?

---

68 Council Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters of 1/03/2002 and Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast) which applies to legal proceedings and judgments of the time after 10 January 2015.

(2) What damages are available in each forum? Overcharges on worldwide sales? Or something less? What are the U.S. sales subject to trebling compared to sales at issue in an arbitration?

(3) What defenses are available in a foreign court compared to what an arbitrator would consider?

(4) Is there joint and several liability, or are there limitations to a party's own sales? How would contribution rights be enforced?

(5) How quickly does one forum proceed compared to the other?

Certainly there are many other important considerations. The firm conclusion now, though, is that the arbitration analysis is much more complicated and cannot be made on the same basis as before foreign remedies became more readily available.

B. Discovery

Lawyers on both sides of the plaintiff-defense fence and both sides of the Atlantic are likely to focus very quickly on these questions: What part of the U.S. discovery record will have to be produced in foreign cases? Are there parts of the foreign case discovery that would not normally be reached by even the broad U.S. discovery procedure—but might be imported into a U.S. case because they are discoverable abroad?

Probably the first battleground in the U.S. court would be the drafting of a protective order. Commonly, protective orders limit use of confidential documents to "this case." Should that language be changed to "this case or any other case with fundamentally similar allegations," *i.e.*, cases filed elsewhere? Arguments for and against opening up the typical language are not difficult to frame. A defendant might begin with the idea that foreign cases should be governed by their discovery laws not, as a practical matter, by what is discoverable in the U.S. The response could be: let the foreign court decide what it wishes to consider, rather than foreclosing the issue by walling off discovery in the U.S. case.

This discussion also assumes a foreign court would honor a U.S. protective order or enter one of its own for the documents at issue. Is there any basis for that assumption? At present, there is very little law on this subject nor is there reason to believe that all judges in all foreign jurisdictions would rule in the same way. Protective orders, of course, are supposed to shield confidential documents with proprietary information in them. Both plaintiffs and defendants would be wise to pay close attention to confidentiality designations.

Also implicit in this discussion has been the idea that U.S. discovery is always broader than foreign discovery and the litigation will concern the extent to which extensive U.S. discovery can be used elsewhere. But could there be information discoverable abroad that would not be discoverable in the U.S. but for its production in a foreign court? And would a foreign court shield that discovery from use elsewhere? Again, this is virtually unexplored territory and the reach of U.S. foreign discovery is sufficiently broad that it may not matter very much. Perhaps a foreign court, however, would have a different calculation of the burden of producing materials situated in that foreign jurisdiction, and those materials might then be brought before a U.S. court.

As noted earlier, corporate immunity and witness statements provided to the European Commission and other national authorities are not discoverable there. Whether they can be discovered in the U.S. has been hotly contested with the European authorities frequently providing amicus statements opposing discovery.[69]

The law requires a multi-factor comity analysis, and some U.S. Courts have recently denied discovery of confidential leniency communications and non-public EC decisions.[70] An earlier case reached a different result.[71]

This is yet another area where there could be an awkward interplay between U.S. and foreign cases. What if U.S. counsel obtains that kind of discovery at the same time she is representing the same claimant abroad in cases where those statements cannot be produced?

At present, there are few reported cases that can provide sound guidance for discovery. As cases proliferate, that may change. Probably the best that can be done now is for there to be close coordination between U.S. and foreign counsel.

C. Settlement

The complexity of settlement analysis has increased in equal measure to the proliferation of foreign remedies. In years past, that calculation was much simpler: What are the sales in the case? What is the overcharge? What is the strength of the liability case? Now, both the U.S. FTAIA jurisdictional analysis and settlement value of foreign cases

---

69 *See*, *e.g.*, Letter of Georg De Bronett, EU Comm'n, *In re Vitamins Antitrust Litig.,* 2002 U.S. Dist. LEXIS 26490 (D.D.C. Jan. 23, 2002) ("[T]he effectiveness of the EU antitrust procedures could indeed be seriously undermined" if leniency communications were discoverable); *In re Rubber Chemicals Antitrust Litig.*, 486 F. Supp. 2d 1078 (N.D. Cal. 2007) (citing to the EC's brief opposing discovery of confidential EC materials); Decl. of P. Lowe, *In re Flat Glass Antitrust Litig.*, No. 08-180 Dkt, 200-3 (Oct. 7, 2009) (disclosure "could seriously undermine the effectiveness of the Commission's and other authorities' antitrust enforcement actions" and "authorizing discovery in American litigation of documents that are strictly confidential under European competition law would be highly detrimental to the sovereign interests and public policies of the European Union"); Mem. of Law of *Amicus Curiae* the European Comm'n i/s/o Defendants' Objections, *In re Payment Card Interchange Fee and Merchant Discount Antitrust Litig.*, 1:05-md-01720 Dkt. 1372 (E.D.N.Y. March 19, 2010) (objecting to production of confidential investigation materials: "These documents are confidential under the laws of the EU and were provided to Visa and MasterCard by the Commission on the explicit condition that they maintain the confidentiality of those documents. Their production would hinder the European Commission's ongoing ability to detect and investigate unlawful, anticompetitive activities."); Letter of European Comm'n, *In re Cathode Ray Tube (CRT) Litig.*, Case 3:07-cv-05944-SC Dkt. 2449 (N.D. Cal. March 26, 2014) (objecting to disclosure of non-final unredacted findings because it would, *inter alia*, undermine the EC's leniency program which requires confidentiality to be effective). The EC has submitted similar amicus briefs to National Courts arguing that corporate leniency statements should not be discoverable. *See*, *e.g.*, Observations of the European Comm'n Pursuant to Art. 15(3) of Reg. 1/2003, *National Grid Electricity Transmissions PLC v. ABB Ltd. et al.*, In the High Court of Justice Chancery Div., March. 11, 2011.

70 *See*, *e.g.*, *In re Rubber Chem. Antitrust Litig.*, 486 F.Supp.2d 1078 (N.D. Cal. 2007) (denying discovery of a leniency applicant's confidential communications with the EC); Order Denying Motion to Compel, *In re Cathode Ray Tube (CRT) Litig.*, Case 3:07-cv-05944-SC Dkt. 2463 (N.D. Cal. March 26, 2014); Order Denying Direct Action Plaintiffs' Renewed Motion to Compel Production of the European Commission Decision; *id.* Dkt. 3133 (N.D. Cal. Nov. 20, 2014).

71 *In re Vitamin Antitrust Litig.*, 2002 U.S. Dist. LEXIS 26490 (D.D.C. January 23, 2002) (allowing discovery of submissions to foreign competition authorities).

must be added to the mix, as well as timing considerations stemming from the speed of proceedings in foreign jurisdictions (or arbitrations).

Normally, global settlements are desirable—is that still true? A plaintiff might try to use a potentially quicker U.S. treble damage process to achieve a global settlement that includes both treble damage value and worldwide sales value (albeit without treble damages). Perhaps a defendant would prefer the opposite course: settle the treble damage case and let the foreign cases develop on their own. At least from a conceptual viewpoint, global arbitration probably would be the most straightforward vehicle to drive settlements.

D. Coordination

The proliferation of foreign companion cases underlines the importance of coordination among counsel. But coordination in itself presents legal issues. A routine practice in the U.S. is for lawyers on the same side to enter into joint defense or common interest arrangements often memorialized in writing. That practice is much less common elsewhere. The validity of a joint defense agreement among U.S., U.K. and EU counsel has not been litigated and is an open question. The common interest privilege, however, has been recognized.[72]

Of course, the information disclosed in such an arrangement must be protectable as privileged. The exchange of non-privileged material among parties with a common interest cannot confer a privilege where one does not otherwise exist. Note also that the EU does not recognize a privilege for in house lawyer communications.[73] Privilege also does not apply to in-house counsel in France, the Netherlands, Austria and Sweden, among other jurisdictions.

As for the subjects of coordination, discovery is an obvious example. But there are other areas that can be equally important:

1. Jurisdiction

Jurisdiction may be available in several forums outside the U.S. Each will have its own rules—albeit rules likely to be increasingly harmonized in Europe under the Directive—and speed to judgment. Each of the possibilities must be compared to what is likely to happen in the U.S.

2. Briefs and Discovery

In most cases, briefing on substantive legal issues will be significantly different. The relevant competition statutes are not the same. Factual representations, however, cannot diverge without potentially serious credibility impacts, nor can representations be different about the availability of discovery and the burdens of producing it.

---

72 *See Winterthur Swiss Insurance Company and another v. AG (Manchester) Ltd.* EWHD 839 (2006); *Buttes Gas and Oil Co. v. Hammel* (No. 3) QB223, CA (1981).

73 *See* Case C-550/07, *Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v. European Commission* (2010).

3. Experts

Using a single economist surely is cheaper than paying for two or more.[74] But how many economists have true transatlantic reputations and are equally comfortable in U.S. and foreign litigation? Economists based in the U.K. or Europe rarely have experience with the intensive scrutiny of expert opinions that is typical of U.S. antitrust litigation. Nor could they be expected to have the same amount of experience with the kinds of expert issues that U.S. economists have been studying for decades. At the same time, coordinating opinions of multiple economists on the same or similar subjects is challenging. It is difficult to see how the opinions of an expert in a U.K. case, for example, would not become known in the U.S. and turned into yet another source of expert discovery, and vice versa.

4. Collateral Impact of Factual Findings

Counsel should be keenly aware of potential collateral effects of foreign judgments. Generally speaking, the doctrine of comity allows U.S. courts to recognize foreign judgments if the party against whom the judgment will asserted had the opportunity for a full and fair hearing, the foreign court had jurisdiction, and it does not contravene U.S. public policy.[75] Once a U.S. court recognizes a foreign judgment, it may have collateral estoppel effects exactly like a domestic judgment. The next question is whether the scope of the preclusive effect is governed by U.S. law or the law of the foreign nation.[76] In short, the rules governing the preclusive effect of foreign judgments are complex.[77] Let it suffice to say that practitioners must beware of the potential collateral impact of foreign judgments as the U.K. and EU become increasingly common jurisdictions for private antitrust actions.

Foreign courts may similarly recognize U.S. judgments and, under certain conditions, give those judgments preclusive effects. German courts, for example, would give effect to foreign judgments if they are recognized under the conditions of the civil procedure code.[78] However, judgments can only have effect in Germany if those effects are recognized under German law. Treble damage judgments are a well-known exception for that reason. In Germany as well as in Japan, foreign judgments containing treble damages and punitive damages are not enforceable.[79] Whether other elements of judgments containing findings on treble damages retain effect is an unresolved question under German law. Generally, German courts would recognize procedural as well as substantive effects of a foreign judgment. The law is complex in particular on the question

---

74 The U.S. trend currently is to break up economic issues, particularly for class certification, among multiple economists.

75 *Hilton v. Guyot*, 159 U.S. 113 (1895).

76 *See*, *e.g.*, *Alfadda v. Fenn*, 966 F. Supp. 1317 (S.D.N.Y. 1997) (applying U.S. law); *United States v. Kashamu*, 656 F.3d 679 (7th Cir. 2011) (suggesting that the foreign court's preclusion rules apply).

77 *See Restatement (Fourth) of Foreign Relations Law of United States Jurisdiction* (Tentative Draft No. 2 March 22, 2016).

78 *See* German Civil Procedure Code (Zivilprozessordnung), par. 328.

79 *Bundesgerichtshof [BGH] [Federal Court of Justice]* June 4, 1992, 118 BGHZ 312 (Ger.); *Ore. State Union No-sokon v. Mansei Ko-gyo Co.*, 51 Minsu 2573 (Sup. Ct., July 11, 1997).

of whether effects will be broader than among the parties, and a detailed assessment of this complex topic is beyond the scope of this article.

With the increasing frequency of parallel cartel damages proceedings around the world, more useful precedents likely will emerge. In the meantime, awareness of this issue is critical.

IV. CONCLUSION

The practice of antitrust law is now truly international. For many years, practitioners have understood that competition enforcement authorities coordinate their efforts, and a plan to deal with many or all of them is necessary. Now the same is true for damages actions that will add many more variables to what are already complex disputes in the U.S. civil arena. Collective actions and private damages actions throughout the EU's 28 member states now have joined an already crowded field of U.S. class actions, direct actions and states' Attorney General cases. Unpleasant surprises await practitioners who do not pay close attention to developments abroad and shape their positions and strategies for a global litigation landscape.

HOME RUN OR STRIKEOUT? THE UNSETTLED RELATIONSHIP BETWEEN THE SPORTS BROADCASTING ACT AND CABLE PROGRAMMING

By Steven M. Perry[1]

I. INTRODUCTION

The Sports Broadcasting Act ("SBA") exempts from the antitrust laws "any joint agreement . . . by which any league of clubs participating in professional football, baseball, basketball, or hockey contests sells or otherwise transfers all or any part of the rights of such league's member clubs in the sponsored telecasting of the games of football, baseball, basketball, or hockey, as the case may be, engaged in or conducted by such clubs."[2]

In the 55 years since the SBA was enacted, only a handful of courts have addressed the question of whether the antitrust exemptions contained in the SBA apply to basic cable programming. This article reaches two conclusions with respect to that question. First, and contrary to what various commentators have assumed, no court has ever held that league-wide agreements that license sports programming on basic cable channels are, or are not, exempt from the antitrust laws under the SBA. Second, the application of current principles of statutory interpresentation demonstrates that the SBA's exemptions do, in fact, apply to basic cable programming.

To be specific, and as discussed in more detail in section II of this article, various commentators have stated that in November 1992, the district court in *Chicago Professional Sports Ltd. Partnership v. National Basketball Association*[3] held that cable programming fell outside the SBA because it did not constitute "sponsored telecasting." Those commentators have, however, overlooked the district court's clarification one month later, when it explained that it had made no such holding:

> "[W]e have not yet ruled on the question of whether the [challenged agreement] is exempt under the SBA. We have merely denied the NBA's motion for summary judgment that it is."[4]

Three years later, the same court confirmed that it had not yet decided the SBA issue.[5]

---

1 Mr. Perry is a partner at Munger, Tolles & Olson LLP, whose clients include media companies and sports leagues. The views expressed in this article are those of the author and do not necessarily represent the views of Munger, Tolles & Olson, its lawyers, or its clients.

2 15 U.S.C. § 1291.

3 808 F. Supp. 646 (N.D. Ill. 1992).

4 *Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n*, No. 90 C 6247, 1992 WL 373027 at *1 (N.D. Ill. Dec. 10, 1992).

5 *See Chicago Prof'l Sports Ltd. P'ship*, 874 F. Supp. 844, 856 n.12 (N.D. Ill. 1995) ("[T]elecasting on TNT may be considered sponsored telecasting because TNT does receive some revenues from advertising in addition to subscription fees. . . .").

Commentators also (incorrectly) cite a Third Circuit decision for the proposition that basic cable programming does not satisfy the "sponsored telecasting" requirement set out in the SBA. In *Shaw v. Dallas Cowboys Football Club Ltd.*,[6] the court addressed the SBA's application to a commercial-free package of NFL games offered by satellite provider DirecTV. Although the court's opinion included broad language, the court neither faced nor decided any issue involving sports programming on basic cable channels, where sponsors and their advertisements take up substantial air time, because the issue before the Court involved *only* commercial-free pay television. Indeed, the district court responsible for implementing the Third Circuit's mandate on remand explicitly stated that the appellate court's decision "did not address whether broadcasting the games on the Internet *or cable television* was an exempt activity under the SBA, but *only* found that satellite broadcasts of NFL games were not exempted." [7]

In sum, the question of whether the SBA exempts league agreements with basic cable programmers from antitrust scrutiny remains unsettled. In golfing parlance, the green is open. This article suggests that if a court today were to apply basic principles of statutory interpretation to the relevant language in the SBA, it would find that the SBA *does* exempt league-wide agreements involving basic cable programming from the antitrust laws. But before we undertake that analysis, some background is in order.

II. A STATUTE IS BORN

A. The Judicial Decision That Prompted Congress to Enact the SBA

The SBA was enacted in large part in response to a district court ruling that the NFL's sale of a games package to the CBS television network violated section 1 of the Sherman Act.[8] The court's decision in 1961 cannot be understood without a discussion of the prior proceedings in the same case that had occurred eight years earlier, in 1953.

In the early 1950's, some of the twelve NFL teams had individual agreements with the soon-to-be-defunct DuMont Network, which televised a single "Game of the Week" and certain other games.[9] Because the NFL was concerned about a potential adverse effect of televised games on stadium admissions, it adopted a set of by-laws in 1951 that imposed restrictions on "[a]ny contract entered into by any club for telecasting or broadcasting its games. . . ."[10] The Department of Justice sued to block the enforcement of several of the restrictions.[11]

The district court, after a lengthy trial, held that some of the NFL by-laws unreasonably restricted competition in violation of the Sherman Act. In particular, the court struck down a by-law that prohibited the "telecasting" of games into a team's home territory on a day

---

6 172 F.3d 299, 301-02, and 301 n.9 (3d Cir. 1999).

7 *Schwartz v. Dallas Cowboys Football Club Ltd.*, 157 F. Supp. 2d 561, 577 (E.D. Pa. 2001) (emphasis added).

8 *United States v. Nat'l Football League* (*U.S. v. NFL II*), 196 F. Supp. 445, 447 (E.D. Pa. 1961).

9 *See NFL on DuMont*, Wikipedia.com, https://Wikipedia.org/wiki/NFL_on_DuMont (last visited on September 12, 2016).

10 *United States v. Nat'l Football League* (*U.S. v. NFL I*), 116 F. Supp. 319, 327-29 (E.D. Pa. 1953).

11 *Id.* at 321.

when that team was playing an away game that was being televised in its home territory.[12] As an example, if Green Bay was playing at Washington, a game that same day between the Bears and the Giants could not be telecast into the Green Bay TV market.

The court held that the NFL had presented "no factual justification for [the] suppression of competing telecasts" in a team's territory if the team was playing an away game, rather than a home game, on that day.[13] The court rejected as "speculation" the NFL's argument that attendance at future home games would decline merely because fans had watched a telecast involving other teams a few weeks earlier.[14]

However, the court upheld as reasonable a bylaw that precluded the broadcasting of "outside games" into the home territories of other teams on days when the other team was playing *at home*.[15] The court observed that:

> "Professional teams in a league . . . must not compete too well with each other, in a business way. . . . If all the teams should compete as hard as they can in a business way, the stronger teams would be likely to drive the weaker ones into financial failure. If this should happen not only would the weaker teams fail, but eventually the whole league, both the weaker and the stronger teams, would fail, because without a league no team can operate profitably.[16]

The court further concluded that weaker teams "benefit greatly" from a restriction on the telecasting of "outside games" into their home territories on days when they are playing at home, because "its immediate effect is to protect the weak teams and its ultimate effect is to preserve the League itself." [17] The court held that:

> "The purposes of the Sherman Act certainly will not be served by prohibiting the defendant clubs, particularly the weaker clubs, from protecting their home gate receipts from the disastrous financial effects of invading telecasts of outside games. The member clubs of the National Football League, like those of any professional athletic league, can exist only as long as the league exists. The League is truly a unique business enterprise, which is entitled to protect its very existency by agreeing to reasonable restrictions on its member clubs. The first type of restriction imposed by [the by-laws] is a reasonable one and a legal restraint of trade."[18]

The court entered a final judgment in 1953 that included a broad prohibition on any agreement that had "the purpose or effect of restricting the areas in which broadcasts or

---

12 *Id.* at 326-27.

13 *Id.*

14 *Id.*

15 *Id.* at 324-25. The court defined "outside games" as games "played outside the home territory of a club in which the club was not a participant." *Id.* at 321 n.2.

16 *Id.* at 323.

17 *Id.* at 325.

18 *Id.* at 325-26.

telecasts of games . . . may be made."[19] The final judgment did allow restrictions on the telecasts of games in the home territory of a team that was playing at home that day.[20]

The NFL, apparently satisfied with the 1953 decision, chose not to appeal it. Indeed, an official NFL publication described the 1953 decision as "laying the groundwork for pro football's emergence as the game of the American mid-century." [21]

At the time of the 1953 trial, each NFL team's practice was to enter into an individual agreement with a sponsor, station or network involving radio and/or television rights. In 1960, however, the American Football League ("AFL") began operations and signed a five-year, league-wide television contract with ABC. In response, the NFL decided to enter into a two-year agreement with CBS that covered all NFL teams.[22] The NFL asked the district court, which had retained jurisdiction over the final judgment, to approve the newly signed CBS agreement. The court chose instead to enjoin the NFL from performing the agreement, holding that the member clubs had "by agreement . . . eliminated competition among themselves in the sale of television rights," in violation of a provision in the final judgment that barred restrictions on the areas in which telecasts could be made.[23]

Three months after the court's order enjoining the NFL's sale of games to CBS, Congress enacted, and President Kennedy signed, the SBA.[24]

B. The Process That Led To The SBA's Enactment

The SBA originated in the Antitrust Subcommittee of the House Judiciary Committee. Rep. Emanuel Cellar, the Chair of both the Judiciary Committee and the Antitrust Subcommittee, explained to the House that "[t]he purpose of this bill is to enable the member teams of a professional sports league to pool their separate rights in the sponsored telecasting of their games and to sell the resulting package of pooled rights to a television network or other purchaser without thereby violating the antitrust laws."[25] Rep. Cellar also noted that the AFL had operated under a pooled contract during the 1960 season and was free to continue to do so, leaving the NFL at a disadvantage.[26]

---

19 *U.S. v. NFL II*, 196 F. Supp. 445, 447 (E.D. Pa. 1961).

20 *Id.* at 447 n.5. The text of the district court's final judgment is not included in the Westlaw versions of the 1953 or 1961 opinions but can be found in the transcript of an August 1961 Congressional hearing. *See Telecasting of Professional Sports Contests: Hearing Before the Antitrust Committee of the House Committee on the Judiciary on H.R. 8757*, 87th Cong., 1st Sess., at 24-27 (Aug. 28, 1961) [hereinafter "8/8/61 H'rg Tr."].

21 *See* The First Fifty Years—The Story of the National Football League 234 (1969).

22 *U.S. v. NFL II*, 196 F. Supp. at 446.

23 *Id.* at 447. The court reasoned that because the agreement gave CBS the right to determine where games would be shown, and because the individual teams had agreed not to sell their television rights separately, the agreement was at odds with the final judgment. *Id.* According to NFL Commissioner Pete Rozelle's subsequent Congressional testimony, the district judge stated at the 1961 hearing that he could not remember why the provision in question had been included in the final judgment, given that a league-wide TV contract was not "at issue at that time." 8/8/61 H'rg Tr. at 6-7.

24 1961 Cong. Rec. 21552 (Sept. 30, 1961).

25 1961 Cong. Rec. 20059 (Sept. 18, 1961).

26 *Id.*

Rep. Cellar further explained that under the district court's recent ruling, "the members of a professional sports league cannot lawfully act in concert to assure member clubs with weak teams or limited home territory television markets an adequate amount of television income and of television coverage for games played away from home. Yet, should these weaker teams be allowed to founder, there is danger that the structure of the entire league would become impaired and its continued existence imperiled."[27] Rep. Cellar stated that as a consequence, the Judiciary Committee "believes that the great public interest in viewing professional league sports warrants some accommodation of antitrust principles . . . ."[28]

The House passed the bill the day it was introduced, after a brief debate.[29] The Senate passed the bill without any meaningful debate three days later, on September 21, 1961.[30] President Kennedy signed the bill into law on September 30, 1961.[31]

III. THERE IS VERY LITTLE CASE LAW DISCUSSING THE MEANING OF "SPONSORED TELECASTING" OR ITS APPLICATION TO CABLE PROGRAMMING

A. The WGN Litigation (1991-1996)

It is undisputed that over-the-air network broadcasts of the four categories of professional sporting events set out in the SBA meet the definition of "sponsored telecasting" as used in the SBA. In contrast, the question of whether "sponsored telecasting" includes cable programming that is in part supported by advertising revenue remains unsettled.

The courts did not address the applicability of the SBA to league agreements with cable programmers until the early 1990's, when the owner of the Chicago Bulls, joined by Chicago-area "superstation" WGN, sued the NBA after the league voted to reduce the number of games that the Bulls could authorize WGN to broadcast.[32] That litigation, which lasted more than seven years, resulted in several opinions that addressed, in a limited fashion, the scope and application of the SBA.

Various commentators have stated that the district court in the *WGN* case held that agreements between a sports league and cable providers or programmers were not

---

27 *Id.* at 20060.

28 *Id. See also id.* at 20061 (statement of Rep. McCulloch that because the "authority to enter into a package television contract is necessary to protect the financial and business interests of the weaker teams of the league," the Judiciary Committee believed it to be "desirable to grant a very narrow exemption from the antitrust laws").

29 *Id.* at 20064.

30 *Id.* at 20662. Senator Hruska offered an explanation of the bill's purpose just prior to the Senate vote: "[t]he purpose of this bill is to permit professional sports leagues to deal jointly in the sale of their TV rights and, by grouping their weaker and stronger clubs and those clubs with greater or lesser home territory population, to provide equal access to television facilities and television income for all member clubs of their league." *Id.* The Senate Report noted an additional concern for "the public interest in viewing professional league sports." S. REP. NO. 1087 (1961), *as reprinted in* 1961 U.S.C.C.A.N. at 3044 [hereinafter "1961 Senate Report"].

31 *Id.* at 21552.

32 *See Chicago Prof'l Sports Ltd. P'ship, et al. v. Nat'l Basketball Ass'n* (*WGN I*), 754 F. Supp. 1336, 1338-40 (N.D. Ill. 1991).

protected by the SBA.[33] A closer reading of the various decisions in the *WGN* litigation demonstrates, however, that while the district court was at times skeptical of the contention that the SBA protected agreements with cable providers or programmers, it did not render any such holding. In fact, the district court expressly stated that it had *not* resolved the issue, in an unpublished 1992 opinion that no court or commentator appears to have noticed.

In *WGN I*, the district court held that an NBA restriction on the number of games that a team could license to a "superstation" was an invalid restraint under the Sherman Act.[34] The court rejected the NBA's argument that the restriction was exempt under the SBA, holding that the SBA did not apply because the broadcasting rights in question were being licensed by the Bulls and had not been transferred or sold on a league-wide basis, as 15 U.S.C. § 1291 requires.[35] The district court enjoined the NBA from enforcing the challenged restriction.[36]

The court in *WGN I* addressed the applicability of the SBA to cable programming only in passing, when it noted that the SBA protected agreements involving "national broadcast rights . . . licensed to NBC (or possibly to TNT, assuming that TNT's broadcasts fit within the statutory meaning of 'sponsored telecasting'). . . ."[37]

The Seventh Circuit affirmed the lower court's injunction.[38] The court of appeals disagreed in part with the district court's interpretation of the SBA, but it ultimately held that the SBA did not apply to the challenged restraints (for reasons not relevant to this article).[39]

The Seventh Circuit's decision did not end the litigation, because the Bulls and WGN had challenged other NBA restraints as well. On remand, the district court denied the NBA's motion for summary judgment on the remaining claims.[40] It is the district court's decision in *WGN III* that commentators cite as holding that league agreements with cable providers and programmers are not covered by the SBA.[41] A careful review of the opinion, and of a subsequent opinion that clarified the district court's intent, proves otherwise.

---

33 *See*, *e.g.*, Babette Boliek, *Antitrust, Regulation, and the "New" Rules of Sports Telecasts*, 65 Hastings L.J. 501, 533 and n.185 (2014) (stating that the district court in the WGN case had found that cable television was not sponsored telecasting under the SBA); Ross C. Paolino, *Upon Further Review: How NFL Networks Is Violating the Sherman Act*, 16 Sports Law. J. 1, 11 (2009) (same).

34 *WGN I*, 754 F. Supp. at 1364. The court accepted the NBA's definition of a "superstation" as a commercial over-the-air station whose signal is received by more than 5% of U.S. cable subscribers. *Id.* at 1345. WGN fit that description at the time, no doubt aided by the fact that its Bulls broadcasts featured Michael Jordan in his prime. The NBA's restrictions on the superstation licensing rights of individual teams were intended to protect the TV audience for the NBA games that the league had licensed to NBC and to cable programmer TNT. *Id.* at 1345-47.

35 *Id.* at 1350.

36 *Id.* at 1364.

37 *Id.* at 1351.

38 *See Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n* (*WGN II*), 961 F.2d 667 (7th Cir. 1992).

39 *Id.* at 671.

40 *See Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n* (*WGN III*), 808 F. Supp. 646, 651 (N.D. Ill. 1992).

41 *See*, *e.g.*, Boliek, *supra* note 33, at 533 n.185; Paolino, *supra* note 33, at 10 n.70.

The NBA restrictions at issue in *WGN III* involved the "NBA Superstation Same Night Rule," pursuant to which individual teams were not permitted to license superstation broadcasts of NBA games on the same night that the league had licensed TNT to broadcast a game.[42] The NBA moved for summary judgment in part on the ground that the "Same Night Rule" was exempt under the SBA by virtue of the rule's inclusion in the NBA's contract with TNT.[43] In the course of denying the NBA's motion for summary judgment, the district court noted that "'[s]ponsored telecasting' is not expressly defined by either the SBA or by any subsequent case law."[44] The court also stated that "*it is not clear* that TNT constitutes 'sponsored telecasting' within the SBA's meaning." [45] The court then quoted the House Report's statement that "[t]he bill does not apply to closed circuit or subscription television," and it stated that the "plain meaning" in 1961 of "subscription television" "might arguably have referred only to a pay-per-view service."[46] On the other hand, the court deemed it "equally likely" that in 1961, "'sponsored telecasting' would not have included such hybrid services as TNT and ESPN."[47]

To recap:

(1) the court in *WGN III* was addressing a summary judgment motion by the NBA based on its preferred interpretation of the SBA;

(2) the court concluded that the proper statutory interpretation of the SBA was "not clear" and that the two differing interpretations proffered by the parties were "equally likely" to be correct; and

(3) the court acknowledged the requirement that it should base its decision on the meaning of the relevant statutory language "at the time the legislation [was] passed," but cited no such evidence.

Nevertheless, despite the court's uncertainty and the lack of relevant evidence, and despite the fact the court was addressing a defendant's motion for summary judgment and was not deciding the outcome of a bench trial, the court stated that it had "conclude[d]" that TNT's programming "falls outside the statutory meaning of 'sponsored telecasting.'"[48]

That certainly sounds like a holding, and various commentators have treated it as such. Fortunately, we do not have to guess about the district court's true intentions because just one month later, the court made those intentions clear when it addressed the NBA's request that the court certify its decision for immediate appeal under 28 U.S.C. § 1292(b).

---

42 *WGN III*, 808 F. Supp. at 647.

43 *Id.*

44 *Id.* at 650.

45 *Id.* at 649 (emphasis added). It is notable that while the court acknowledged that statutes "must be construed according to the plain meaning of their terms at the time the legislation is passed," the court's opinion referenced *no* contemporaneous uses of "sponsored," "telecasting," or "sponsored telecasting." *Id.* at 650.

46 *Id.* at 650.

47 *Id.*

48 *Id.* at 650.

The district court denied the NBA's request on several grounds, but the "more important" ground was that:

> "*we have not yet ruled* on the question of whether the Superstation Same Night Rule is exempt under the SBA. We have merely denied the NBA's motion for summary judgment that it is."[49]

This statement makes it obvious that the court's purported holding in its November 1992 opinion that league agreements with TNT were not exempt under the SBA was poor drafting, not a holding, and has no precedential effect.[50]

Three years later, the district court in the *WGN* case held a nine-week bench trial on plaintiffs' remaining claims. As discussed below, the court's post-trial opinion makes it even clearer that the court had not held in *WGN III* that league-wide agreements with cable programmers were not protected under the SBA.

In the three years between the district court's initial rulings and the trial, the NBA had taken various steps in an effort to satisfy the SBA requirement (at issue in *WGN I* and *WGN II*) that to be exempt from antitrust scrutiny, an agreement must involve a transfer or partial transfer of "the rights of [the] league's member clubs," rather than a transfer of an individual team's rights.[51] Under the NBA's revised approach, NBC had the right to televise all 1107 regular season NBA games, but the NBA retained the ability to license up to 85 games "to national cable networks (including superstations)."[52] The district court found that "on its face, [this] transfer falls within the language of section 1291" of the SBA.[53]

The district court then addressed, but did not decide, the proper interpretation of "sponsored telecasting" as used in the SBA. As noted above, the NBA's agreement with NBC allowed the NBA to license 85 games to cable networks.[54] The agreement separately allowed the NBA to "enter into agreements for subscription and pay-per-view transmissions of games . . . ."[55] When describing this provision, the district court added a footnote that demonstrates that the court had *not* held in *WGN III* that league agreements with TNT, a cable programmer, fell outside the SBA. The footnote begins with a statement that an NBA agreement for "subscription and pay-per-view transmission of games" is "not covered by the [SBA] because the SBA only applies to agreements regarding 'sponsored telecasting.'" [56] The court then *contrasted* such programs with TNT's cable programming:

---

49 *Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n* (*WGN IV*), No. 90 C 6247, 1992 WL 373027, at *2 (N.D. Ill. Dec. 10, 1992) (emphasis added).

50 The court's December 1992 opinion appears to have been entirely overlooked by courts and commentators. Westlaw does not identify any court decision or article that cites the district court's clarification in *WGN IV* of its intent in *WGN III*.

51 *Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n* (*WGN V*), 874 F. Supp. 844, 852-54 (N.D. Ill. 1995).

52 *Id.* at 853.

53 *Id.* at 855.

54 *Id.* at 856.

55 *Id.*

56 *Id.* at 856 n.12.

> "While telecasting on TNT may be considered sponsored telecasting because TNT does receive some revenues from advertising in addition to subscription fees, *see* [*WGN III*], pure subscription or pay-per-view telecasts clearly are not considered sponsored telecasting."[57]

In other words, the district judge cited his prior opinion in *WGN III* not for the proposition that league agreements with TNT fell *outside* the SBA, but for the proposition that telecasting on TNT "may be considered sponsored telecasting because TNT does receive some revenues from advertising. . . ."[58] It is self-evident that the district judge would not have cited to his decision in *WGN III* for the proposition that TNT broadcasts "may be considered sponsored telecasting" if, in that opinion, he had held that they were *not* "sponsored telecasting."

Ultimately, the court in *WGN V* did not have to reach the cable programming issue, because it held that the challenged agreement between the NBA and NBC fell outside the SBA under section 1292. That section removes any exemption from the antitrust laws if the agreement in question contains restrictions on the licensee's right to televise the licensed games.[59] Because the NBA's agreement with NBC contained provisions that meant that "under the plain terms of the contract, no more than 111 games can be televised nationally," section 1292 was held applicable.[60]

The district court went on to hold that for reasons not relevant here, the NBA-NBC agreement violated the antitrust laws. On appeal, the Seventh Circuit upheld the district court's determination that the NBA's agreement with NBC fell outside the SBA under section 1292, but the court reversed the district court's ruling that the agreement violated the antitrust laws and remanded for a new trial.[61] The Seventh Circuit's opinion did not discuss the applicability of the SBA to cable programming. The trial court docket shows that the matter subsequently settled in late 1996, without any ruling on whether TNT's cable programming was, or was not, "sponsored telecasting."[62]

B. The Shaw Litigation (1997-2002)

The plaintiffs in *Shaw v. Dallas Cowboys Football Club Ltd.* were football fans who alleged that an agreement between the NFL and satellite TV provider DirecTV that allowed DirecTV to market a "Sunday Ticket" games package violated the antitrust laws.[63] The defendants moved to dismiss the complaint on the principal ground that the SBA exempted the alleged conduct from the antitrust laws. The district court disagreed and held

---

57 *Id.*

58 *Id.*

59 *Id.* at 856.

60 *Id.*

61 *Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n (WGN VI)*, 95 F.3d 593, 596-600 (7th Cir. 1996).

62 *See Chicago Prof'l Sports Ltd. P'ship v. Nat'l Basketball Ass'n*, No.1:90-cv-06247 (N.D. Ill. Dec. 19, 1996), ECF No. 691-92 (Stipulation and Agreed Order of Dismissal; Minute Order Dismissing With Prejudice).

63 *See Shaw, et al. v. Dallas Cowboys Football Club Ltd.* (*Shaw I*), No. CIV.A. 97–5184, 1998 WL 419765, at *1-2 (E.D. Pa. June 23, 1998).

that DirecTV's "Sunday Ticket" package did not result from a league transfer of "all or any part of the rights of . . . member clubs in the sponsored telecasting" of football games. [64]

The court began its analysis by defining the word "sponsor," as used in the phrase "sponsored telecasting," as "[o]ne that finances a project or event carried out by another person or group, especially a business enterprise that pays for radio or television programming in return for advertising time."[65] The court held that "[o]nly telecasting which is performed with such a sponsor can meet the meaning of the phrase 'rights . . . in the sponsored telecasting.'"[66] After reviewing the legislative history of the SBA and the district court's decision in *WGN III*, the court held that "satellite broadcasting" of NFL games by DirecTV, which charged subscribers $139 per season to view a package of commercial-free games, did not involve "sponsored telecasting."[67]

The district court certified its decision in *Shaw I* for interlocutory review, and the Third Circuit affirmed.[68] The Court of Appeals began by stating that the "purpose [of the SBA] was to preserve the availability of NFL games on free broadcast television."[69] The court's principal authority for that proposition was a statement in the 1961 Senate Report that had expressed the committee's concern for "the public interest in viewing professional league sports."[70] The cited report did not, however, refer to "free" television and did not suggest that the SBA's scope was limited to over-the-air network programming.[71]

The Third Circuit then stated its agreement with the district court's definition of "sponsored telecasting,"[72] although the Court of Appeals, *sub silentio*, added a significant gloss to that definition. The district court, as noted above, had defined "sponsored telecasting" as telecasting that is sponsored by someone other than the telecaster, "especially" a "business enterprise that pays for radio or television programming in return for advertising time." The Court of Appeals repeated this language, but *added* that the telecasts in question "are therefore provided free to the general public."[73]

---

64 *Id.* at *4-5.

65 *Id.* at *3 (quoting THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 17411 (3rd Ed. 1992)).

66 *Id.*

67 *Id.* at *4. The court noted in *dicta* (and incorrectly) that the district court in *WGN III* had "held that TNT was more like subscription television than like sponsored telecasting, and so a contract with TNT was not exempt . . . ." *Id.* (citing *WGN III*, 808 F. Supp. at 649-50). A review of the briefing in connection with *Shaw I* (available in the docket folder on Westlaw) reveals that none of the parties had alerted the *Shaw* court to the December 1992 opinion in *WGN IV* in which the district court clarified that no such holding had been intended or made.

68 *Shaw v. Dallas Cowboys Football Club, Ltd.* (*Shaw II*), 172 F.3d 299, 302-03 (3d Cir. 1999).

69 *Id.* at 301 and n.7.

70 *Id.* at 301 n.7.

71 *See* 1961 Senate Report, 1961 U.S.C.C.A.N. at 3042, 3044.

72 *Shaw I*, 1998 WL 419765 at *3.

73 *Shaw II*, 172 F.3d at 301. *See also id.* at 301 n.9 (referring to a "sponsored telecast" as one "transmit[ted] in a form freely receivable by the public").

Some commentators have cited the Third Circuit's opinion as holding that league agreements with cable programmers are not exempt from the antitrust laws under the SBA because they supposedly do not involve "free" telecasting.[74] The better view, and the view that the district court on remand adopted, is that any statements by the Third Circuit in *Shaw II* that went beyond DirecTV's satellite transmissions were merely *dicta*.[75]

It is important in this regard to remember that the defendants in *Shaw* had *not* contended that the satellite programming they delivered to consumers (which did not have advertisements) was, itself, "sponsored telecasting," but had instead argued that the SBA applied to the DirecTV package because the NFL games in the package had *previously* been broadcast with commercial interruptions.[76] The district court and the Third Circuit therefore had no reason to address, and made no precedential holdings regarding, the applicability of the SBA to live sports programming on basic cable channels, where sponsors and their advertisements are ubiquitous.

The district court in *Shaw* acknowledged these limitations on remand. In the process of approving the parties' eventual settlement of the class action, the court addressed the question of whether previous opinions in the case had involved the application of the SBA to cable programming. The court reached this issue because the parties had included in the settlement agreement a class-wide release of all claims regarding the transmission of NFL games "whether by broadcast, television, cable television, satellite television, the Internet or any form of technology . . . ."[77] The court held that the proposed release was overbroad. The court reasoned that:

> (1) plaintiffs' complaint "does not suggest that they have asserted any claims with respect to NFL programming by broadcast, cable television, or the Internet," and (2) "although defendants appealed the district court's denial of their motion to dismiss, *the Third Circuit's ruling did not address whether broadcasting the games on the Internet or cable television was an exempt activity under the SBA, but only found that satellite broadcasts of NFL games were not exempted*."[78] In other words, those commentators who have described the Third Circuit's opinion in *Shaw II* as holding anything about cable programming are simply wrong, as the district court responsible for implementing the Court of Appeals' mandate had squarely held.

C. The *Kingray* Litigation (2000-2002)

The only other case that has been cited as rendering a ruling on whether the SBA applies to cable programming is *Kingray, Inc. v. National Basketball Association, Inc.*[79] The plaintiffs in that case asserted antitrust claims against DirecTV and the NBA in connection

---

74 *See, e.g.,* Paolino, *supra* note 33, at 11.

75 *See In re Friedman's Inc.*, 738 F.3d 547, 552 (3d Cir. 2013) ("If a determination by our Court is not necessary to our ultimate holding, 'it properly is classified as *dictum*.' It is well established that 'we are not bound by our Court's prior *dicta*.'") (citation omitted).

76 *Shaw I*, 1998 WL 419765 at *2.

77 *Schwartz v. Dallas Cowboys Football Club, Ltd.*, 157 F. Supp. 2d 561, 575-78 (E.D. Pa. 2001).

78 *Id.* at 577 (emphasis added).

79 188 F. Supp. 2d 1177, 1182 (S.D. Cal. 2002).

with the NBA's agreement that DirecTV could offer a "bundled package of" NBA games to purchasers of the "NBA League Pass." The plaintiffs had alleged in their First Amended Complaint that the DirecTV-NBA agreement did not fall under the SBA because "sponsored telecasting" under the SBA "pertains only to network broadcast television and does not apply to non-exempt channels of distribution such as cable television, pay-per-view, and satellite television networks."[80]

The district court in *Kingray* never reached the SBA issues that had been flagged in the Complaint. Instead, the court dismissed the First Amended Complaint, without leave to amend, on the ground that the plaintiffs were indirect purchasers who did not have standing to pursue their federal antitrust claims.[81] Nevertheless, one district judge has relied on the above-quoted passage from *Kingray* to support its statement (in *dicta*) that the SBA was "inapplicable" to telecasts by Comcast of NHL and MLB games.[82] It appears that the court in *Laumann* did not realize that the court in *Kingray* had merely been reciting plaintiffs' allegations.[83]

With the possible exception of the *Laumann* court's misunderstanding of the *Kingray* opinion, the author has not located any judicial decision since 2002 that addressed the applicability of the SBA to cable programming. That leads us, finally, to an effort to apply principles of statutory interpretation to the phrase "sponsored telecasting" as used in the SBA.

IV. A TRADITIONAL APPROACH TO STATUTORY INTERPRETATION LEADS TO THE CONCLUSION THAT CABLE PROGRAMMING IS "SPONSORED TELECASTING" UNDER THE SBA

If the issue addressed in this article is, in fact, unsettled and unfettered by precedent, we then face the question: is today's basic cable programming of professional sports "sponsored telecasting" under the SBA? To reach the answer, we review the current approach to statutory interpretation and then apply that approach to the relevant language in the SBA.

---

80 *Id.* at 1183 (quoting ¶ 43 of the First Amended Complaint). *See* First Amended Complaint, *Danray, Inc. v. Nat'l Basketball Ass'n, Inc.*, Case No. 00CV1545 (S.D. Cal. July 16, 2001), ECF No. 145, ¶ 43.

81 *Kingray*, 188 F. Supp. 2d at 1182.

82 *See Laumann v. Nat'l Hockey League*, 907 F. Supp. 2d 465, 489, and 489 n.141 (S.D.N.Y. 2012) (denying motion to dismiss antitrust claims).

83 The SBA issues were not even before the court in *Laumann* because the defendants in that case had not, in their motion to dismiss, asserted an SBA defense. *See* Plaintiffs' Memorandum of Law in Opposition to Defendants' Motions to Dismiss the Complaints, Case No. 12-cv-1817 (S.D.N.Y. Sept. 5, 2012), ECF No. 80, at 30 n.39 ("Defendants in this case do not assert the SBA as a defense to Plaintiffs' allegations.").

A. If the Statutory Text Is Unambiguous, Judicial Inquiry Ceases

It is now settled that if the text of a statute is unambiguous, the judiciary's role is to apply the statutory provision without further analysis or debate. [84]

These principles apply even if, as here, the statute in question provides exemptions to the antitrust laws and thus should be narrowly construed. As the district court observed in *Northland Cranberries, Inc. v. Ocean Spray Cranberries, Inc.* , the courts "have repeatedly rejected proposed narrow interpretations of statutory exemptions from the antitrust laws where those interpretations are inconsistent with the plain language of the statute."[85] In *Northland Cranberries*, the court rejected an argument that a statutory reference to "persons engaged in the production of agricultural products" should be construed to refer only to "American persons" engaged in such activities.[86] The court held that the term "persons" was "plain and unambiguous" and that the text of the statute neither "stated or implied" any limitation on the ordinary meaning of the word.[87]

To determine the plain meaning of words used in a statute, courts routinely begin by consulting dictionaries published at around the time that the statute was enacted.[88] Where the language used in a statute involves technical terms or terms reflecting business practices, the courts can turn to specialized dictionaries.[89]

No court has yet undertaken this inquiry, and none of the opinions described in this article discussed any contemporaneous dictionary definitions of "sponsored," "telecasting" or "sponsored telecasting." We undertake that inquiry below.

---

84 *See City of Arlington, Texas v. F.C.C*, 133 S. Ct. 1863, 1868 (2013) ("If the intent of Congress is clear, that is the end of the matter; for the court . . . must give effect to the unambiguously expressed intent of Congress"). *See also Kloeckner v. Solis*, 133 S. Ct. 596, 607 n.4 (2012) ("[E]ven the most formidable argument concerning the statute's purposes could not overcome the clarity [of] the statute's text."); *Exxon Mobil Corp. v. Allapattah Servs., Inc.*, 545 U.S. 546, 568 (2005) ("As we have repeatedly held, the authoritative statement is the statutory text, not the legislative history or any other extrinsic material"); *Microsoft Corp. v. Comm'r of Internal Revenue*, 311 F.3d 1178, 1186 (9th Cir. 2002) ("When the plain language of a statute is clear, we need look no further to divine its meaning.").

85 382 F. Supp. 2d 221, 226 (D. Mass. 2004).

86 *Id.* at 224-25.

87 *Id. See also United States v. Tucor Int'l, Inc.*, 189 F.3d 834, 837 (9th Cir. 1999) (rejecting an argument that an antitrust exemption covering "common carriers" should be limited to "ocean common carriers"); *Int'l Raw Materials, Ltd. v. Stauffer Chem. Co.*, 978 F.2d 1318, 1319 (3d Cir. 1992) (rejecting an argument that an antitrust exemption for "associations" should be construed as referring only to associations of American-owned firms).

88 *See, e.g., Cook Cnty., Illinois v. United States ex rel. Chandler*, 538 U.S. 119, 125-26 (2003) (consulting law dictionaries published in 1856 and 1859 to interpret a statute adopted in 1863); *Microsoft Corp.*, 311 F.3d at 1183 (relying on "[d]ictionary definitions contemporary to the original enactment" of the statute in question).

89 *See* Jason Weinstein, *Against Dictionaries: Using Analogical Reasoning to Achieve a More Restrained Textualism,* 38 U. MICH. J.L. REFORM 649, 654 (2005) (noting that between 1994 and 2002, the Supreme Court "[u]sually . . . use[d] a specialized dictionary to define technical terms").

B. The Meaning of "Sponsored Telecasting," As Used In 1961, Is Clear

If a professional football, baseball, basketball or hockey league transfers its clubs' rights in the "sponsored telecasting of [the club's] games," the parties' agreement is exempt from the antitrust laws under the SBA.[90] Pursuant to the principles of statutory interpretation described above, we begin by reviewing dictionaries, including technical dictionaries, to determine the contemporaneous meaning of the phrase "sponsored telecasting." Fortunately, we do not have to look far, for in 1961, the same year in which the SBA was enacted, Prof. Howard Jacobson published "A Mass Communications Dictionary." Jacobson described his dictionary as "a reference work of common terminologies for press, print, broadcast, film, advertising and communications research."[91]

Jacobson's dictionary included definitions for "telecast" and "sponsor," as set out below:

> "Sponsor—Advertisers who use TV and/or radio to inform and sell their individual products and services to the public."
>
> "Telecast—A broadcast, program or show on television";[92]

In light of these definitions, it is apparent that "sponsored telecasting," when used in 1961 in the mass communications and advertising arena, referred to television broadcasts that included advertisements for individual products or services.[93] That description easily fits today's sports programming on basic cable, where paid advertising is ubiquitous. As a result, the courts should hold, if the issue arises, that the SBA exempts from antitrust scrutiny those league agreements that involve basic cable programming.

Because the meaning of "sponsored telecasting" as used in 1961 is clear, a court should render its ruling without diving into legislative history. As the Supreme Court has repeatedly held, the "authoritative statement is the statutory text, not the legislative history or any other extrinsic material."[94] Moreover, even if a court were to find "sponsored telecasting" to be ambiguous, the legislative history of the SBA does not contain any basis for adopting a more restrictive definition, as discussed below.

---

90 15 U.S.C. § 1291.

91 Jacobson, A Mass Communications Dictionary (1961) (title page). *See also id.* at viii (noting that the dictionary's editors had "gathered up the current working terminologies in most phases of mass communication").

92 *Id.* at 320, 338.

93 The 1992 general dictionary that the district court in *Shaw I* relied upon contained a similar definition of "sponsor": "one that finances a project or event carried out by another person or group, especially a business enterprise that pays for radio or television programming in return for advertising time." *Shaw I*, 1998 WL419765, at *3 (E.D. Pa. June 23, 1998) (quoting The American Heritage Dictionary of the English Language 17211 (3rd Ed. 1992)). The court in *U.S. v. NFL I* similarly defined "'live' telecasts" as "telecasts made simultaneously with the playing of the game as contrasted with movies of the game telecast subsequent to the playing of the game." *U.S. v. NFL I*, 116 F. Supp. 319, 321 n.4 (E.D. Pa. 1953). This definition provides additional evidence that the word "telecasting" in the 1950s applied to any program viewed on a television.

94 *Exxon Mobil Corp. v. Allapattah Servs. Inc.*, 545 U.S. 546, 568 (2005). *See also Microsoft Corp.*, 311 F.3d at 1186 ("When the plain language of a statute is clear, we need look no further to divine its meaning.").

C. Even If a Court Were to Consider "Sponsored Telecasting" to Be Ambiguous, an Analysis of the Statute's Purpose And Legislative History Would Still Lead to the Conclusion that Today's Basic Cable Programming Should Be Considered "Sponsored Telecasting"

1. Introduction

As noted in Section II(A) of this article, the SBA was enacted in large part in response to a district court's ruling in 1961 that the NFL's sale of a games package to CBS violated the antitrust laws. Congress acted quite quickly: the SBA was passed by both houses, *and* signed into law by President Kennedy, only sixty-three days after the district court's ruling.[95]

The House Report that accompanied the bill in question stated that its purpose "is to enable the member clubs of a professional football, baseball, basketball, or hockey league to pool their separate rights in the sponsored telecasting of their games and to permit the league to sell the resulting package of pooled rights to a purchaser, such as a television network, without violating the antitrust laws."[96] The chair of the House Judiciary Committee (and sponsor of the bill), Rep. Cellar, similarly informed the House that the antitrust exemption provided by the SBA allows the sale of pooled rights "to a television network *or other purchaser.*"[97] The Senate Report also contains broad language.[98] This phrasing strongly suggests that Congress had in mind purchasers other than over-the-air television networks, and that such networks were identified as an *example* of "sponsored telecasting," not as the only possible beneficiary of the exemption provided by the SBA.

Congress did not, in 1961, provide any specific definition of "sponsored telecasting." The legislative history does, however, contain suggestions about what is *not* "sponsored telecasting." The bill's sponsor, Rep. Cellar, stated that the SBA "applies only to sales of rights in sponsored telecasting; it does not apply to closed circuit or subscription television."[99] The House Report contains the same language.[100] As discussed below, those two types of programming—as they existed in 1961—were substantially different from today's basic cable programming.

---

95 1961 Cong. Rec. 21552 (Sept. 30, 1961).

96 *See* H.R. Rep. No. 1178 at 2 (Sept. 13, 1961).

97 107 Cong. Rec. 20059 (Sept. 18, 1961) (emphasis added).

98 *See* S. Rep. No. 1087, 87th Cong., 1st Sess., reprinted in 1961 U.S.C.C.A.N. at 3042, 3044 (stating that the public interest would be served "by exempting joint agreements under which a league sells or transfers pooled television rights of its members to a purchaser") [hereinafter S. Rep. No. 1087].

99 107 Cong. Rec. 20060 (Sept. 18, 1961).

100 *See* H.R. Report No. 1178 at 5 (Sept. 13, 1961) ("The bill does not apply to closed circuit or subscription television.").

2. Today's Basic Cable Programming Is Substantially Distinguishable From the "Closed Circuit" and "Subscription Television" Programming That Congress Pointed to as Not Covered by The SBA

a. "Subscription Television" In the 1950s and Early 1960s

According to industry historians, the 1950s and early 1960s saw the development and testing of "a form of television known variously as 'pay-television,' 'subscription television,' or 'toll television.'"[101] These terms "referred to forms of television supported by direct viewer payments, not advertising," and "were the precursors to today's *premium* cable channels . . . ."[102]

According to Mullen, the "pay television industry, which had experienced technical, regulatory and economic fits and starts throughout the 1950's, made another series of appearances during the early 1960's."[103] The FCC gave temporary approval to pay television in March 1959, and "three major system tests" then took place.[104] In 1960, International Telemeter launched a test system in a Toronto suburb of a wired pay-for-view service that customers accessed by feeding coins into a box that was wired to their television.[105] The service offered movies, sports, and other programming on a pay-per-program basis.[106] The test shut down in 1965.[107]

Zenith launched a similar test of its Phonevision service in Hartford, Connecticut in 1962. As with International Telemeter, the Phonevision service was activated by inserting coins into the customer's decoder device, on a per-program basis.[108] The 1962 test in Hartford involved a UHF station that broadcast commercial off-the-air programs during the day but switched to encrypted Phonevision pay-per-view programming in the evening.[109] Subscription figures "never attained levels sufficient to justify costs, however," and Zenith eventually abandoned the test.[110] The third test launch was Subscription Television, Inc. ("STV"), which had been developed in the 1950s by Skiatron Television and Electronics Corporation. Mullen at 52. STV, which had a programming mix similar to the two systems described above, was operational in San Francisco and Los Angeles for four months in 1964.[111] Although STV's schedule included exclusive game coverage of the San Francisco Giants and the recently relocated Los Angeles Dodgers, the test was deemed unsuccessful.[112]

---

101 Megan Mullen, Television in the Multichannel Age 52 (2008).

102 *Id.* (emphasis added) (referencing HBO, Showtime and other pay channels).

103 *Id.* at 75.

104 *Id.*

105 *Id.* at 75-76.

106 *Id.*

107 *Id.*

108 *Id.*

109 *Id.*

110 Patrick R. Parsons, Blue Skies: A History of Cable Television at 112 (2008).

111 *Id.* at 76-77.

112 *Id.*

b. "Closed Circuit Television" in the 1950s and Early 1960s

According to the Museum of Broadcast Communications, "Closed Circuit Television" is a "transmission system in which live or prerecorded signals are sent over a closed loop to a finite and predetermined group of receivers. . . ."[113] In the 1950s and 1960s, boxing promoters used Closed Circuit Television to show boxing matches in movie theaters, which became a "lucrative source of ancillary revenue" for those promoters.[114] Efforts to put NFL games on closed circuit television continued as late as 1977, when the founder of Subscription Television, Inc., Bill Sargent, formed a closed-circuit provider called Special Event Entertainment and offered the NFL $400 million to show playoff games, including the Super Bowl, through a national closed-circuit network.[115] According to the *Times*, Sargent's bid "topped the money offered by the commercial television networks but would have forced fans to pay for a seat at a movie theater to watch the games. . . . It did not happen."[116]

It is clear from the above descriptions that the "Closed Circuit" and "Subscription Television" offerings that Congress was concerned about in 1961 are readily distinguishable from today's basic cable programming. The former offerings involved the transmission of a single, commercial-free program to a consumer in exchange for payment for that program and represented, according to an industry historian, "the precursors to today's premium cable channels," such as HBO and Showtime.[117] Today's basic cable, on the other hand, involves the transmission to consumers of hundreds of channels of programming (many of which are available 24/7) that cover a full spectrum of interests and that contain a substantial amount of commercial advertising, all for a single monthly fee. In other words, the statement in the House Report that the SBA "does not apply to closed circuit or subscription television" provides no basis for a conclusion that "sponsored telecasting," as used in the SBA, does not include today's basic cable programming.[118]

---

113 Encyclopedia of Television, "Closed Circuit Television," found at *http://www.museum.tv/encyclopedia.htm (last visited Sept. 18, 2016).*

114 *Id.*

115 Wolfgang Saxon, *Bill Sargent, 76, A Pioneer in Closed-Circuit and Pay TV*, N.Y. Times, Oct. 31, 2003, http://www.nytimes.com/2003/10/31/arts/bill-sargent-76-a-pioneer-in-closed-circuit-and-pay-tv.html?_r=0.

116 *Id.*

117 Mullen, Television in the Multichannel Age 52 (2008).

118 Some commentators who argue that the SBA applies only to over-the-air broadcasts of professional sporting events point to an exchange during the 1961 Congressional hearing between House Judiciary Committee Counsel Herbert Malete and NFL Commissioner Pete Rozelle. Malete asked Rozelle if he understood "that this bill covers only the free telecasting of professional sports contests, and does not cover pay TV?" Mr. Rozelle answered "Absolutely." 8/8/61 H'rg Tr. at 36. It is not clear from this exchange if Mr. Rozelle was focused on the word "free" in counsel's question or was thinking of the types of "pay television" that were prevalent at the time. In any event, under modern principles of statutory interpretation, this exchange between committee counsel and a witness cannot be relied upon to alter the language that Congress chose to use in the SBA ("sponsored telecasting") by inserting different language ("free telecasting"). *See generally Laborers' Local 265 Pension Fund v. iShares Trust*, 769 F.3d 399, 405 (6th Cir. 2014) (observing that oral testimony by individual witnesses at committee hearings "is typically accorded little weight"); *Public Citizen v. Farm Credit Admin.*, 938 F.2d 290, 292 (D.C. Cir. 1991) (*per curiam*) (noting that the "testimony of witnesses before congressional committees prior to passage of legislation is generally weak evidence of legislative intent").

3. The Stated Purposes of the SBA Would Be Best Fulfilled by Applying It to Cable Programming

If the phrase "sponsored telecasting" were ambiguous, and *if* the Court were to consider Congress' overall statutory purpose in deciding how to define that phrase, the outcome remains clear. Congress' purpose in enacting the SBA was two-fold: (1) to protect the "public interest in viewing professional league sports"[119]; and (2) to "permit professional sports leagues to deal jointly in the sale of their TV rights and, by grouping their weaker and stronger clubs and those clubs with greater or lesser home territory population, to provide equal access to television facilities and television income for all member clubs of their league."[120] Because the percentage of U.S. households who access only over-the-air network broadcasts is around 17%, while basic cable programming is available to the substantial majority of U.S. households,[121] it is obvious that the SBA's purposes would *not* be served if the SBA applied only to over-the-air broadcasts and would instead be best served by including *both* over-the-air and basic cable programming within the definition of "sponsored telecasting."[122]

V. CONCLUSION

It may be surprising that in the 55 years since the enactment of the Sports Broadcasting Act, no court has ever definitively ruled that agreements between professional sports leagues and basic cable programmers are, or are not, protected by the antitrust exemptions set out in the Act. But as set out in this article, the green is indeed open, and the fact is that the operative language that Congress chose to use to trigger the statutory exemptions ("sponsored telecasting"), when examined through the statutory interpretation lens that courts use today, quite clearly includes basic cable programming, whose "telecasts" of professional sporting events are "sponsored," as those terms were used in 1961.

---

119 S. Rep. No. 1087, 1961 U.S.C.C.A.N. at 3044.

120 *Id.* (statement by Sen. Hruska).

121 *See* Deborah D. McAdams, "Survey: 17 Percent of U.S. Households Are OTA-Only," available at www.TVTechnology.com/news/0002/17-percent-of-us-households-are-otaonly/278987 (last visited Sept. 18, 2016).

122 *See generally King v. Burwell*, 135 S. Ct. 2480, 2489 (2015) (holding that where the text of a statute appears to be ambiguous, the courts should look to "the remainder of the statutory scheme" because it "often" reveals that "only one of the permissible meanings produces a substantive effect that is compatible with the rest of the law") (quoting *United Sav. Assn. of Tex. v. Timbers of Inwood Forest Associates, Ltd.*, 484 U.S. 365, 371 (1988)).

NEVER SAY NEVER: THE NINTH CIRCUIT'S MISGUIDED CATEGORICAL APPROACH TO INDIVIDUAL DAMAGES QUESTIONS WHEN ASSESSING RULE 23(B)(3) PREDOMINANCE

By John M. Landry[1]

I. INTRODUCTION

To qualify for class treatment under Federal Rule of Civil Procedure 23(b)(3), damages (or restitution) claims must present common questions that "predominate over any questions affecting only individual class members."[2] Yet, calculating each class member's damages inherently entails some degree of individual inquiry and proof. As a result, what role individual damages questions should properly play in a predominance inquiry is a source of controversy.

When questions concerning liability are entirely common, however, various courts of appeals accept that individual damages questions do not predominate. But these courts express this rule as a general—not categorical—one, recognizing that, in certain instances, individual damages questions can reach a level of magnitude and complexity sufficient to overwhelm common questions.

Like other circuit courts, the Ninth Circuit initially adopted what appeared to be the general rule. In *Blackie v. Barrack,*[3] a Ninth Circuit panel stated that the "amount of damages is invariably an individual question and does not defeat class action treatment."[4] The panel then went on to consider the nature of the damages proof in that case. It supported its affirmance of the district court's class certification order by observing that computing damages for each class member would be "virtually a mechanical task."[5]

But, in a series of recent panel decisions, the Ninth Circuit has now unmistakably rejected any rule other than an absolute, categorical one: individual damages questions alone never, *ever* defeat class certification.[6] Hence, once a district court perceives liability as posing entirely common questions, its predominance inquiry ends there, and individual damages questions, whatever their nature or complexity, become instantly irrelevant. Although these panel opinions purport to adhere to earlier circuit precedent, their strict, categorical approach arguably constitutes a change in Ninth Circuit law. Certainly, if it is a change, it is a nontrivial one because when applied the rule truncates the district court's Rule 23(b)(3) predominance analysis. And its application is likely to be frequent given, for example, the number of California false advertising cases litigated under California's

---

1 John M. Landry is a special counsel in the Los Angeles office of Shepard Mullin Richter & Hampton LLP. A member of the firm's Business Trial Practice Group, Mr. Landry practices in a broad spectrum of subject areas with emphasis on class action defense, antitrust, and securities litigation. This article reflects his views alone.

2 Fed. R. Civ. P. 23(b)(3).

3 *Blackie v. Barrack,* 524 F.2d 891 (9th Cir. 1975).

4 *Id.* at 905.

5 *Id.*

6 *See, e.g., Pulaski & Middleman, LLC v. Google Inc.,* 802 F.3d 979, 987-88 (9th Cir. 2015), *cert. denied,* 136 S. Ct. 2410 (2016).

Unfair Competition Law ("UCL") in the Ninth Circuit, cases the Ninth Circuit insists present no individualized liability determinations and so would automatically qualify for categorical treatment.

The Ninth Circuit's "categorical rule" that never permits individual damages questions alone to defeat class certification is a misstep. First, the rule's seeming departure from previous panel precedent suggests a violation of intra-circuit *stare decisis*. Second, the rule conflicts with the U.S. Supreme Court's decision in *Comcast Corp. v. Behrend*,[7] which rests on the notion that individual damages *may* overwhelm common liability questions and defeat class certification. Indeed, the Ninth Circuit's own reading of *Comcast, i.e.,* that a plaintiff show its damages method matches the liability case, makes no sense as a Rule 23 predominance requirement when applied in cases where the categorical rule also applies because the categorical rule, by definition, would obviate the need for any further predominance showing. Lastly, the Ninth Circuit's categorical approach, by ignoring damages issues altogether, effectively certifies issue-only, liability classes under Federal Rule of Civil Procedure 23(c)(4) without addressing whether a liability-only class actually advances the lawsuit's disposition.

This article discusses Rule 23(b)(3)'s predominance requirement, the general rule on the effect of individual damages questions on predominance, the Ninth Circuit's initial approach, and the genesis of the Ninth Circuit's present categorical rule. It then explains why the categorical rule should be abandoned.

II. RULE 23(B)(3)'S PREDOMINANCE REQUIREMENT

Plaintiffs purporting to assert monetary claims (damages or restitution) on behalf of a consumer or other purchaser class in federal court must proceed via Rule 23(b)(3). Unlike traditional class actions authorized under Rule 23(b)(1) or (b)(2), in which claimants tap the same limited fund or secure indivisible injunctive relief, Rule 23(b)(3) aggregates claims seeking divisible, individualized amounts of money.[8] The justification for this is judicial economy, provided judicial economy is even achievable due to some cohesiveness present. The test for cohesiveness finds expression in Rule 23(b)(3)'s predominance element which asks whether "questions of law or fact common to the class predominate over any questions affecting only individual members."[9] Only if the answer is yes can aggregation yield the desired efficiencies.

The predominance test is hard to pin down as the term "predominate" is imprecise. The Supreme Court's recent statement that common questions predominate when they are "more prevalent or important," lends no greater precision.[10] Moreover, although Rule 23(b)(3) itself makes no distinction between questions going to liability versus those

---

7 133 S. Ct. 1426 (2013).

8 As the U.S. Supreme Court has confirmed, "individualized monetary claims belong in Rule 23(b)(3)." *Wal-Mart Stores, Inc. v. Dukes,* 131 S. Ct. 2541, 2558 (2011).

9 Fed. R. Civ. P. 23(b)(3). In addition, subdivision (b)(3) requires that class treatment be superior to other available adjudication methods.

10 *See Tyson Foods, Inc. v. Bouaphakeo,* 136 S. Ct. 1036, 1045 (2016). The Ninth Circuit has used similar language. *See Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1022 (9th Cir. 1998) (stating predominance exists "[w]hen common questions present a significant aspect of the case") (internal quotation marks omitted).

going to damages, courts tend to treat liability-related questions as more important and thus more determinative of predominance. This is observable, for example, in antitrust cases where predominance largely turns on whether there is class-wide proof of "fact of injury" (or impact), an element of the claim itself.[11] Hence, in cases where liability questions will, to some degree, vary by individual class member, common-question predominance is less likely. In such cases, individual damages questions are relevant in determining if individual questions (either liability or damages) predominate.[12] But when liability questions are entirely common, the question is whether individual damages questions *alone* may predominate.

III. INDIVIDUAL DAMAGES QUESTIONS AND PREDOMINANCE

Awarding damages to class members invariably requires some degree of individualized proof. As Professor Rubenstein points out, "[i]n most any damage class action, each class member is likely to be entitled to a specific amount of damages pertinent to the harm she suffered."[13] He offers securities class actions as an example where "each shareholder's damage will depend on the quantity of shares that she owned." Indeed, from the outset, it was recognized that the mere need for individual damages determinations should not automatically bar Rule 23(b)(3) class certification. The advisory committee to Rule 23 used this example:

> The court is required to find . . . that the questions common to the class predominate over the questions affecting individual members . . . . In this view, a fraud perpetrated on numerous persons by the use of similar misrepresentations may be an appealing situation for a class action, and it *may* remain so despite the need, if liability is found, for separate determination of the damages suffered by individuals within the class.[14]

As the advisory committee's note indicates, individual damages questions may—or may not—predominate over common liability questions. But, when liability questions are entirely common, a rule has developed. Simply stated, individual damages questions do not preclude class certification. This rule, however, is widely understood to be only a general rule, not a categorical one, and various circuit courts have expressed it in distinctly non-categorical terms.[15]

---

11 *See* 8 Julian O. von Kalinowski, et al., Antitrust Laws and Trade Regulation § 166.03[3][a][i] (2d ed. 1997).

12 *See Klay v. Humana, Inc.,* 382 F.3d 1241, 1260 (11th Cir. 2004) ("It is primarily when . . . significant individualized questions going to liability exist that the need for individualized assessments of damages is enough to preclude 23(b)(3) certification.").

13 2 William B. Rubenstein, Newberg on Class Actions § 4.54 (5th ed. 2015).

14 Fed. R. Civ. P. 23 advisory committee's note to 1966 amendment (emphasis added).

15 *See, e.g., In re Visa Check/MasterMoney Antitrust Litig.,* 280 F.3d 124, 139 (2d Cir. 2001) ("Common issues *may* predominate when liability can be determined on a class-wide basis, even when there are some individualized damage issues.") (emphasis added); *Tardiff v. Knox County,* 365 F.3d 1, 6 (1st Cir. 2004) (stating "the need for individualized damage decisions does not *ordinarily* defeat predominance where there are still disputed common issues as to liability") (emphasis added).

The First Circuit, in *Smilow v. Southwest Bell Mobile Systems, Inc.*,[16] after surveying the various circuits, observed: "Where, as here, common questions predominate regarding liability, the courts *generally* find the predominance requirement to be satisfied even if individual damages remain."[17] Likewise, the leading treatise on class actions summarizes the law as follows: "individual damage calculations *generally* do not defeat a finding that common issues predominate."[18] Some courts of appeals state this same rule by recognizing that individual damages questions may, even if only infrequently, predominate over common liability questions.[19] Cases from the Third, Fourth, Fifth, and Eleventh Circuits, provide actual examples of individual damages questions alone predominating over common liability questions.[20]

Several observations are possible from the case law. Individual damages questions are most likely to predominate when calculations are particularly non-formulaic or "labyrinthine."[21] Such calculations may defeat predominance unless a proposed class-wide method—some database, formula or expert's model—overcomes the complexity or dissimilitude, rendering the computations a less individualized or more mechanical task. For example, the Fifth Circuit has recognized that "[c]lass treatment . . . may not be suitable where the calculation of damages is not susceptible to a mathematical or formulaic calculation, or where the formula by which the parties propose to calculate individual damages is clearly inadequate."[22] Absent a satisfactory class-wide method, the concern is that individual damages will require "separate mini-trials" and thereby overwhelm any common questions.

Although individual damages decisions alone rarely defeat class certification, the general, non-categorical nature of the rule remains and shapes the scope of a district court's Rule 23(b)(3) inquiry. Hence, even when liability issues are common, a general,

---

16 323 F.3d 32 (1st Cir. 2003).

17 *Id.* at 40.

18 Rubenstein, *supra* note 11.

19 *See Wallace B. Roderick Revocable Living Trust v. XTO Energy, Inc.,* 725 F.3d 1213, 1220 (10th Cir. 2013) (stating "although individualized monetary claims belong in Rule 23(b)(3), predominance may be destroyed if individualized [damages] issues will overwhelm those questions common to the class") (internal citations and quotation marks omitted); *Klay v. Humana, Inc.,* 382 F.3d at 1260 ("Of course, there are also extreme cases in which computation of each individual's damages will be so complex, fact-specific, and difficult that the burden on the court system would be simply intolerable.").

20 *See Chiang v. Veneman,* 385 F.3d 256, 273 (3d Cir. 2004) (denying class certification and stating "there are cases where the question of damages is so central that it can, in some sense, overtake the question of liability"), *abrogated on other grounds by In re Hydrogen Peroxide Antitrust Litig.,* 552 F.3d 305, 318 n.18 (3d Cir. 2008); *Lienhart v. Dryvit Systems, Inc.,* 255 F.3d 138, 149 (4th Cir. 2001) (finding no common questions predominated where damages determinations would require the "functional equivalent of a full-blown trial on damages causation for each putative class member"); *Bell Atl. Corp. v. AT&T Corp.,* 339 F.3d 294, 303-04 (5th Cir. 2003) (affirming denial of certification because "any adequate estimation of actual damages" would require "individualized inquiries" overwhelming common issue); *Little v. T-Mobile USA, Inc.,* 691 F.3d 1302, 1308 (11th Cir. 2012) (affirming district court's ruling that "variation in individual damages render[ed] the class unsuitable for certification on predominance grounds").

21 *See Comcast,* 133 S. Ct. at 1431 (noting that court of appeals below had required that plaintiffs' model "assure [it]" that damages "will not require labyrinthine individual calculations.").

22 *Bell Atl.*, 339 F.3d at 307.

non-categorical approach has important practical effects. District courts must still consider all potential individual issues, whether liability or damages, and understand the nature of the damages proof. Plaintiffs, even when a district court is likely to view liability issues as entirely common, must disclose how they intend to prove each class member's damages, frequently by submitting an expert's proposed formula or model to advance a more simplified, class-wide approach.

IV. THE NINTH CIRCUIT'S INITIAL, NON-CATEGORICAL APPROACH

The Ninth Circuit's approach to individual damages questions appears to have begun with a non-categorical rule that, like that articulated in other circuits, did not invariably find the requisite predominance whenever liability presented only common questions.

A. *Blackie v. Barrack*

The Ninth Circuit first addressed the effect, if any, the need for individual damages calculations might have on Rule 23(b)(3)'s predominance element in *Blackie,* a securities fraud case. In affirming the district court's class certification order, the panel endorsed a fraud-on-the-market presumption of individual reliance that allowed for a class-wide liability determination.[23] Defendants, however, contended that individual damages amounts would still vary by class member and so predominate over the common questions. The panel cited to several district court decisions certifying securities fraud cases as Rule 23(b)(3) class actions and stated: "The amount of damages is invariably an individual question and does not defeat class action treatment."[24] The panel then found that, "should the class prevail, the amount of price inflation during the period can be charted and the process of computing individual damages will be virtually a mechanical task."[25] Hence, the court looked but saw no evidence suggesting that computing individual damages would entail more than the normal level of complexity typically encountered in securities fraud cases, given the availability of price-inflation studies.

Blackie, by all indications, established only a general rule that individual damages questions do not defeat class certification. It did not state that individual damages questions could never predominate over common liability questions. In stressing the particular mechanical nature of the securities-fraud damages computations at issue, *Blackie* signaled that the outcome might have been different had those computations presented more complexity.

Two years after *Blackie,* the Ninth Circuit again spoke to the issue of individual damages in another securities fraud case and, relying on *Blackie,* upheld the district court's class certification order "because these damage issues do not, as a rule, defeat class certification in cases *such as these*."[26] Tellingly, other courts of appeal read *Blackie* as

---

23 *Blackie,* 524 F.2d at 906.

24 *Id.* at 905.

25 *Id.*

26 *Arthur Young & Co. v. U.S. Dist. Ct.*, 549 F.2d 686, 696 (9th Cir. 1977) (emphasis added).

positing only a general rule, one that leaves open the possibility that damages questions might predominate in certain instances.[27]

B. *Yokoyama v. Midland National Life Insurance Co.*

Thirty-five years after *Blackie,* a Ninth Circuit panel applied *Blackie* to decide whether individual damages questions defeated class certification in a consumer fraud case. In *Yokoyama v. Midland National Life Insurance Co.,*[28] plaintiffs sued an insurance company claiming it deceptively sold annuity products in violation of Hawaii law. The district court denied plaintiffs' motion to certify a Rule 23(b)(3) class because it believed Hawaii law required proof of each purchaser's subjective reliance. It also ruled that damages would involve "highly individualized and fact specific determinations," explaining:

> the amount of damage sustained by a single class member would depend on factors such as the financial circumstances and objectives of each class member; their ages; the [annuity] selected; any changes in the fixed interest rate for that particular [annuity]; the performance of the selected index; any changes in the index margin for that particular [annuity]; any cap on the indexed interest; the length of the surrender periods; whether the individual had undertaken or wanted to undertake an early withdrawal of funds; any benefit the individual policy holder derived from the form of the annuity itself, including the tax-deferral of credited interest; and the actual rate of return on the [annuity].[29]

The panel reversed because it found the district court plainly erred in applying Hawaii law.[30] The statute imposed an objective not subjective reliance test, obviating the need to examine the circumstances of each annuity's purchase. The panel surmised that the same error likely affected the district court's views on damages, and so doubted that damages would involve anything close to the complex, hyper-individualized analyses the district court had feared.[31] Although individual damages calculations of some sort would need to be made, the panel cited *Blackie* and stated: "In this Circuit, . . . damage calculations alone cannot defeat certification."[32]

Hence, *Yokoyama* purported to follow *Blackie* and articulated the rule in a manner similar to *Blackie,* expressing no departure from *Blackie.* Further, *Yokoyama* undoubtedly viewed *Blackie* as embracing a non-categorical rule similar to that expressed in *Smilow v. Southwest Bell Mobile Systems, Inc.*[33] because *Yokoyama* specifically cited *Smilow* as "in accord" with *Blackie.*[34] As noted above, the First Circuit in *Smilow* recognized a non-

---

27 *See, e.g., Windham v. American Brands, Inc.,* 565 F.2d 59, 67-68 (4th Cir. 1977).

28 594 F.3d 1087 (9th Cir. 2010).

29 *Id.* at 1093-94.

30 *Id.* at 1092.

31 *Id.* at 1094.

32 *Id.*

33 323 F.3d 32, 40 (1st Cir. 2003).

34 *Yokoyama,* 594 F.3d at 1089.

categorical approach, observing merely that courts "have *usually* certified Rule 23(b)(3) classes" when common issues otherwise predominated.[35] *Smilow* did not hold that individual damages questions can never predominate over common liability questions, and that has never been the rule in the First Circuit. Hence, as of *Yokoyama,* the Ninth Circuit, by most indications, took the same general, non-categorical approach to individualized damages questions as other circuits.

V. THE NINTH CIRCUIT'S (NEW) CATEGORICAL RULE

In a series of recent panel decisions, the Ninth Circuit's approach to individual damages questions under Rule 23(b)(3) seems to have suddenly become absolute.

A. *Leyva v. Medline Industries, Inc.*

Any non-categorical approach in the Ninth Circuit abruptly ended beginning with *Leyva v. Medline Indus. Inc.,*[36] a wage-and-hour case. There, the district court denied class certification on the ground that issues regarding "the amount of pay owed" predominated over common liability questions. A Ninth Circuit panel reversed, holding that "damage calculations alone cannot defeat certification."[37] It added: "In deciding otherwise, the district court . . . appl[ied] the wrong legal standard."[38] Later in the opinion, the panel noted that defendant's own time-keeping database would "feasibly and efficiently" permit accurate damages calculations once common liability questions were adjudicated.[39] But it purported to note this to show that damages in the case would measure only the lost wages resulting from the unlawful practices—a Rule 23(b)(3) requirement that *Leyva* believed *Comcast* now imposed, *i.e.,* that damages stem from only those actions that created the liability.

The *Leyva* panel purported to rely on *Yokoyama* despite the fact that the rule *Leyva* applied was categorical. Indeed, under *Leyva,* any district court ruling that individual damages predominate over common liability questions constitutes instant error via the district court's application of "the wrong legal standard."[40] Yet, *Yokoyama* did not necessarily suggest a categorical application, particularly as it cited *Smilow* with approval. Accordingly, a strict, categorical approach is not one that the Ninth Circuit necessarily embraced before *Leyva*.[41]

---

35 *Smilow,* 323 F.3d at 39 (emphasis added).

36 716 F.3d 510 (9th Cir. 2013).

37 *Id.* at 513 (quoting *Yokoyama*, 594 F.3d at 1074).

38 *Id.* at 514.

39 *Id.*

40 *Id.*

41 Shortly after *Leyva,* in *Jimenez v. Allstate Ins. Co.,* 765 F.3d 1161 (9th Cir. 2014), an appeal challenging class certification on due process grounds, a Ninth Circuit panel identified *Leyva* as stating a rule consistent with that in *Yokoyama.* See 765 F.3d at 1167.

B. *Pulaski & Middleman, LLC v. Google, Inc.*

Two years later, in *Pulaski & Middleman, LLC v. Google, Inc. ("Pulaski"),*[42] a Ninth Circuit panel, purporting to apply *Yokoyama,* confirmed that individualized damages (or, here, restitution) calculations *can never* alone defeat Rule 23(b)(3)'s predominance element. Plaintiffs were internet advertisers who had purchased Google's ad-placement service known as AdWords. They alleged Google falsely touted the service, causing plaintiffs to unwittingly pay for advertising placed on less valuable "parked domain and/or error page websites."[43] Plaintiffs alleged they would not have paid for this advertising (or not paid as much) had they known the truth and sought restitution.[44]

The district court denied plaintiffs' class certification motion on the ground that common questions did not predominate. Among other things, it found that Google's use of a non-uniform auction process to sell, price and place ads would cause the calculation of each class members restitution award to require an exceedingly high degree of individualized analysis and proof.[45] Moreover, none of plaintiffs' proposed methods for measuring restitution, even if valid, adequately addressed and reduced the enormous complexity of the task.[46] The district court, interpreting *Yokoyama*'s rule (*i.e.*, damage calculations alone do not defeat class certification) as non-categorical, held that it did not apply in this instance because of the intensely individualized nature of the calculations and the absence of any proposed method to render them sufficiently formulaic.[47]

The Ninth Circuit panel reversed. Without discussion, it treated *Yokoyama* as espousing a categorical rule, one applicable in all cases regardless of the degree of individualized computations required.[48] Thus, it found that the district court erred in concluding the rule in *Yokoyama* did not apply. The panel also rejected Google's argument that the Supreme Court's decision in *Comcast* placed in doubt the use of the categorical rule. The panel, as the panel in *Leyva* had done previously, treated *Comcast* as requiring only that any proposed class damages method align with the case's theory of liability, and declared that "*Yokoyama* [which pre-dated *Comcast*] remains the law of this court, even after *Comcast*."[49]

C. *Vaquero v. Ashley Furniture Industries, Inc.*

Most recently, in *Vaquero v. Ashley Furniture Indus., Inc.,*[50] a putative wage-and-hour-class action, a Ninth Circuit panel upheld a district court's class certification order despite the need for individualized damages calculations. It cited *Blackie, Yokoyama, Leyva,* and

---

42 802 F.3d 979 (9th Cir. 2015).

43 *Id.* at 983.

44 *In re Google Adwords Litig.,* 2012 U.S. Dist. LEXIS 1216, at *26 (N.D. Cal. Jan. 5, 2012).

45 *Id.* at *46.

46 *Id.* at *49.

47 *Id.* at *46 n.13.

48 *Pulaski,* 802 F.3d at 987-88.

49 *Id.* at 988.

50 824 F.3d 1150 (9th Cir. 2016).

Pulaski as all uniformly adhering to the categorical rule that the presence of individual damages cannot, by itself, defeat class certification under Rule 23(b)(3).[51]

VI. THE RECENT PANEL DECISIONS CANNOT BE JUSTIFIED ON INTRA-CIRCUIT *STARE DECISIS* GROUNDS

The categorical rule identified above has arguably emerged in the Ninth Circuit just recently. Moreover, as also demonstrated above, the rule appears to depart from the rule articulated and applied in *Blackie* and in *Yokoyama*—a rule which did not necessarily foreclose the possibility that individual damages questions may, in certain circumstances, overwhelm common liability issues.

If the categorical rule is new, then *Leyva, Pulaski* and *Vaquero's* portrayal of *Blackie* and *Yokoyama* is revisionist. The panels in those more recent cases simply imprinted on to *Blackie* and *Yokoyama* a categorical approach that was not there.[52] This is problematic. One circuit panel cannot alter the rule of another. Changes in intra-circuit precedent require *en banc* review—the normal mechanism by which intra-circuit precedent evolves.[53]

The predominance element at issue here deserved a more-studied, less-revisionist assessment of Ninth Circuit precedents. The categorical rule, once triggered, eliminates any need to examine how a plaintiff intends to prove individualized damages, and so truncates the scope of the district court's Rule 23(b)(3) examination. Any change in law that, as here, reduces the requisite showing of predominance is significant. Nor will it necessarily be difficult or rare for putative consumer class plaintiffs to trigger the categorical rule. For example, *Pulaski* itself, to pave the way for its application of the categorical rule, noted that claims under California's UCL and similar statutes do not require individualized proof to establish liability.[54] Hence, simply by alleging certain claims, a plaintiff can invoke the categorical rule and satisfy Rule 23 (b)(3) predominance. Given the issue's importance and the uncertain circuit precedent surrounding it, the issue, when next addressed by a Ninth Circuit panel, would be appropriate for subsequent *en banc* review.

VII. THE CATEGORICAL RULE CONFLICTS WITH *COMCAST* (AND EVEN THE NINTH CIRCUIT'S OWN CONSTRAINED READING OF *COMCAST*)

The categorical rule contradicts the key, underlying premise on which the Supreme Court's majority opinion in *Comcast* rests. The *Comcast* facts are well known. There, cable subscribers brought antitrust claims based on four competition-injury theories and, to support class certification, submitted a class-wide damages model measuring their aggregate effect.[55] The district court granted class certification even though only one of the four theories could be adjudicated as a class action and the proposed damages model

---

51 *Id.* at 1155.

52 *See, e.g., Pulaski,* 802 F.3d at 988.

53 *See Hart v. Massanari,* 266 F.3d 1155, 1171-72 (9th Cir. 2001).

54 *Pulaski,* 802 F.2d at 986.

55 *Comcast,* 133 S. Ct. at 1431.

failed to isolate and measure just the harm from that one theory, and the court of appeals affirmed.[56] The Supreme Court, however, reversed.[57]

On its surface, *Comcast* held that the plaintiffs' damages model in that case did not isolate and measure the harm caused by the plaintiffs' only operative liability theory, and so was invalid.[58] But this narrow ruling was fatal to class certification only because the parties conceded that individual damages issues would predominate absent a damages model that could serve as a class-wide method of proof.[59] It is impossible to imagine the Court undertaking its analysis if the main underlying and conceded premise—that individual damages issues alone may predominate—had no basis in fact or law. Indeed, the majority opinion treated the parties' concession as well founded, noting that, even if plaintiffs' damages model had been limited to a single injury theory, it would have still failed to show predominance if it could not adequately account for and overcome significant geographic variations in the damages proof.[60]

Interestingly, the minority opinion in *Comcast t*ook no issue with the central premise that individual damages issues alone could predominate. Rather, it was concerned that the majority opinion might be read to suggest that a class-wide method of proving damages was *always* necessary for class certification.[61] The Ninth Circuit's categorical rule, perhaps in reaction to *Comcast,* goes too far the other way.[62]

The categorical rule also conflicts with the Ninth Circuit's own reading of *Comcast.* According to *Leyva, Comcast* requires that plaintiffs "show that their damages stemmed from the defendant's action creating the liability."[63] Yet, the Ninth Circuit's categorical rule, when it is triggered, terminates the predominance inquiry at that point, rendering individual damages questions (along with any proposed method, formula or model for showing individual damages on a class-wide basis) irrelevant. This means that, when the rule applies, a plaintiff is not required to do anything further on the predominance issue. And if a plaintiff (for whatever reason) still chooses to disclose her damages method at the class certification stage, Ninth Circuit courts have no basis to scrutinize the method under *Comcast* as *Comcast* was entirely grounded on the predominance element of Rule 23(b)(3).[64] Thus, for example, in *Pulaski,* after applying the categorical rule to find that common questions predominated, the panel had no basis under *Comcast* to then assess, as

---

56 *Id.*

57 *Id.* at 1434-35.

58 *Id.* at 1435.

59 *Id.* at 1430.

60 *Id.* at 1435 n.6.

61 *See id.* at 1436.

62 Just this last Term, the Supreme Court, in discussing Rule 23(b)(3) predominance, used non-categorical language from a treatise to describe situations when common questions *may* predominate despite the need to adjudicate "other important matters" separately, such as damages. *See Tyson Foods,* 136 S. Ct. at 1045.

63 *Leyva,* 716 F.3d at 514.

64 If the *Comcast*-based requirement that "damages stem[ ] from the defendant's action creating the liability" only applies if a plaintiff chooses to disclose a damages model at the Rule 23 stage, then the requirement is an incentive for non-disclosure.

it did, plaintiffs' proposed class-wide restitution method to determine if it aligned with plaintiffs' liability cases. Further analysis under *Comcast* was superfluous.

VIII. BY IGNORING INDIVIDUAL DAMAGES ISSUES, THE CATEGORICAL RULE *DE FACTO* CERTIFIES A LIABILITY-ONLY CLASS

In the end, the Ninth Circuit, by adopting a categorical rule that applies even in cases where individualized damages issues will breakdown into "mini-trials," is, without explicitly saying so, advancing the concept of a liability-only class akin to an "issues class" permitted under Rule 23(c)(4), which authorizes "a class action with respect to particular issues."[65] The Ninth Circuit recently came close to admitting as much in *Jimenez v. Allstate Insurance Co.* The panel in *Jimenez* relied on *Leyva* to reject an argument that class certification violated defendant's due process right to assert individualized affirmative defenses at trial.[66] It viewed *Leyva* as authorizing the bifurcation of liability and damages. It also cited "as consistent with . . . *Leyva*", cases from other circuits that have certified liability-only classes.[67]

A liability-only class leaves damages determinations for separate non-class proceedings. But a district court's *sua sponte* use of a liability-only class is controversial as it can be used to "manufacture predominance" where it might otherwise not exist.[68] Ordinarily, a district court also would need to conclude that the proposed issue-class "materially advanced the disposition of the litigation as a whole."[69] This is something the courts in *Leyva, Pulaski* and *Vaquero* did not address.

The Ninth Circuit's official position on the use of issue-only classes under Rule 23(c)(4) is uncertain.[70] But, by its categorical rule, the Ninth Circuit is essentially making liability-only classes a default option to allow district courts to certify Rule 23(b)(3) classes without regard to how damages will be decided. Wherever the Ninth Circuit stands on liability-only classes, the categorical approach is an abridgment of Rule 23(b)(3)'s predominance test.

IX. CONCLUSION

The categorical rule that individual damages issues alone *never* defeat class certification likely reflects the Ninth Circuit's departure from earlier circuit precedent and conflicts with *Comcast*. The rule also allows *de facto* use of liability-only classes to ensure common-question predominance that might not otherwise exist. The rule should be discarded for the general rule that individual damages issues *may* alone defeat class certification.

---

65 Fed. R. Civ. P. 23(c)(4).

66 *See Jimenez,* 765 F.3d at 1168.

67 *See id.* at 1167-68 (citing among other cases *In re Whirlpool Corp. Frontloading Washer Prods. Liab. Litig.,* 722 F.3d 838 (6th Cir. 2013) and *Butler v. Sears, Roebuck and Co.,* 727 F.3d 796 (7th Cir. 2013)).

68 *Castano v. Am. Tobacco Co.,* 84 F.3d 734, 745 n.21 (5th Cir. 1996).

69 Manual for Complex Litigation (Fourth) § 21.24 (2004).

70 *See Valentino v. Carter-Wallace, Inc.,* 97 F.3d 1227, 1234 (9th Cir. 1996) (suggesting in dicta the possibility of certifying an issue-only class under Rule 23(c)(4) when predominance element might not permit class certification of the entire action).

EXCEPTIONS TO THE RULE: CONSIDERING THE IMPACT OF NON-PRACTICING ENTITIES AND COOPERATIVE REGULATORY PROCESSES IN THE UPDATE TO THE ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY

By Robin Feldman[1]

The Department of Justice (DOJ) and Federal Trade Commission (FTC) released a proposed update to the 1995 Antitrust Guidelines for the Licensing of Intellectual Property on August 12, 2016.[2] *The following comments were submitted to the DOJ and FTC in response to the proposed update.*

My primary comments pertain to the basic principle underlying the Guidelines and Update, that intellectual property licensing "is generally procompetitive."[3] While this premise is sound when analyzing traditional intellectual property markets, there is now a large secondary market for patents, populated by non-practicing entities (NPEs), for which the intensity of that statement no longer holds true and which requires a more nuanced approach. In that context, a stark statement of general procompetitiveness, without qualification, can hamper efforts by states and market actors to grapple with modern manifestations of anticompetitive behavior.

As explained in greater depth below, I recommend the following amplifications to the language in Sections 2.0 and 3.2 of the Update to take into account a secondary market in which intellectual property licenses may not serve procompetitive ends. The suggested language is italicized below:

- **2.0 General Principles**

(c) [T]he Agencies recognize that intellectual property licensing . . . is generally procompetitive *because it leads to competition in the marketplace and to the creation of new and useful products. Not all licensing, however, serves procompetitive ends, and its impact must be examined in the particular market context.*

- **3.2 Markets Affected by Licensing Arrangements**

Licensing arrangements raise concerns under the antitrust laws if they are likely to affect adversely the prices, quantities, qualities or varieties of goods and services either currently or potentially available . . . . The Agencies will typically analyze the competitive effects of licensing arrangements within the relevant markets for the goods affected by

---

1 Professor Feldman is the Harry & Lillian Hastings Professor of Law and Director of the Institute for Innovation Law at the University of California Hastings College of the Law. She has published two books, RETHINKING PATENT LAW (Harv. Univ. Press 2012) and THE ROLE OF SCIENCE IN LAW (Oxford 2009), as well as numerous articles. Professor Feldman has chaired the Executive Committee of the Antitrust Section of the American Association of Law Schools and was elected to the American Law Institute in 2012 where she serves as an advisor to the ALI's Restatement of Copyright Project.

2 U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY PROPOSED UPDATE (Aug. 12, 2016), *available at* https://www.justice.gov/atr/file/883941/download [hereinafter UPDATE].

3 *Id.* § 2.0.

the arrangements. In other cases, however, the Agencies may analyze the effects within a market for technology or a market for research and development.

In light of modern secondary markets for intellectual property and the existence of entities whose core activity does not involve products, an entity could adversely affect prices in a product, technology, or research and development market without necessarily holding a monopoly in that market. The following hypothetical is illustrative:

> An entity that aggregates patents approaches an automobile manufacturer, asking that the manufacturer buy a license for a patent related to the production of shoes. The automobile manufacturer demurs, and the patent holder reveals 100 more patents for technology markets unrelated to automobiles. The automobile manufacturer agrees to pay for a license to the portfolio, given that the risks and costs of litigation—even for unrelated or invalid patents—may be higher than the cost of the license. Others in the automobile manufacturing industry agree to license the portfolio, following similar logic. The cost of such licensing may be passed on to the consumer in the form of higher prices. Thus, the price of automobiles may be raised through increased production costs, notwithstanding the fact that the patent portfolio holder did not hold any patents validly related to automobile production.

Finally, as also explained below, I suggest a short addition to the language related to refusals to deal. The new language, italicized below, relates to circumstances in which pharmaceutical companies refuse to cooperate with generics or other competitors on approval or on safety plans required by the Food and Drug Administration (FDA).

• 2.1 Standard Antitrust Analysis Applies to Intellectual Property

The Agencies apply the same general antitrust principles to conduct involving intellectual property that they apply to conduct involving any other form of property. . . . The antitrust laws generally do not impose liability upon a firm for a unilateral refusal to assist its competitors, in part because doing so may undermine incentives for investment and innovation. *Regulatory processes that require interaction with or cooperation among competitors, however, may present special circumstances.*

Background Discussion:

The basic principle that intellectual property licensing is generally procompetitive is sound when analyzing traditional intellectual property markets. Different dynamics apply, however, in the extensive secondary markets for intellectual property that have expanded rapidly over the last decade.

I. LICENSING IN THE SECONDARY MARKETS DOES NOT NECESSARILY SERVE PROCOMPETITIVE ENDS

A. Power Operates Differently in the Secondary Markets

Market power, as understood in the three traditional markets,[4] has the potential to operate differently in the secondary markets. Traditionally, market power is measured in relationship to a particular product, and one might be concerned about potential anticompetitive behavior when an entity holds powerful patents related to a particular product, technology, or process.

The intellectual property landscape, however, has changed substantially over the last decade. Specifically, a secondary market has developed in which large numbers of patents that would have had little value in the past are now being grouped and monetized, irrespective of the underlying subject matter of the patent.[5] When these unmoored patent rights are traded and arbitraged on a large scale or in a widespread manner, that activity resembles a market of its own. Non-practicing entities (NPEs), whose primary activities focus on licensing or litigating patents, are key players in the secondary market.

Characteristics of the secondary market are allowing rights holders to bargain for returns well above the value of the rights they hold. This bargaining power flows from the low cost of asserting patents against a product company relative to the costs and risks of defending against the assertion. The ability to group patents together for patent assertion, even if the patents are weak or unrelated, enhances the impact. Widespread concerns about patent quality make such behavior particularly problematic.[6]

In light of modern secondary markets, an entity could acquire market power in a primary market without necessarily holding a monopoly in that specific market or in any individual product market. As illustrated in the example suggested above for inclusion in Section 3.2 of the Update, one simply needs a large enough group of any type of patent, together with tough tactics, to have a negative effect in a market one otherwise would not impact.

Given that extensive numbers of patents are now being monetized for purposes that have nothing to do with a particular product, along with characteristics of the operation of this extensive secondary market, an unqualified statement that licensing is generally procompetitive lacks sufficient nuance. Additional factors, discussed below, also cast doubt on the applicability of the procompetitive principle in the context of the secondary market.

---

4 The three markets are the goods market, the technology market, and the research and development market. *See* UPDATE, *supra* note 2, § 3.2.

5 *See* Robin Feldman, *Intellectual Property Wrongs*, 18 STAN. J.L. BUS. & FIN. 250, 257-73 (2013).

6 *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, INTELLECTUAL PROPERTY: ASSESSING FACTORS THAT AFFECT PATENT INFRINGEMENT LITIGATION COULD HELP IMPROVE PATENT QUALITY 28-32 (2013), *available at* http://www.gao.gov/assets/660/657103.pdf [hereinafter GAO REPORT] (detailing how many stakeholders believe some patents "have unclear property rights and make overly broad claims"); Shawn P. Miller, *Where's the Innovation: An Analysis of the Quantity and Qualities of Anticipated and Obvious Patents*, 18 VA. J.L. & TECH. 1, 6–7 (2013) (estimating that up to 39% of software patents and 56% of business method patents could be found at least partially invalid, compared to 28% of all patents).

B. The Rise in NPE Litigation, Along with NPE Litigation Tactics, Casts Doubt on the Applicability of the Procompetitive Principle in Secondary Markets

The number of patent lawsuits has more than doubled since 2007, increasing from around 2,500 suits in 2007 to over 5,800 in 2015,[7] and much of this increase is fueled by NPEs. For example, NPEs filed 2,750 patent suits in 2012, an increase of more than 600% since 2007.[8] In addition, by 2012, lawsuits by NPEs represented the most common type of patent litigation, increasing from about 20% of lawsuits in 2007 to nearly 60%.[9] According to one private study, NPEs filed a full two-thirds of the patent lawsuits in 2015.[10] Although different studies focus on different segments of the data, the results are remarkably consistent across similar measures.[11] The amount of litigation activity from NPEs has risen substantially in the last decade.

NPEs have become adept at pointing out the costs and risks of challenging a patent demand in comparison to the ease of purchasing a license, and they commonly sue twenty or more defendants in the same industry at the same time, settling with each in exchange for a nonexclusive license.[12] With patent litigation defense costs often reaching well into

---

7 *See* Robin Feldman, Tom Ewing & Sara Jeruss, *The AIA 500 Expanded: The Effects of Patent Monetization Entities*, 17 UCLA J.L. & Tech. 1, 42 (2013) (showing that the number of patent lawsuits rose from 2,512 in 2007 to 5,038 in 2012); Matthew Sag, *IP Litigation in United States District Courts:1994 to 2014,* 101 Iowa L. Rev. 1065, 1075 tbl.3 (2016) (reporting number of patent cases as 1,555 in 1994, 2,883 in 2007, 5,620 in 2012, and 5,368 in 2014); *id.* at 1080 fig.4 (showing that the number of patent lawsuits doubled in the sixteen years between 1994 and 2014, and doubled again between 2010 and 2013); Brian Howard, *Lex Machina 2015 End-of-Year Trends*, Lex Machina (Jan. 7, 2016), https://lexmachina.com/lex-machina-2015-end-of-year-trends/ (showing that the number of patent cases filed grew to 5,830 in 2015).

8 *See The Patent Litigation Landscape: Recent Research and Developments*, Council of Economic Advisers Issue Brief 4 (March 2016) [hereinafter *Patent Litigation Landscape*] (referencing IPO study described in *Patent Demands and IPOs*); Robin Feldman & Evan Frondorf, *Patent Demands and Initial Public Offerings*, 19 Stan. Tech. L. Rev. 52, 55 (2015) [hereinafter *Patent Demands and IPOs*].

9 *See* Feldman & Frondorf, *Patent Demands and IPOs*, *supra* note 8, at 55; *Patent Litigation Landscape*, *supra* note 8, at 3 (noting that NPEs brought 60% of patent litigation cases in 2014).

10 *See 2015 Patent Dispute Report*, Unified Patents (Dec. 31, 2015), *available at* https://www.unifiedpatents.com/news/2016/5/30/2015-patent-dispute-report (reporting that NPEs initiated 66.9% of District Court patent cases in 2015).

11 Variation between studies generally depends on definitional choices made by researchers. For example, using a sample of 500 patent infringement cases, Jeruss, Feldman & Walker found that the proportion of lawsuits filed by NPEs increased from 22% of cases in 2007 to almost 40% of cases in 2011. *See* Sara Jeruss, Robin Feldman & Joshua H. Walker, *The America Invents Act 500: Effects of Patent Monetization Entities on US Litigation*, 11 Duke L. & Tech. Rev. 357, 377 (2012). Meanwhile, using the same sample, the nonpartisan Government Accountability Office (GAO) found that the proportion rose from 17% in 2007 to only 24% in 2011. *See* GAO Report, *supra* note 6, at 17. The majority of the difference can be explained by the GAO's choice not to include individuals and trusts as potential NPEs, choosing instead to focus only on entities organized as corporations and partnerships.

12 *See* Mark A. Lemley & Robin Feldman, *Patent Licensing, Technology Transfer, and Innovation*, 106 Am. Econ. Rev. 188 (2016).

the millions of dollars, coupled with the uncertainty of litigation, a rational company may well choose to settle a patent demand, even if the infringement claim lacks merit.[13]

In short, modern patent demand behavior frequently is based on exploiting the costs and risks of litigation to extract a settlement, rather than on the value of the patent. In other words, licensing does not appear to be procompetitive as a rule within the secondary markets.

C. The Timing of NPE Licensing Requests Casts Doubt on the Applicability of the Procompetitive Principle in Secondary Markets

Concern that NPE licensing behavior is not procompetitive is further illustrated in the context of initial public offerings (IPOs) or other cash shock events. In my recent study of product companies that had an IPO between 2007 and 2012, 40% of respondents received patent demands during the periods around the time of their IPOs, with those demands coming largely from NPEs. The effects were even more pronounced for information technology companies, with almost 60% of those respondents reporting patent demands around the time of their IPOs.[14] Almost all of the demands received from technology companies originated from NPEs.[15] Another study found that a company was five times more likely to be sued by an NPE following a large, positive cash infusion, such as a funding event or IPO, and that a cash shock was a significant predictor of the number of times a company was sued by NPEs.[16]

Whether NPEs are motivated by the lure of deep pockets afforded by a cash shock or by the leverage opportunities afforded by an IPO period, the timing of their licensing demands is yet another indication that the activity is driven by issues other than the merits of individual patent claims. Licenses procured in this manner are unlikely to be procompetitive.

In short, the burgeoning secondary market for patent monetization is rife with opportunities for behavior that is anything but procompetitive. As a result, qualification of the statement that licensing is generally procompetitive is essential for providing a full picture of modern intellectual property markets, especially in the context of patents.

II. REGULATORY PROCESSES THAT REQUIRE COOPERATION AMONG COMPETITORS PRESENT SPECIAL CIRCUMSTANCES TO THE REFUSAL TO ASSIST COMPETITORS

Section 2.1 of the Update states, in relevant part, "[t]he antitrust laws generally do not impose liability upon a firm for a unilateral refusal to assist its competitors, in part

---

13 *See Patent Litigation Landscape*, *supra* note 8, at 7 (noting that "accused infringers may decide to settle rather than bear the cost of fighting what they believe to be allegations without merit, and patent holders with meritorious claims (and limited resources) may decide to settle rather than bearing the costs of fully enforcing their patent rights.").

14 *See* Feldman & Frondorf, *Patent Demands and IPOs*, *supra* note 8, at 54.

15 *Id.*

16 *See* Lauren Cohen, Umit D. Gurun & Scott Duke Kominers, *Patent Trolls: Evidence from Targeted Firms* 14 (Harv. Bus. Sch. Working Paper No. 15-002, 2015), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2464303.

because doing so may undermine incentives for investment and innovation."[17] While this is a sound position generally, regulatory processes that require interaction or cooperation among competitors present special circumstances and call into question the propriety of refusing to assist a competitor.

In particular, drug companies in the pharmaceutical industry have used administrative processes and regulatory schemes to obstruct generics from getting to market.[18] Delays of even six months can be worth hundreds of millions of dollars in revenue with a blockbuster drug, creating great temptation for this type of behavior.

For example, under the Hatch-Waxman system for expedited approval of generic drugs, generic companies need a sample of the brand-name drug in order to demonstrate to the FDA that the two drugs are equivalent. Companies have refused to provide samples to potential generic competitors, arguing that they have the right of "refusal to assist," despite the structure of the Hatch-Waxman system.

Similarly, with medicines that require heightened safety protocols, the brand company and generic hopeful must work together to establish those protocols before the generic can receive approval. Brand companies have delayed or refused to cooperate with their potential generic competitors on such plans. In some cases, this behavior has persisted even when the FDA has explicitly instructed the brand company to provide the samples needed or to cooperate with the generic on the safety plans.

As a general principle, a refusal to assist is not anticompetitive. In the case of certain regulatory processes that rely on competitor cooperation, however, such as the Hatch-Waxman system for approval of generic drugs, there are special circumstances. These circumstances should be referenced in Section 2.1 of the Update.

---

17 UPDATE, *supra* note 2, § 2.1.

18 For detailed discussion of these game-playing techniques, *see* Robin Feldman & Evan Frondorf, *Drug Wars: A New Generation of Generic Pharmaceutical Delay*, 53 HARV. J. ON LEGIS. 499 (2016); Robin Feldman, Evan Frondorf & Andrew K. Cordova, *Empirical Evidence of Drug Pricing Games: A Citizen's Pathway Gone Astray*, STAN. TECH. L. REV. (forthcoming 2016), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833151; Robin Feldman, *Regulatory Property: The New IP*, COLUM. J.L. & ARTS (forthcoming 2016), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2815667; *see also CREATES Act: Ending Regulatory Abuse, Protecting Consumers and Ensuring Drug Price Competition: Hearing Before S. Comm. on the Judiciary, Subcomm. on Antitrust, Competition Policy and Consumer Rights*, 114th Cong. (2016) (statement of Professor Robin Feldman, Director of the Institute for Innovation Law, University of California Hastings College of the Law), *available at* https://www.judiciary.senate.gov/imo/media/doc/06-21-16%20Feldman%20Testimony.pdf; *Treating the Opioid Epidemic: The State of Competition in the Markets for Addiction Medicine: Hearing before H. Comm. On the Judiciary, Subcomm. on Regulatory Reform, Commercial and Antitrust Law*, 114th Cong. (2016) (statement of Professor Robin Feldman, Director of the Institute for Innovation Law, University of California Hastings College of the Law), *available at* https://judiciary.house.gov/wp-content/uploads/2016/09/Feldman-Testimony.pdf.

COMMENTS ON PROPOSED UPDATE ON INTELLECTUAL PROPERTY LICENSING GUIDELINES

By Michael A. Carrier[1]

I applaud the agencies for updating the Intellectual Property (IP) Licensing Guidelines. I have two general reactions.

First, in these (or supplemental) guidelines, the agencies could consider addressing IP licensing issues related to (1) standard essential patents (SEPs), (2) patent assertion entities (PAEs), and (3) drug patent settlements. Although addressed in agency orders and speeches, each of these topics could benefit from further elaboration in the form of guidelines.

Second, to offer a more nuanced analysis, the agencies in three places could recognize the crucial regulatory and industry context.

Suggestion 1: At the end of footnote 13 on page 6, consider adding this sentence: "This general statement may be modified given the regulatory context."

Reason: Regulatory regimes may promote goals other than fostering incentives for investment and innovation. Brand drug companies, for example, have used restricted-distribution schemes to prevent generic firms from engaging in bioequivalence testing, which prevents them from entering the market. This contravenes a central objective of the Hatch-Waxman Act of encouraging generic entry and is the focus of the pending bipartisan CREATES Act. The regulatory setting was vital to the *Trinko* decision, and absent a recognition of this context, the agencies' proposed revision could neglect important government objectives.

Suggestion 2: At the end of footnote 17 on page 9, consider adding this sentence: "On the other hand, the creation and exploitation of massive patent portfolios could threaten concern as they are valuable because of their size rather than the validity of each patent in the portfolio."

Reason: Although aggregation could address the "double marginalization" problem in which different firms apply their own markups, large patent portfolios also could present significant anticompetitive effects including patent holdup, raising rivals' costs, and even increased price and reduced innovation.[2]

Suggestion 3: Consider adding a footnote after "specific firms" on the last line of text on page 16 and then adding a new footnote: "The anticompetitive effects presented in, and need for the use of, research-and-development markets may vary based on industry."

---

1 Michael A. Carrier is a Distinguished Professor at Rutgers Law School, co-author of the leading IP/antitrust treatise, and author of more than 85 articles and book chapters on these issues.

2 *See* Michael A. Carrier, *Patent Assertion Entities: Six Actions the Antitrust Agencies Can Take*, at 2-3, CPI Antitrust Chronicle (Jan. 2013).

Reason: Many of the criticisms that have been leveled against R&D markets apply much less, if at all, in certain settings. Pharmaceutical R&D, for example, is characterized by specific firms that can be identified, the absence of inefficient duplication, and the importance of competition for innovation.[3]

3 *See* Michael A. Carrier, *Two Puzzles Resolved: Of the Schumpeter-Arrow Stalemate and Pharmaceutical Innovation Markets*, 93 Iowa L. Rev. 393, 401-14 (2008).

DISPATCHES FROM THE WEST COAST: FEDERALISM, COMPETITION, AND COMMENTS ON THE UNITED STATES' PROPOSED UPDATE TO THE ANTITRUST GUIDELINES FOR LICENSING INTELLECTUAL PROPERTY[1]

By Emilio Varanini[2] and Cheryl Johnson[3]

I. INTRODUCTION

The United States Department of Justice and the Federal Trade Commission (the "Agencies") issued in August of this year the Proposed Update to the Antitrust Guidelines for Licensing Intellectual Property (the "Proposed Update") and sought comments from the public.[4] Though the official comment period closed on September 26, 2016, it is anticipated that the finalization of the Proposed Update will take some time.

States like California are on the front lines in finding the appropriate mix between intellectual property ("IP") and antitrust so as to continue the unprecedented growth of industries in their states, such as the high-technology industry, the biotech industry, and the creation of new content and services.[5] It is therefore important for states that the balance be struck true in rewarding innovation through the grant of IP rights without allowing the anticompetitive leveraging of those rights to create entrenched monopolies

---

1 The comments expressed in this Article are the personal views of the authors and should not be ascribed in any way to the California Office of the Attorney General. The authors also wish to thank Luminita Nodit and Neal Luna of the Washington Attorney General's Office for their comments and suggestions from which this Article greatly benefitted.

2 Emilio Varanini is a senior Deputy Attorney General in the California Attorney General's Office who has taken the lead in several investigations involving copyright and trade secrets as well as high technology markets. He has been lead counsel in such IP cases as *People of the State of California v. Pratibha Synthex, People of the State of California v. Ningbo Beyond*, and *Bunner v. DVDCCA*. He is currently Secretary, and a Member of the Executive Committee, for the International Law Section of the State Bar of California.

3 Cheryl Johnson is a senior Deputy Attorney General in the California Attorney General's Office who has taken the lead in several pharmaceutical and Non-Practicing Entity cases involving antitrust, unfair competition, and patents and authored the *amicus curiae* brief of the California Attorney General's Office in *In re Cipro Cases I & II*, 348 P.3d 845 (Cal. 2015). She is a member of the patent bar, and is a Past Chair of the Section of Antitrust, Unfair Competition, and Privacy of the State Bar of California.

4 *See* U.S. Dep't of Justice and Fed. Trade Comm'n, *Proposed Update, Antitrust Guidelines for the Licensing of Intellectual Property*, August 12, 2016, https://www.ftc.gov/system/files/documents/reports/antitrust-guidelines-licensing-intellectual-property-proposed-update-1995-guidelines-issued-us/ip_guidelines_published_proposed_update.pdf.

5 *See, e.g.*, *Economy of California*, Wikipedia, https://en.wikipedia.org/wiki/Economy_of_California (last visited Oct. 10, 2016) (discussion of Silicon Valley); *Uber (company)*, Wikipedia, https://en.wikipedia.org/wiki/Uber_(company) (last visited Oct. 10, 2016); Rich Taylor, *Video Game Industry Adds Billions to U.S. Economy*, Huffington Post, http://www.huffingtonpost.com/rich-taylor/the-billion-dollar-video-game-industry_b_6148684.html (Nov. 13, 2014, updated Jan. 13, 2015) (discussing how seven states, including California, employ 80% of the workers in this industry); Junfu Zhang & Nikesh Patel, The Dynamics of California's Biotechnology Industry (Pub. Policy Inst. of Cal. 2005) (discussing origins of biotech industry in California as well as California's accounting for 40% of the market).

and cartels that hinder competition.[6] States like California have brought important cases in the areas of pharmaceuticals and high-technology involving the intersection of IP and antitrust.[7] And as guardians of federalism and the resulting split of sovereignty in the U.S. Constitution,[8] states like California have a strong interest in reconciling and harmonizing the workings of IP laws with other laws and doctrines, including state and federal antitrust law.[9] As antitrust enforcers for the State of California with a substantial background in IP, we set out our own personal views on this Proposed Update against this backdrop.

II. AN OVERVIEW OF THE PROPOSED UPDATE: SETTING OUT WHERE IT ADVANCES THE BALL AND WHERE ADDITIONAL THINKING WOULD BE HELPFUL TO STRIKING THE TRUE BALANCE BETWEEN IP AND ANTITRUST

We support substantial aspects of the Proposed Update, including: the importance of closely reviewing acquisitions or transfers of IP; the application of a rule of reason analysis in Sherman Act Section 2 monopoly cases;[10] and, within the rule of reason framework for Sherman Act Section 1 joint conduct and Section 2 monopoly cases, the need for the determination not just of a restraint's "fit" but also whether practical and significantly less restrictive alternatives exist.[11] Our comments focus on the following issues:

Overbroad presumption that IP licensing agreements are procompetitive. The Proposed Update presumes that all IP licensing agreements are procompetitive such that the first step for the Agencies will be to rule out *plausible* efficiencies for those agreements before proceeding with a more in-depth analysis. Such a presumption may be appropriate in certain instances, such as a vertical IP licensing agreement in which an IP rights holder licenses its property to a product using that IP absent concerns about foreclosure or

---

6 *See, e.g.*, *In re Cipro Cases I & II*, 348 P.3d 845, 855-56, 858, 863 (Cal. 2015) (analyzing the reach of federal patent law in addressing the legality of reverse payment pharmaceutical settlements under state antitrust law).

7 *See, e.g.*, *United States v. Microsoft*, 253 F.3d 34 (D.C. Cir. 2001) (en banc); Press Release, California Office of the Att'y Gen., Attorney General Kamala D. Harris Files Lawsuit Against Pharmaceutical Company for Inflating Prices for Opioid Addiction Treatment (Sept. 22, 2016), https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-lawsuit-against-pharmaceutical-company; *Abbott Labs. Settle States' Tricor Generics Suit for $22.5 Million*, 17 No. 11 Andrews Antitrust Litig. Rep. 8 (Feb. 11, 2010).

8 *See Alden v. Maine*, 527 U.S. 706, 714 (1999) (discussing the dual sovereignty of the states and federal government).

9 *See In re Cipro I & II*, 348 P.3d at 855-56, 858-62; Peter Lee, *The Supreme Assimilation of Patent Law*, 114 Mich. L. Rev. 1413, 1425-26 (2016).

10 *See* Diana De Leon, *The Judicial Contraction of Section 2 Doctrine*, 45 Loy. L.A. L. Rev. 1105, 1122 (2012) (discussing the increased use of the rule of reason by lower courts in assessing monopoly claims); *id.* at 1164-65 (arguing in favor of a modified rule of reason test for Section 2 monopolization claims in accordance with the views of the late Commissioner Rosch of the Federal Trade Commission).

11 *See, e.g.*, Proposed Update, § 4.2. We also agree with Section 3.1, at note 25, of the Proposed Update that access to IP can be required to remedy anticompetitive conduct.

raising a rival's costs.[12] The presumption, however, should not apply when the licensing agreement (1) sweeps beyond the scope of the IP grant; or (2) involves a horizontal arrangement between competitors. Although there are certain horizontal licensing agreements, such as patent pools, that may be procompetitive, the Agencies should insist, as they historically have, that the participants provide safeguards to avoid possible anticompetitive effects.

The failure to spell out how IP licensing conduct such as fixing resale prices (known as resale price maintenance or "RPM") and tying can be likely anticompetitive under certain circumstances. The Proposed Update would better serve the public interest and the business community by delineating those circumstances under which IP licensing conduct is likely anticompetitive. Given that RPM can be used, for example, to evade the first sale or exhaustion doctrines, it should be presumed to be anti-competitive when used in an IP licensing agreement *at least* when RPM restraints cover more than 50% of a market, are imposed by dominant firm, or were initiated by licensees.

The failure to address licensing arrangements when the licensor has monopoly power. The Agencies need to set out a more specific inquiry under the rule of reason of licensing-related conduct that present special concerns of anticompetitive effects in the context of Section 2. For example, the Agencies may wish to infer anticompetitive effects under the rule of reason in Section 2 cases involving tying/bundling and exclusive dealing and neither assume actual efficiencies nor reject practical, significantly less restrictive alternatives absent adequate explanations supplied by the licensor.

Trinko[13] *does not compel the Agencies to recognize an extremely wide scope for IP holders to condition access to their IP even when those firms have market power.* While we certainly agree that a firm can refuse to license its IP in the first instance, it is another matter whether *Trinko* can or should be read for the broader proposition that a firm has a wide scope in how it conditions access to its IP[14]—even when it has market power.[15] *Actavis*[16] and *Microsoft*[17] do not support such an expansive view on access. Moreover, *Trinko* itself was a narrow decision involving competitor access in a highly regulated industry. We believe

---

12 We commend the Proposed Update for recognizing the concerns that can accompany vertical licensing agreements in upstream and downstream markets involving products or research and development. The Supreme Court has also found that business conduct can have differing impacts on upstream and downstream markets that warrant a different analysis of the impact on each of these markets. *See Weyerhaeuser Co. v. Ross-Simmons Hardware Co.*, 549 U.S. 312, 321-22 & n.2 (2007). But the Agencies should not presume that a justification for this conduct, when these concerns are present, exists. *See ZF Meritor LLC v. Eaton Corp.*, 696 F.3d 254, 277-78 (3d Cir. 2012) (discussing alleged lower costs as a justification for exclusive dealing).

13 *Verizon Commc'ns v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398 (2004).

14 We take no position on the issue of whether, and under what conditions, access must be afforded to standard-essential patents though we interpret the more general Proposed Update as not addressing the more specific issues of antitrust, unfair competition, IP, and contract law involved with standard-essential patents.

15 We also agree with the proposition that market power does not flow solely from the IP right itself as well as with the discussion of market power set out in the Proposed Update. Proposed Update, § 2.2.

16 *Federal Trade Commission v. Actavis*, 133 S.Ct. 2223 (2013).

17 *United States v. Microsoft*, 253 F.3d 34 (D.C. Cir. 2001) (en banc).

that these proposed clarifications would signal to the business community the kind of licensing conduct they should avoid in highly concentrated and cartelized markets.[18]

III. THE AGENCIES SHOULD ONLY PRESUME LICENSING AGREEMENTS ARE PROCOMPETITIVE UNDER LIMITED CIRCUMSTANCES

At multiple points in both the Proposed Update and the original Guidelines, licensing agreements are presumed to be procompetitive. The Proposed Update could be clarified to state that this presumption does not apply if the IP licensing agreement sweeps beyond the scope of the IP grant or if the IP licensing agreement involves competitors.

A. Licensing Agreements Cannot Be Assumed to Be Procompetitive When They Sweep Beyond the Scope of the Underlying IP Grant

IP rights encourage and safeguard innovation and further competition in the development of new technologies and products by affording a government grant of exclusivity.[19] But the extent of the IP grant must be carefully respected to prevent entrenching monopolies that restrain competition and innovation.[20] A trade secret can be protected forever—as long as reasonable steps are taken to ensure its confidentiality—but may be subject to reverse engineering.[21] A copyright can only protect an expression of

---

18 The Proposed Update refers to the Agencies' assumption that IP licensing agreements are procompetitive as a presumption. Presumptions are used in litigation to structure the burdens of production and proof either according to statutory requirements, *see, e.g.*, *Halo Elec. v. Pulse Elecs.*, 136 S.Ct. 1923 (2016); *Octane Fitness LLC v. Icon*, 134 S.Ct. 1749 (2016), or according to economic teachings, market realities, and administrability concerns, *see, e.g.*, *United States v. Delta Dental of R.I.*, 943 F. Supp. 172, 190 (D.R.I. 1996) ("'legal presumption that rest on formalistic distinctions rather than actual market realities are generally disfavored in antitrust law'") (quoting *Eastman Kodak Co. v. Image Technical Servs.*, 504 U.S. 451, 466-67 (1992)); *see also Kimble v. Marvel Entertainment LLC*, 135 S.Ct. 2401, 2412-13 (2015) (noting that the Supreme Court has revised its legal analysis in antitrust law as economic understanding evolves). We recognize that the Agencies have declared that the statements made in the Proposed Update may not accord with the positions they take in litigation such that these Guidelines will be nothing more than helpful statements of prosecutorial intent. Proposed Update, § 5.3 & n.73. But the courts have nonetheless referred in the past to the original Guidelines as support for changes in the law. *See Illinois Tool Works Inc. v. Independent Ink, Inc.*, 547 U.S. 28, 45 (2006). The Agencies should keep this point in mind as they update the original Guidelines.

19 *See, e.g.*, Proposed Update, § 1.0 (explaining that IP rights confer exclusivity for the purpose of promoting innovation and enhancing consumer welfare).

20 *See Kimble v. Marvel Entertainment LLC*, 135 S.Ct. 2401, 2406-07 (2015) ("Patents endow their holders with superpowers, but only for a limited time. Congress struck a balance between fostering innovation and ensuring public access to discoveries. . . . But a patent typically expires 20 years from the day the application for it was filed. And when the patent expires, the patentee's prerogatives expire too, and the right to make or use the article, free from all restrictions, passes to the public. This Court has carefully guarded that cut-off date, just as it has the patent laws' subject-matter limits: In case after case, the Court has construed those laws to preclude measures that prevent free access to formerly patented, as well as unpatentable, inventions.") (internal citations omitted). Similarly, other courts have observed that there is "*a fundamental right to compete through imitation of a competitor's product*, which right can only be *temporarily* denied by the patent or copyright laws." *Leatherman Tool Group, Inc. v. Cooper Indus., Inc.*, 199 F.3d 1009, 1011-12 (9th Cir. 1999) (internal citations and quotation marks omitted).

21 *See, e.g.*, Defend Trade Secrets Act, 18 U.S.C. § 1839; *see also Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 483-91 (1974).

an idea rather than the underlying idea itself—and is subject to an exception for fair use.[22] And under the first sale doctrine in copyright law as well as the doctrine of exhaustion in patent law, a purchaser of a product containing an already-licensed IP right may resell that product freely without running afoul of IP laws.[23]

Patents themselves can be found to be invalid if they patent laws of nature, natural phenomenon, or abstract ideas.[24] Because of concerns over the validity and quality of patent grants[25]—not to mention difficulties in ascertain the existence and scope of patents reading on a potential product prior to its manufacture—patents can be subject to *post hoc* challenge not just in court but via a new statutory administrative process.[26]

The Supreme Court has repeatedly signaled its concern about exceeding the scope of IP grants, most recently by rejecting the argument that a firm can charge royalties for the use of a patent that exceeded the underlying term of the patent, finding such an arrangement to be an impermissible extension of the underlying grant.[27] Similarly, the Proposed Update should expressly recognize that a licensing agreement can be used to extend an IP right past the terms of a government grant, such as, but not limited to, the following circumstances: (1) barring challenges to a patent's validity; (2) requiring an overbroad reciprocal grant of other IP rights; or (3) by using the IP right to engage in anticompetitive bundling or discrimination against rivals.

---

22 *See, e.g.*, *Oracle America, Inc. v. Google, Inc.*, 750 F.3d 1339 (Fed. Cir. 2014); *Oracle America, Inc. v. Google, Inc.*, 2016 WL 3181206 (N.D. Cal. June 8, 2016).

23 *See Kirtsaeng v. John Wiley & Sons, Inc.*, 133 S.Ct. 1351, 1363-67 (2013) (applying the first sale doctrine to copies of copyrighted works lawfully made abroad); *Quanta Computer, Inc. v. LG Electronics, Inc.*, 553 U.S. 617, 621, 625-29 (2008) (applying the patent exhaustion doctrine to method patents).

24 *See Intellectual Ventures LLC I v. Symantec Corp.*, Nos. 2015-1769, 2015-1770, 2015-1771 (slip. op.) (Fed. Cir. Sept. 30, 2016), http://www.cafc.uscourts.gov/sites/default/files/opinions-orders/15-1769.Opinion.9-28-2016.1.PDF (explaining the legal standard for distinguishing laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts).

25 *See, e.g.*, *In re Cipro Cases I & II*, 348 P.3d 845, 859-60 (Cal. 2015) (discussing the process of reviewing patent applications and of allowing challenges to a patent's validity); *see also, e.g.*, *Actavis,* 133 S.Ct. at 2230-31 (recognizing that a valid patent carries with it the right to exclude only products that are infringing and noting that no such right exists if the patent is invalid).

26 *See Cuozzo Speed Technologies, LLC v. Lee*, 136 S.Ct. 2131 (2016).

27 *Kimble*, 135 S.Ct. at 2407-08, 2409-10, 2411-12, 2415. In *Actavis*, the Supreme Court rejected immunity for settlement conduct claimed to be within the scope of the underlying patent, 133 S.Ct. at 2230-33, thus further reinforcing the notion that a procompetitive presumption for conduct outside of the scope of an IP grant is improper.

Such agreements can be anticompetitive when a firm has market power.[28] And it can't be assumed in these circumstances, under either economic teaching or case law, that licensing agreements which extend the scope of a government grant of IP are presumptively procompetitive and thus exempt from the antitrust laws.[29]

B. Licensing Agreements Cannot Be Presumed to Be Procompetitive When Between Competitors

The Proposed Update suggests that IP licensing agreements between competitors will be presumed to be procompetitive.[30] Historically, they were viewed in the same fashion as other horizontal agreements between competitors. Patent pools, for example, could be used to implement *per se* illegal price-fixing and market allocation cartels.[31] And patent pools can otherwise still be anticompetitive when (1) an excluded firm from a pool cannot compete absent access; (2) limitations on access to the pool are not a reasonable fit; or (3) the net competitive effects are negative.[32] But pool participants could show that their patent pool deserved to be treated as being procompetitive, and subject to a rule of reason analysis, only if they provided facts to explain how the pool was designed to accomplish procompetitive ends based on market realities and only if they explained how they planned to institute safeguards against anticompetitive ends.[33]

The Proposed Update appears to depart from this practice in two ways. First, it starts from the premise—that must then be disproven—that such pools all serve procompetitive

---

28 *See, e.g.*, Thomas Cheng, *Antitrust Treatment of the No Challenge Clause*, 5 NYU J. Int. Property and Ent. Law 437, 506-508 (2016) (proposing a market power screen no analyze no challenge clauses).

29 *See, e.g.*, *Kimble*, 135 S.Ct. at 2414 ("While we recognize that post-patent royalties are sometimes not anticompetitive, we just cannot say whether barring them imposes any meaningful drag on innovation. . . . Neither Kimble nor his amici have offered any empirical evidence connecting *Brulotte* [*v. Thys Co.*, 379 U.S. 29 (1964) (charging post patent expiration royalties violated the patent laws)] to decreased innovation; they essentially ask us to take their word for the problem."). This principle does not go completely unacknowledged in the Proposed Update, as Example 4 of Section 3.3 contemplates that the validity of the patent at issue plays a role in the antitrust analysis of that hypothetical.

30 *Compare, e.g.*, Proposed Update, § 3.4 (using the example of a vertical licensing agreement between an IP holder and a manufacturer of a product to illustrate the procompetitive efficiencies of such agreements but not limiting the scope of its presumption of procompetitive efficiencies to such arrangements) *with e.g.*, Proposed Update, § 4.1.2 (in discussing certain arrangements involving exclusivity, noting that such arrangements "generally" raise concerns when they have a horizontal aspect such as cross-licenses among competitors with collective market power, grantbacks, and acquisitions); *see also* Proposed Update, §§ 4.1-4.3. It may well be that certain agreements between competitors such as price-fixing, market allocation, output limitation, or bid rigging that do not involve a joint venture, or concealment or deception as with a typical cartel, may be subject to a "check" such as an abbreviated market impact analysis to confirm that they should be treated as being *per se* illegal for purposes of civil liability. *See United States v. Apple, Inc.*, 791 F.3d 290, 310 (2d Cir. 2015) (discussing hub and spoke conspiracy with vertical and horizontal elements). But such a "check" is not the same thing as self-imposing an apparent requirement to disprove the existence of any or all plausible procompetitive efficiencies as a threshold matter even if not (apparently) advanced by defendants.

31 *See United States v. Glaxo Group, Ltd.*, 410 U.S. 52 (1973); *Zenith Radio Corp. v. Hazeltine Research, Inc.*, 395 U.S. 100 (1969); *United States v. United States Gypsum*, 333 U.S. 364 (1948); *Vulcan Powder Co. v. Hercules Powder Co.*, 96 Cal. 510 (Cal. 1892).

32 *See* Proposed Update, §§ 4.2, 5.5.

33 *See, e.g.*, U.S. Dep't of Justice, Bus. Rev. Ltr. to MPEG-LA (Jun. 26, 1997), http://www.usdoj.gov/atr/public/busreview/1170.htm.

ends. Second, it states that the presence or absence of safeguards may be of no moment in focusing prosecutorial resources on those pools that are the most problematic. That approach is not supported by economic teaching or prior experience[34] and is in considerable tension with Supreme Court case law on the review of joint ventures among competitors involving licensing of copyrights. In such cases, not only were defendants required to supply evidence of efficiencies, but the existence of effective safeguards to avoid anticompetitive effects was highlighted when permitting participants in such ventures to independently license their rights to third parties.[35] A licensing venture between competitors, including a patent pool, lacking appropriate safeguards, or the failure by the licensing parties to that venture to advance procompetitive justification based on market realties for it, warrants a closer look at that venture from antitrust enforcers.[36]

Generally speaking, there is no reason to assume that horizontal licensing agreements between competitors are generally procompetitive any more than there is a reason to assume horizontal agreements between competitors involving any other type of product, service, or property right are generally procompetitive. Even the one example in Section 2.3 of the Proposed Update of a horizontal agreement between competitors to address blocking patents assumes that the patents are valid and that they are blocking, even though historically the burden of providing facts sufficient to verify such claims in this context would have fallen on the parties to this arrangement.[37]

IV. THE PROPOSED FULL RULE OF REASON ANALYSIS MAY NOT BE WARRANTED FOR RESALE PRICE MAINTENANCE, TYING, AND CERTAIN CONDUCT INVOLVING MONOPOLIZATION

We further believe the public interest would be better served by clearly delineating circumstances where the full rule of reason may not be applied because of licensing conduct which is more likely to be anticompetitive and less likely to be procompetitive. That conduct is likely in cases involving RPM, tying, and certain conduct involving the illegal acquisition or maintenance of monopoly.

---

34 *See* Scott Sher, Jonathan Lutinski, and Bradley Tennis, *The Role of Antitrust in Evaluating the Competitive Impact of Patent Pooling Arrangements*, 13 Sedona Conf. L. 111, 114-23, 130-31 (2011); Richard Gilbert, *Antitrust for Patent Pools: A Century of Policy Evolution*, 2004 Stan. Tech. L. Rev. 3, 108 (2004).

35 *See Broadcast Music, Inc. v. Columbia Broadcast System, Inc. et al.*, 441 U.S. 1, 8-16, 20-24 (1979).

36 *See, e.g.*, Philip Goter, *Princo, Patent Pools, and the Risk of Foreclosure: A Framework for Assessing Misuse*, 96 Iowa L. Rev. 699, 711-12 (2011) (mentioning the need for safeguards to enable individual licensing and avoid the inclusion of non-essential patents); *id.* at 731 (noting that the possible justifications for patent pools depend greatly on the facts of the case). The provisions of the Proposed Update on grantbacks suffer from a similar problem. Historically, the Agencies have insisted on safeguards for such grantbacks to avoid them being used for anticompetitive ends. *See* Proposed Update, § 5.6 n.85. And the Proposed Update—properly in our view—recognize that grantbacks involving horizontal competitors may have anticompetitive effects. Proposed Update, § 4.1.2. Yet, the Proposed Update fails to recognize that appropriate safeguards should be present as one precondition to presuming such arrangements to be procompetitive.

37 *Cf., e.g.*, Cheng, *supra* note 28, at 498-506, 508-10 (explaining that a lot of the procompetitive justifications for no challenge clauses to a patent's validity fall away when the firm requiring such a clause has market power).

Resale Price Maintenance. RPM in the licensing scheme context may be anticompetitive when it is an end-run around the important first sale and patent exhaustion doctrines.[38] To apply a full rule of reason inquiry here incentivizes agreements that exceed limits on IP grants without a corresponding economic benefit.[39] At the very least, economic teaching would support viewing RPM as likely leading to anticompetitive effects when it is implemented by upstream by licensor firms having 50 percent or more market share of a relevant market,[40] when it is implemented by a market dominant firm,[41] or when it originates downstream from licensees.[42] And economic teaching would also suggest not only an inquiry into whether there are actual efficiencies that correlate to the market in which the RPM scheme is being implemented,[43] but also whether practical and significantly less restrictive alternatives, such as vertical territorial restrictions,[44] do not exist.[45]

Tying. The courts have found tying to be anticompetitive without the need to show foreclosure.[46] Recent economic scholarship support this findings (i.e. when a firm has market power in the tying product market).[47] The Proposed Update suggests that tying should warrant investigation only under a full rule of reason analysis in which the analysis of the degree of actual foreclosure in the affected markets would be required.[48] This approach, motivated by the view that package licensing of multiple IP rights in a

---

38 *Cf. Kirtsaeng*, 133 S.Ct. at 1363-67 (discussing how the first sale doctrine in the copyright context protects the freedom to resell and how the freedom to resell is important to global trade).

39 *See, e.g.*, Jarad Daniels, *Don't Discount Resale Price Maintenance: The Need for FTC Guidance on the Rule of Reason for RPM Agreements*, 84 Geo. Wash. L. Rev. 182, 213 (2016).

40 *See, e.g.*, Brief for William S. Comanor and Frederic M. Scherer in Support of Neither Party, 2007 WL 173679, *10, *Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877 (2007) (hereinafter "Comanor-Scherer Brief"); *see also* Daniels, *supra* note 39, at 214; Org, for Econ. Coop. & Dev. ("OECD") Policy Roundtables, *Resale Price Maintenance*, DAF/Comp(2008)37, 43, 46-48 (Sept. 10, 2008).

41 *See Leegin Creative Leather Prods., Inc. v. PSKS, Inc.*, 551 U.S. 877, 893-94 (2007); *see also* Daniels, *supra* note 39, at 214 (citing statements of the Agencies); OECD Policy Roundtables, *supra* note 40, at 43, 46-48.

42 Daniels, *supra* note 39, at 213 (citing statements of the Agencies); *see Leegin*, 551 U.S. at 897-98; *see also* Comanor-Scherer Brief, *supra* note 40, at *8-9; OECD Policy Roundtables, *supra* note 40, at 43-44, 46-48.

43 *See* Marina Lao, *Internet Retailing and Free-Riding: A Post-Leegin Analysis*, 14 J. Internet L. 1 (2011).

44 We agree with the discussion in Section 2.3 of the Proposed Update on vertical territorial and field-of-use restrictions associated with vertical licensing agreements.

45 We do understand that new entry as a procompetitive justification for RPM does not raise the same concerns the availability of significantly less restrictive alternatives if evidence is provided that this efficiency is a real one based on market realities. *See, e.g.*, *Leegin*, 551 U.S. at 917-18 (Breyer, J., dissenting); *see also* Daniels, *supra* note 39, at 215 (citing statements of the Agencies).

46 The Supreme Court has held that tying can be *per se* illegal as long as the defendant has market power in the market for the tying product and the tie affects a not insubstantial amount of sales in the tied product. *Jefferson Parish v. Hyde*, 466 U.S. 2, 15-17 (1984).

47 *E.g.*, Einer Elhauge, *Rehabilitating Jefferson Parish: Why Ties Without a Substantial Foreclosure Share Should Not Be Per Se Legal*, 80 Antitrust L.J. 463 (2016); Barack Richman & Steven Usselman, *Elhauge on Tying; Vindicated by History*, 49 Tulsa L. Rev. 689, 693-95, 698-99, 701, 703, 706, 711 (2014); Nicolas Economides, *Tying, bundling, and loyalty/requirement rebates*, *in* Research Handbook of the Economics of Antitrust Law 5 (Einer Elhauge ed., 2012); Einer Elhauge, *Tying, Bundled Discounts, and the Death of the Single Monopoly Profit Theory*, 123 Harv. L. Rev. 397 (2009).

48 Proposed Update, § 5.3.

licensing agreement can be procompetitive "in some circumstances," does not address whether de facto or de jure *coerced* licensing of multiple IP rights, or of IP rights with the use of a product,[49] should be analyzed under the full rule of reason with a required foreclosure inquiry. Such efficiencies can, however, often be achieved by practical and less restrictive *non-coercive* alternatives, as is often the case for patent pool and copyright licensing schemes.[50] The Proposed Update cites to the *Microsoft* decision, which involved a Section 1 (of the Sherman Act) claim of software tying, to support its proposed full rule of reason analysis, including a foreclosure analysis. But *Microsoft* articulates a different standard for a Section 2 (of the Sherman Act) claim involving illegal monopoly maintenance,[51] and its articulation of a special standard for software tying has been rejected by commentators.[52]

Section 2 (Illegal Acquisition or Maintenance of Monopoly). We commend the Agencies for continuing to recognize that special concerns involving IP licensing activities by monopolists, where the IP may be invalid, support causes of action recognized by the courts.[53] We would suggest that the Agencies build on this by also considering whether certain specific conduct might pose higher risks of anticompetitive effects, and a lower likelihood of benefits, than if that conduct involved non-monopolists.[54] Specifically, tying/bundling[55] and exclusionary dealing are likely to have anticompetitive effects

---

49 Tying arrangements condition the sale of one distinct product or service (the "tying product") on the sale of another distinct product or service (the "tied product") or the agreement not to purchase the tied product or service from any other supplier. *See, e.g.*, *Illinois Tool Works*, 547 U.S. at 33-34; *Eastman Kodak*, 504 U.S. at 461-462; *IBM v. United States*, 298 U.S. 131, 135 (1936).

50 *See, e.g.*, *Rehabilitating Jefferson Parish*, *supra* note 47, at 494-95, 515 (characterizing the Court's jurisprudence on tying as imposing a presumption that tying can't be justified because of the likelihood of less restrictive alternatives). We believe it not to be an accident that outside of the franchise context, the only case to have apparently accepted an efficiencies defense to tying—and notably cited by the Proposed Update—is *United States v. Jerrold Electronics Corp.*, 187 F.Supp. 545, 560 (ED. Pa. 1960), *aff'd* 365 U.S. 567 (1961) (per curiam), involving new entry.

51 *Microsoft,* 253 F.3d at 60-62, 64-67, 95-97.

52 *See, e.g.*, Philip Areeda & Herbert Hovenkamp, Antitrust Law, ¶ 1728f2, at 326 (2004).

53 *See* Proposed Update, § 6. The *Walker Process* line of decisions mentioned in this Section require evidence that a patent was secured by fraud as part of a Section 2 claim involving illegal leveraging of a IP right. This is because that doctrine functions as a sword, exposing the monopolist to trebled damages.

54 Conduct committed by a monopolist can be viewed as anticompetitive even when that same conduct might be viewed as procompetitive if committed by a non-monopolist. *See Eastman Kodak Co. v. Image Technical Services.*, 504 U.S. 451, 488-89 (1992) (Scalia, J., dissenting) (discussing tying); *ZF Meritor LLC*, 696 F.3d at 270-71 (discussing exclusive dealing); *cf. Death of the Single Monopoly Profit Theory, supra* note 47, at 436-37 n.104 (the application of the consumer welfare standard to antitrust law does not require the assessment of consumer welfare standards on a case-by-case basis but rather can support rules and standards).

55 Bundling can present competition concerns in this space. *See, e.g.*, Goter, *supra* note 36, at 713-14 (patent pools can be used to foreclose competition with existing patented products or to foreclose competition with licensors in specified markets or fields-of-use).

when a firm has monopoly power in a relevant market.[56] For monopolistic conduct with such special concerns, the Agencies may want to consider stating that procompetitive efficiencies—or the fit between individual restraints and such efficiencies—will not be assumed[57] and that monopolistic licensors should be required to explain how practical, significantly less restrictive alternatives do not support inferences of liability or of their conduct having a net negative competitive effect.[58]

V. *TRINKO* DOES NOT SUPPORT ACCORDING A WIDE SCOPE TO THE RIGHT TO CONDITION ACCESS TO IP NO MATTER THE ANTICOMPETITIVE EFFECTS INVOLVED

The recognized right to try to exclude in an IP grant[59] is distinct from the question of how a firm with market power can condition access to its IP rights. *Actavis* recognized that a patent grant did not allow a branded drug manufacturer to settle on whatever terms it wished with a competing generic drug manufacturer, no matter the anticompetitive effects involved.[60] *Microsoft* similarly recognized that the copyright grant to Microsoft did not allow Microsoft to condition access to its operating system on any act designed to disable competition from rival web browser manufacturers.[61] On a whole range of actions by firms with market power, such as barring challenges to IP rights of questionable validity or scope or discriminating among competitors in affording access, the right to try to exclude may be used to cloak acts having a net anticompetitive impact.[62]

We suggest that the Proposed Update need not view *Trinko* as requiring such an expansive view of how a firm with market power can condition access to its IP rights. *Trinko* rejected a Section 2 claim that competitors be afforded access to a

---

56 *See* C. Scott Hemphill & Tim Wu, *Parallel Exclusion*, 122 YALE L. J. 1182, 1200, 1201-03, 1205-06 (2013); *see also* Michal Gal & Daniel Rubinfeld, *The Hidden Costs of Free Goods: Implications for Antitrust Enforcement,* 80 ANTITRUST L.J. 521, 533-35, 541-42 (2016); *cf. Death of the Single Monopoly Profit Theory, supra* note 47, at 445-47 (explaining that even in the set of very limited circumstances in which tying shouldn't be struck down under Section 1 of the Sherman Act's quasi-*per se* or structured rule of reason theory, it can be struck down as illegal monopolization under Section 2 of the Sherman Act); *id.* at 476 n.50 (noting the position of Areeda and Hovenkamp that foreclosure from exclusionary conduct should be presumed unreasonable when it reaches a total of 50 percent for five or fewer sellers).

57 *See, e.g.*, Brief of Amicus Curiae Frederic Scherer, at 9-10, *Illinois Tool Works, Inc. v. Independent Ink, Inc.*, 547 U.S. 28 (2006) (advocating based on quick look cases, Section 2 cases, and the U.S. Merger Guidelines that burden be placed on defendants to come forward with evidence justifications for tying conduct); *see also In re Cipro Cases I & II*, 348 P.3d at 869-70; C. Scott Hemphill, *Less Restrictive Alternatives in Antitrust Law*, 116 COLUM. L. REV. 927, 983 (2016).

58 *See* Hemphill, *supra* note 57, at 979-83; *see also Jefferson Parish*, 466 U.S. at 266 n.42 (discussing tying); *Fortner Enterprises, Inc. v. U.S. Steel Corp.*, 394 U.S. 495, 503 (1969) (same); *see also* PHILIP AREEDA, EINER ELHAUGE, & HERBERT HOVENKAMP, ANTITRUST LAW, ¶ 1760f at 357 (2d ed. 2004) (same). New entry as a procompetitive justification for tying does not raise the same concerns about fit and the availability of practical, significantly less restrictive alternatives if defendants provide evidence showing that this efficiency is a real one based on market realities. *See* Proposed Update, § 4.2.

59 *See Actavis*, 133 S.Ct. at 2230-31 (recognizing that a valid patent carries with it the right to try to exclude products that are infringing).

60 *Actavis*, 133 S.Ct. at 2230-2233.

61 *Microsoft*, 253 F.3d at 64-67.

62 *Cf. Actavis*, 133 S.Ct. at 2232-33 (discussing overly restrictive patent licensing agreements struck down under the antitrust laws); Cheng, *supra* note 28, at 498-506, 508-10.

telecommunication company's infrastructure because an extensive regulatory scheme had already been put into place governing when and under what circumstances such access must be afforded.[63] *Trinko* did not rule out liability for a firm with market, let alone monopoly, power conditioning access to its IP in a manner that had an anticompetitive effect. And *Trinko* was not seen in *Actavis* as a bar to the Court's holding that the grant of an IP right to a firm with market power did not allow its holder to do whatever it wanted with that right, no matter how anticompetitive, so long as it did not exceed the scope of the IP grant.[64]

VI. CONCLUSION

Protecting innovation and the development of new products and services[65] is important to the continued growth of the United States economy in the 21st century,[66] and IP rights can play a key role in that effort.[67] It is the United States' advantage in innovation that is aiding in the reshoring of manufacturing into the U.S. in a striking reversal of historical trends.[68] The recognition and enforcement of IP rights enables the grant of IP rights to be effective in meeting that goal of furthering innovation and the development of products and services.[69]

But the increased concentration and de facto cartelization of the United States economy raises its own concerns that have called for policies enhancing competition as well as increased enforcement of antitrust laws.[70] IP can't be exempt from these concerns

---

63 *Trinko*, 540 U.S. at 409-11, 415-16.

64 Avoiding reliance on an expansive interpretation of *Trinko* also avoids treating patents as conferring an absolute right to exclude and thereby working an end run around the conditional nature of patent grants.

65 Innovation goes beyond traditional research and development in including the development of new products such as new kinds of entertainment content such as Netflix and Amazon Prime, and new services such as product delivery—see, *e.g.*, Andy Pasztor, *Package-Delivery Drones Likely Years Away from Federal Approval,* Wall St. J. (Sep. 29, 2016).

66 *See, e.g.*, Thomas Nicholas, *What Drives Innovation?* 77 Antitrust L.J. 787 & nn.1-2 (2011) (collecting materials on how innovation "matters for just about everything.").

67 *See, e.g.*, Stephen Haber, *Patents and the Wealth of Nations*, 23 Geo. Mason L. Rev. 811 (2016) (collecting studies and historical analysis); Alden Abbott, *Abuse of Dominance by Patentees: A Pro-Innovation Perspective*, 14 Antitrust Source 1 (Oct. 2014) (same); *but cf.* Nicholas, *supra* note 66 (suggesting that whether IP rights enhance innovation involves a more complex analysis of welfare trade-offs and that antitrust laws should consider the other means by which innovation can be furthered such as prizes).

68 *E.g.,* Jackie Northam, *As Overseas Costs Rise, More U.S. Companies Are 'Reshoring,'* All Things Considered, NPR (Jan. 27, 2014), http://www.npr.org/sections/parallels/2014/01/22/265080779/as-overseas-costs-rise-more-u-s-companies-are-reshoring; *Reshoring Manufacturing: Coming Home, A Growing Number of American Companies Are Moving Their Manufacturing Back to the United States,* The Economist (June 19, 2013); Special Report, TD Economics, *Offshoring, Onshoring, and the Rebirth of American Manufacturing* (Oct. 15, 2012) (report on file with the author).

69 *See, e.g.*, H.R. Rep. No. 113-657, Trade Secrets Protection Act of 2014, pp. 5-6; *see also, e.g., Altavion v. Konka Minolta Sys. Lab., Inc.*, 171 Cal. Rptr. 3d 714, 719, 737 (Cal. App. 2 Dist. 2014); Brief of the California Attorney General as *Amicus Curiae*, *Bunner v. DVDCCA*, 75 P.3d 1 (Cal. 2003); sources cited in note 62 *supra*.

70 *See, e.g.*, Benefits of Competition and Indicators of Market Power, Council of Economic Advisers Issue Brief (Apr. 2016); *Too Much of a Good Thing*, The Economist, 23-28 (Mar. 26, 2016).

as IP does not confer some sort of special exemption in that regard.[71] If cross-border recognition, and enforcement, of IP rights is going to be an inherent component of furthering trade and the growth of exports from the United States,[72] then it is essential to the credibility of such a strategy for the Agencies to be more proactive in recognizing the circumstances under which IP can be used for anticompetitive ends.[73]

71 *See Microsoft*, 253 F.3d. at 63 (finding Microsoft's claim of "absolute and unfettered right to use its intellectual property as it wishes . . . borders upon the frivolous.").

72 *See, e.g.*, Trans-Pacific Partnership Agreement chs. 9 & 18, Aust.-Brunei-Can.-Chile-Japan-Mex.-N.Z-Peru-Sing.-U.S.-Viet., Feb. 4, 2016, U.S. Trade Representative, http://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text.

73 *See, e.g.*, Press Release, U.S. Dep't of Justice, Justice Department Withdraws Report on Antitrust Monopoly Law: Antitrust Division to Apply More Rigorous Standard with Focus on the Impact of Exclusionary Conduct on Consumers (May 11, 2009), https://www.justice.gov/opa/pr/justice-department-withdraws-report-antitrust-monopoly-law.

CALIFORNIA ONLINE PRIVACY LAWS: THE BATTLE FOR PERSONAL DATA

By Jonathan Levine and Heather Haggarty[1]

I. INTRODUCTION

In 2011, the World Economic Forum published a report describing personal data as the new asset class—the "new oil of the Internet and the new currency of the digital world."[2] This is truer now than ever. With technology eliminating barriers to privacy and the demand for data creating both opportunities for economic growth and exploitation, legislatures and courts are scrambling to address privacy concerns in this ever-shifting technological landscape. While most online privacy laws and protections have only been enacted in the last decade, California is leading the way with key statutes to safeguard the privacy rights of individuals and businesses. This article focuses on a handful of these laws. Part II provides an overview of the Comprehensive Computer Data Access & Fraud Act (CDAFA),which prohibits unauthorized access to computer data and systems. Part III focuses on the Customer Records Act (CRA), also referred to as the Database Breach Act or the Breach Act, which protects personal information. Part IV discusses the Consumer Protection Against Computer Spyware Act, which prohibits unauthorized installation of spyware on an individual's computer. Last, the article concludes with a discussion of the California Online Privacy Protection Act (OPPA), which addresses the collection of personal information by operators of commercial websites.

II. COMPREHENSIVE COMPUTER DATA ACCESS & FRAUD ACT[3]

With the intent of providing protection to individuals, businesses and government agencies against unauthorized access and interference with computer data and systems, the CDAFA imposes criminal penalties for knowingly accessing and using a computer, or data from a computer, without permission.[4] A violation of section 502 is punishable as a felony or misdemeanor.[5] The statute also provides for a private right of action.[6]

---

1 Jonathan Levine is a founding partner of Pritzker Levine LLP and a member of the Privacy Law Subcommittee of the Antitrust, UCL and Privacy Section of the State Bar of California. Heather Haggarty is an associate with Pritzker Levine LLP.

2 World Economic Forum, *Personal Data: The Emergence of a New Asset Class* (Feb. 17, 2011) http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

3 Cal. Penal Code § 502.

4 *Facebook v. Grunin*, 77 F. Supp. 3d 965, 971-72 (N.D. Ca. 2015).

5 *People v. Hawkins*, 98 Cal. App. 4th 1428, 1437-38 (2002).

6 Cal. Penal Code § 502(e)(1).

Specifically, a person is guilty if he or she knowingly and without permission:

- Accesses and alters, damages, deletes, destroys or otherwise uses any data, computer, computer system, or computer network in order to either (a) devise or execute any scheme or artifice to defraud, deceive, or extort, or (b) wrongfully control or obtain money, property, or data;
- Accesses and takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;
- Uses or causes to be used computer services;
- Accesses and adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network;
- Disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network;
- Provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section;
- Accesses or causes to be accessed any computer, computer system, or computer network;
- Introduces any computer contaminant (i.e. a virus or worm) into any computer, computer system, or computer network;
- Uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network;
- Disrupts or causes the disruption of government computer services or denies or causes the denial of government computer services to an authorized user of a government computer, computer system, or computer network;
- Accesses and adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a public safety infrastructure computer system computer, computer system, or computer network;
- Disrupts or causes the disruption of public safety infrastructure computer system computer services or denies or causes the denial of computer services to an authorized user of a public safety infrastructure computer system computer, computer system, or computer network;

- Provides or assists in providing a means of accessing a computer, computer system, or public safety infrastructure computer system computer, computer system, or computer network in violation of this section; or

- Introduces any computer virus or worm into any public safety infrastructure computer system computer, computer system, or computer network. [7]

A. Application of "Access"

As discussed below, the California courts' evolving interpretation of "access" which is defined under the CDAFA as "to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network"[8] has broadened the scope and reach of the CDAFA beyond malicious hacking to include unauthorized taking or use of data.

In *People v. Hawkins*, one of the earlier cases to interpret the CDAFA, an employee was charged with violating section 502(c)(2) of the CDAFA[9] after he left his employer to start a competing business and downloaded his entire computer directory from his employer's computer system, which happened to include his employer's proprietary source code.[10] The employee argued that the statute lacked a *mens rea* requirement because "knowingly" only modifies "accesses," and that only knowing access triggers strict liability under the statute.[11] He reasoned that he, therefore, could not be convicted of a felony.[12] The court rejected the employee's argument that the statute creates strict criminal liability, noting that evidence of accidental copying would have negated the mental element of section 502(c)(2).[13]

In *People v. Childs*, an employee was charged under section 502(c)(5)[14] after refusing to provide his employer with the user name and password for his employer's computer network.[15] The employee argued that the charged offense did not apply because the legislative intent of the statute was to address *unauthorized* access to computers and data. He had *authorized* access to his employer's computer network.[16] The court rejected his

---

7 *Id.* §§ 502(c)(1)—502(c)(14).

8 *Id.* § 502(b)(1).

9 Cal. Penal Code § 502(c)(2) ("Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.").

10 *People v. Hawkins*, 98 Cal. App. 4th 1433, 1437 (2002).

11 *Id.* at 1439.

12 *Id.*

13 *Id.*

14 Cal. Penal Code § 502(c)(5) ("Disrupting or causing the disruption of computer services or denying or causes the denial of computer services to an authorized user of a computer, computer system, or computer network for refusing to provide passwords and access codes to a city computer network.").

15 *People v. Childs*, 220 Cal. App. 4th 1079 (2013).

16 *Id.* at 1098-99.

interpretation, reasoning that unauthorized access was an implied element of section 502(c)(5) and that his reliance on the use of "unauthorized access" in subdivision (a) "too narrow."[17] The court found that "[d]isrupting or denying computer services to an authorized user could reasonably be read to fall within 'interference' with computers, even without a showing of unauthorized access."[18] The court further underscored this point, noting that only some of the offenses under section 502(c) mention access and that difference was intentional.[19]

In *United States v. Christensen*, the Ninth Circuit held that "access" included logging into a database with a valid password and subsequently taking, copying, or using information in the database improperly.[20] The court distinguished the CDAFA from the federal Computer Fraud and Abuse Act (CFAA),[21] noting that the CDAFA does not require *unauthorized* access, rather only *knowing* access.[22] Citing *United States v. Nosal*, the court made clear that the CFAA is limited to criminalizing access that is not authorized, rather than use that is unauthorized, and noted that the CFAA was not intended to expand beyond an anti-hacking statute into a misappropriation statute.[23] In contrast, the court held that, under the CDAFA, what is illegal is the taking, copying or use without permission, regardless of whether the individual was authorized to access the information itself.[24]

With *United States v. Christensen* holding that a showing of "unauthorized access" is not required for liability under section 502(c), the CDAFA has effectively become a powerful tool for prosecutors and plaintiffs seeking to impose civil and criminal liability for authorized users who take or copy data without authorization.

B. Application of "Without Permission"

In addition to interpreting what constitutes knowing access, the courts have also weighed in on what it means to act "without permission" under section 502(c). Expanding the definition of "unauthorized" under the CDAFA to include use that is not permitted, the courts, as the cases below highlight, have been forced to grapple with whether finding a website's terms of use are enough to impose liability or whether there must be a higher threshold, such as overcoming technical or code-based barriers, required before finding a defendant liable under the CDAFA.

In *Facebook, Inc. v. ConnectU*, ConnectU obtained login information and passwords that were voluntarily submitted by Facebook users. The information allowed ConnectU

---

17 *Id.* at 1101.

18 *Id.* at 1101-02.

19 *Id.* at 1102. *See also NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 966 (N.D. Cal. 2014).

20 *United States v. Christensen*, 801 F.3d 970, 994 (9th Cir. 2015) (opinion amended and superseded on denial of rehearing *United States v. Christensen*, 828 F.3d 763 (9th Cir. 2015)).

21 *Id.*

22 *Id.*

23 *Id.* at 992.

24 *Id.* at 994.

to access Facebook to gather millions of e-mail addresses for solicitation.[25] ConnectU argued that because the Facebook users voluntarily provided the access information, it did not constitute "unauthorized access." However, because using the email addresses for solicitation was prohibited by a standard clause in Facebook's terms of use, the court denied ConnectU's motion to dismiss, holding that such activity constituted knowing access and use "without permission" under the CDAFA.[26] The court stated that notwithstanding the statutory title "unauthorized access," the violation turns on unauthorized (i.e., "without permission") taking, copying, or use of data.[27] Moreover, the court found that ConnectU was subject to Facebook's terms of use, and disputing ConnectU's contention that this finding would allow private parties to determine what is criminal, the court held that "[t]he fact that private parties are free to set the conditions on which they will grant such permission does not mean that private parties are defining what is criminal and what is not."[28]

It is on this last point in *Facebook v. ConnectU* that the court in *Facebook, Inc. v. Power Ventures, Inc.* disagreed. [29] In *Power Ventures*, defendant Power moved for summary judgment on the basis that Facebook did not have standing to bring a claim under section 502 because it had not made an adequate showing that it had suffered damage or loss within the meaning of the statute.[30] The court rejected this argument finding that defendant admitted that Facebook took steps to block Power's access to the Facebook website.[31] Finding that Facebook had standing to bring suit under section 502, the court also rejected Power's argument that any steps taken were minimal—no more than few mouse clicks and keystrokes—stating that "[s]ection 502 sets no threshold level of damage or loss that must be reached to impart standing to bring suit. Under the plain language of the statute, any amount of damage or loss may be sufficient."[32] Power also argued that it could not have liability under section 502 because there was "no evidence that Power ever accessed the Facebook website without the express permission of the user and rightful owner of the accessed data."[33]

In considering Power's liability under section 502, the court found that the permission given by Facebook users to access Facebook was not a defense since Power's use of "automated devices" (in this case, bots) violated an express term of Facebook's terms of use.[34] The court then looked at the question of whether such a violation of the terms of use constituted "without permission," noting that this is a challenging question because millions of internet users access websites every day without having read

---

25 *Facebook v. ConnectU LLC*, 489 F. Supp. 2d 1087,1091 (N.D. Cal. 2007).

26 *Id.*

27 *Id.*

28 *Id.*

29 *Facebook v. Power Ventures*, No. C 08-05780, 2010 WL 3291750 (N.D. Cal. July 20, 2010).

30 *Id.* at *3.

31 *Id.* at *4.

32 *Id.*

33 *Id.* at *5.

34 *Id.* at *7.

or understood the terms of use.[35] The court disagreed with the holding in *Facebook v. ConnectU*, finding that allowing private parties to set the conditions upon which they will grant permission raises constitutional concerns because it essentially places "in private hands unbridled discretion to determine the scope of criminal liability recognized under the statute."[36] The court went on to find that if private parties' terms of use were used to determine whether "without permission" was established under section 502, internet users would not have adequate notice as to what actions could subject them to criminal liability as the terms of use could be changed at any time.[37] "Thus, in order to avoid rendering the statute constitutionally infirm, the [c]ourt finds that a user of internet services does not access or use a computer, computer network, or website without permission simply because that user violated a contractual term of use."[38] However, the court found that accessing or using a computer, network, or website "in a manner that overcomes technical or code-based barriers" constitutes "without permission," and may subject a user to liability under section 502.[39]

Though many courts have followed the *Power Ventures* court's broader interpretation, this split of authority regarding whether California law imposes a "technical or code-based barrier" requirement on CDAFA claims has not yet been resolved definitively, particularly with regard to the "without permission" language of CDAFA.[40] In *NovelPoster v. Javitch Canfield Group*, the court noted the different interpretations. In holding that plaintiff had alleged sufficient facts to supports its claims under section 502(c) of the CDAFA, the court stated that "the holding in *Power Ventures* is best understood as applying only to those CDAFA provisions which, like the provisions specifically at issue in that case, require a showing of unpermitted access or use, not to section 502(c)(5)."[41] The court also found that alleging that defendants changed the passwords to NovelPoster's accounts, prohibiting plaintiff's access by eliminating that technical barrier, was sufficient at the pleading stage to show that defendant's overcame a technical barrier.[42]

C. Criminal Penalties

Depending on which violation a defendant is convicted under this statute, the defendant can be subject to imprisonment for up to three years and a $10,000 fine.[43]

---

35 *Id.*

36 *Id.* at *8.

37 *Id.* at *11.

38 *Id.*

39 *Id.*

40 *See NovelPoster v. Javitch Canfield Grp.*, 140 F. Supp. 3d 954, 966 (N.D. Cal. 2014); *Loop Al Labs v. Gatti*, 2015 WL 5158639, at *4 (N.D. Cal. Sept. 2, 2015); *Synopsys v. A Top Tech*, No. C13-cv-02965SC, 2013 WL 5770542, at *11 (N.D. Cal. Oct. 24, 2013).

41 *NovelPoster*, 140 F. Supp. 3d at 967.

42 *Id.*

43 Cal. Penal Code § 502(d).

D. Private Right of Action and Damages

In addition to criminal penalties, the statute provides a private right of action for compensatory damages and injunctive relief, or other equitable relief to the owner or lessee of the computer, computer system, computer network, computer program or data who has been damages or had losses as a result the violations described above.[44] The action must be brought within three years of the date of the act complained of, or the date of discovery, whichever is later.[45]

Compensatory damages include any expenditure reasonably and necessarily incurred to verify that computer, computer system, computer network, computer program or data was or was not altered, deleted, or damaged by the access.[46] Unlike the statute's federal counterpart, there is no minimum level of monetary loss.[47] A showing that the plaintiff expended resources to curtail the defendant's access suffices for standing, even where the costs of investigating and responding to unwanted access are nominal.[48]

In addition, the court may award punitive or exemplary damages where it is proved by clear and convincing evidence that a defendant has been guilty of oppression, fraud or malice as defined in section 3294(3) of the Civil Code in willful violation of CDAFA.49 The court may also award reasonable attorneys' fees.[50]

III. CALIFORNIA CUSTOMER RECORDS ACT (CRA) [51]

A. Sections 1798.81 and 1798.81.5—Obligation to Protect Personal Information

The CRA requires businesses that own, license, or maintain personal information about Californians, except those that are subject to certain other information and/or privacy laws,[52] to take reasonable steps to dispose of customer records containing personal information within its control by shredding, erasing or otherwise modifying the information to make it unreadable or indecipherable through any means.[53] In addition, such a business must implement and maintain reasonable security procedures and practices to protect the personal information that a business maintains but does not own or license.[54] "Personal information" refers to user name/email address plus password

---

44 *Id.* § 502(e); *see also Mintz v. Mark Bartelstein and Assocs.*, 906 F. Supp. 2d 1017, 1032 (C.D. Cal. 2012).

45 Cal. Penal Code § 502(e)(5).

46 *Id.* § 502(e).

47 *See Facebook v. Power Ventures*, No. C 08-05780 JW, 2010 WL 3291750, at *4 (July 20, 2010).

48 *Id.*

49 Cal. Penal Code §502(e)(4).

50 *Id.* § 502(e)(2).

51 Cal. Civ. Code § 1798 et. seq. This statute is also referred to as the Database Breach Act or the Breach Act. *See In re Adobe Sys. Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1208 n.3 (N.D. Cal. 2014).

52 *See* Cal. Civ. Code § 1798.81 and §1798.81.5(a) and (b).

53 *Id.* § 1798.81.

54 *Id.* § 1798.81.5(b) and (c).

to access account, or an individual's first name or initial and last name where combined with any of the following, when either the name or the data elements are not encrypted:[55]

- Social security number, driver's license number or California Identification Card number;
- Account number, credit or debit card number along with any required security code, access code, or password giving access to an individual's financial account;
- Medical or health insurance information; or
- Information collected by an automated license plate recognition system.

To sue, plaintiff must be a "customer" which is defined as "an individual who provides personal information to a business *for the purpose of purchasing or leasing a product or obtaining a service* from the business."[56] CRA does not require that notification be given to individuals residing outside of California as they do not have standing[57]

In *In re Adobe Systems Privacy Litigation*, customers whose personal information had been compromised alleged that computer hackers had accessed defendant's servers with the intent to steal customer data, including names, usernames, passwords, e-mail addresses, telephone numbers, mailing addresses, and credit card numbers, that some of the personal information had been successfully decrypted, and that some of the information stolen in the data breach had already surfaced on websites used by the hackers.[58] Defendants asserted that plaintiffs did not have standing to bring a claim based on its alleged violation of section 1798.82 because plaintiffs did not allege that they suffered any particular injury stemming from defendant's failure to reasonably *notify* plaintiffs of the 2013 data breach.[59] The court found that plaintiffs sufficiently alleged concrete and imminent threat of future harm to establish Article III injury-in-fact at the pleadings stage, as necessary to seek class action injunctive relief against defendant pursuant to the CRA provision governing failure to implement reasonable security measures.[60] In holding this, the court noting that some of the stolen data already appeared on the Internet and that "to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact."[61]

---

55 *Id.* § 1798.82(i) (defining "encrypted" as "rendered unusable, unreadable, or indecipherable to an unauthorized person through security technology or methodology generally accepted in the field of information security").

56 *Id.* § 1798.80(c).

57 *See In Re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942 (S.D. Cal. 2012).

58 *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 1207 (N.D. Cal. 2014).

59 *Id.* at 1211.

60 *Id.* at 1216.

61 *Id.* at 1215.

B. Section 1798.82—Breach of Security Obligations

If a person or business that conducts business in California and owns or licenses computerized data that includes personal information experiences a security breach of such information, it is required to notify residents of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized party expediently and without unreasonable delay[62] If the person or business that maintains this computerized data does not own the data that was breached, they must notify the owner or licensee immediately upon discovery.[63]

A notification of security breach must be written in plain language and follow the template outlined by the statute.[64] Notice may be provided by written notification, electronic notice, or under certain conditions substitute notice which includes email notice, conspicuous posting or major statewide media.[65] If the person or business notifying was the source of the breach, it must also offer to provide identity theft prevention and mitigation services at no cost to the person affected for not less than 12 months.[66]

In Sony Gaming Networks and Customer Data Security Breach Litigation, plaintiffs alleged that Sony violated section 1798.82 of CRA by failing to notify plaintiffs of the breach in the most expedient time possible and without unreasonable delay.[67] Plaintiffs sought injunctive relief, attorneys' fees, and economic damages as a result of the violation.[68] Sony moved to dismiss the claim arguing that plaintiffs failed to allege why notice of the breach within the 90–day safe harbor provision set forth in Section 1798.84(d) was unreasonable and how plaintiffs' economic damages flowed from the purported unreasonable delay.[69] The court rejected Sony's safe harbor argument noting that it was inapplicable because it only applies to the sale of information to marketers without disclosure.[70] The court however granted Sony's motion to dismiss the claims seeking economic damages because plaintiffs failed to allege how they were damaged by the ten-day delay.[71]

C. Damages

A plaintiff must allege actual damages because of unreasonable delay in notifying about the breach (and not just the intrusion itself) to recover actual damages.[72]

---

62 Cal. Civ. Code §1798.29(a).

63 *Id.* § 1798.82(b).

64 *Id.* § 1798.82(d)(1).

65 *Id.* § 1798.82(j).

66 *Id.* § 1798.82(d)(2)(G).

67 *In re Sony Gaming Networks and Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 955 (S.D. Cal. 2014).

68 *Id.* at 1009.

69 *Id.*

70 *Id.*

71 *Id.*

72 *Id.*

D. Section 1798.83—Sharing Personal Information with Third Parties

Section 1798.83 of the CRA, coined the "Shine the Light Law," ("STL") regulates the business practice of sharing personal information of customers with third-parties for the purpose of direct marketing."[73] STL does not bar sharing consumer marketing information with third parties.[74] "Rather, it was designed to 'shine the light' on information-sharing practices by requiring businesses to establish a procedure by which the consumer can obtain information about such practices."[75] STL applies to a "covered business" which includes any business with 20 or more full or part-time employees[76] that has an established business relationship with at least one California resident,[77] and has within the immediately preceding calendar year disclosed personal information as defined above to third parties for the purpose of direct marketing.[78, 79]

As described by the court in *Miller v. Hearst Communications, Inc*:

> The STL law allows consumers to make requests to covered businesses for information relating to how they have shared consumer information with third parties during the immediately preceding calendar year. These businesses may respond to consumer requests in two ways. First, they can simply disclose how they have shared consumer information with third parties. Alternatively, they can respond by providing the consumer the "right to prevent disclosure of personal information," in which case the businesses are not required to disclose their actual information sharing practices. To give consumers a central location to send STL inquiries, the law requires that a business "designate [and publicize] a mailing address, electronic mail address, or, if the business chooses to receive requests by telephone

---

73 *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 460 (2013) (internal citations omitted).

74 Cal. Civ. Code § 1798.83(e)(8) ("'Third party' is defined as any business that is a separate legal entity from the business that has an established business relationship with a customer; that has access to a database that is shared among businesses, if the business is authorized to use the database for direct marketing purposes, unless the use of the database is exempt from being considered a disclosure for direct marketing purposes pursuant to subdivision (d).").

75 *Boorstein v. Men's Journal, LLC*, No. CV 12-771 DSF, 2012 WL 2152815, at *1 (C.D. Cal. June 14, 2012).

76 Cal. Civ. Code §1798.83(c)(1).

77 *Id.* § 1798.83(a).

78 *Id.* § 1798.83(e)(2) ("Direct marketing purposes" is defined as "the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes. The sale, rental, exchange, or lease of personal information for consideration to businesses is a direct marketing purpose of the business that sells, rents, exchanges, or obtains consideration for the personal information.").

79 *Id.* § 1798.83(a) ("If the business knows or reasonably should know that the third parties used a customer's personal information for the third parties' direct marketing purposes, that business shall, after the receipt of a written or electronic mail request, or, if the business chooses to receive requests by toll-free telephone or facsimile numbers, a telephone or facsimile request from the customer" provide certain information free of charge. For detailed notice requirements, *see* Cal. Civ. Code § 1798.83(a) and (b).

or facsimile, a toll-free telephone or facsimile number, to which customers may deliver requests." Finally, the law includes a remedy provision, which provides that any consumer who is "injured by a violation" may institute a civil action to recover damages.[80]

Thus in order to comply with section 1798.83 of STL, a business has two options. The business can designate a mailing address, electronic mail address, a toll-free telephone or facsimile number, to which customers may deliver a request for information concerning personal information collected and third parties that received the personal information for the third parties' direct marketing purposes during the preceding calendar year as well as one of the following:

1) Notify all agents and managers who directly supervise employees who regularly have contact with customers of the designated addresses or numbers or the means to obtain those addresses or numbers and instruct those employees that customers who inquire about the business's privacy practices or the business's compliance with Section 1798.83 are to be informed of the designated addresses or numbers or the means to obtain the addresses or numbers;[81]

2) Add a link on the business's homepage to a webpage titled "Your Privacy Rights" or add the words "Your Privacy Rights" to the homepage's link to its privacy policy. "Your Privacy Rights" must be in the same style and font size as the link to the business's privacy policy. If the business does not display a link to its privacy policy on its homepage, or does not have a privacy policy, the words "Your Privacy Rights" must be written in larger type than the surrounding text, or in contrasting type, font or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language. The first page of the link must describe customers' rights pursuant to Section 1798.83 and provide the designated mailing address, e-mail address, as required, or toll-free telephone number or facsimile number, as appropriate. If the business elects to add the words "Your California Privacy Rights" to the home page's link to the business's privacy policy in a manner that complies with this subdivision, and the first page of the link describes a customer' s rights pursuant to this section, and provides the designated mailing address, electronic mailing address, as required, or toll-free telephone or facsimile number, as appropriate, the business need not respond to requests that are not received at one of the designated addresses or numbers; or[82]

3) Make the designated addresses or numbers or means to obtain the designated addresses or numbers readily available upon request of a customer at every place of business in California where the business or its agents regularly have contact with customers.[83]

---

80 *Miller v. Hearst Comm'ns, Inc.*, No. CV 12-0733-GHK (PLAx), 2012 WL 3205241, at *4 (C.D. Cal. Aug. 3, 2013) (internal citations omitted).

81 Cal. Civ. Code §1798.83(b)(1)(A).

82 *Id.* § 1798.83(b)(1)(B).

83 *Id.* § 1798.83(b)(1)(C).

Once the business receives the customer's request, the business must provide all of the following in writing or by electronic mail free of charge within 30 days of a receipt of a request from a customer for information if sent to an address designated by the company, or 150 days if the request is sent to an address not designated by the business:[84]

1) a list of the categories of personal information disclosed by the business to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year; and[85]

2) the names and addresses of third parties that received personal information from the business for the third parties' direct marketing purposes during the preceding calendar year and, if the nature of the third parties' business cannot reasonably be determined from the third parties' name, examples of the products or services marketed, if known to the business, sufficient to give the customer a reasonable indication of the nature of the third parties' business.[86]

A business is not obligated to respond to an information request under STL from the same customer more than once during any calendar year.[87] It's also important to note that some disclosures are considered exempt, including, "the use of personal information (A) by bona fide tax exempt charitable or religious organizations to solicit charitable contributions, (B) to religious organizations to solicit charitable contributions, (C) by a third party when the third party receives personal information solely as a consequence of having obtained for consideration permanent ownership of accounts that might contain personal information, or (D) by a third party when the third party receives personal information solely as a consequence of a single transaction where, as a result of the transaction, personal information has to be disclosed in order to effectuate the transaction."[88]

Alternatively, if a business does not want to share such information in the manner required in section 1798.83(b), it can comply with section 1798.83 by including in its published privacy policy that it will not disclose a customer's personal information to third parties for the third parties' use in direct marketing without the customer's consent (opt-in or opt-out) and then by (1) notifying the customer of his or her right to prevent

---

84 *Id.* § 1798.83(b)(1)(C).

85 *Id.* § 1798.83(a)(1).

86 *Id.* § 1798.83(a)(2).

87 *Id.* § 1798.83(c)(1).

88 *Id.* § 1798.83(e)(2).

disclosure of personal information, and (2) providing the customer with a cost-free means to exercise that right.[89]

Finally, a "safe harbor" is provided to businesses if a business is alleged to have not provided all the information required by Section 1798.83(a) or to have provided inaccurate information or to have not provided the information in a timely manner and its violation is not willful, intentional or reckless.[90] In such a case, the business may assert as a complete defense in any action in law or equity that it thereafter provided the required information to all customers who were provided incomplete or inaccurate information within 90 days of the date the business knew that it had failed to provide as required.[91]

E. Application of STL

In *Boorstein v. Men's Journal, LLC,* the plaintiff alleged that defendant violated STL by failing to properly designate its contact information or provide a description of California consumers' rights under the STL, and as a result defendant's sale of his personal information to third parties decreased the market value of the information, causing him injury.[92] The court rejected his "diminished-value-of-information theory" asserting that defendant's failure to comply did not reduce the value of plaintiff's personal information.[93] The court reasoned that, unlike in established precedent in "information injury" cases in which the plaintiff requested information and was denied, the plaintiff here erroneously argued that it was not necessary for him to make an STL request in order to establish injury.[94] The court also stated that defendant's failure to provide its contact information in order to make an STL request is a procedural injury, not an "informational injury."[95] The court also held that plaintiff's did not establish economic harm by arguing that the value of plaintiff's magazine subscription was reduced by defendant's failure to comply and therefore did not establish statutory injury.[96]

---

89 *Id.* § 1798.83(c)(2) ("If a business that is required to comply with this section adopts and discloses to the public, in its privacy policy, a policy of not disclosing personal information of customers to third parties for the third parties' direct marketing purposes unless the customer first affirmatively agrees to that disclosure, or of not disclosing the personal information of customers to third parties for the third parties' direct marketing purposes if the customer has exercised an option that prevents that information from being disclosed to third parties for those purposes, as long as the business maintains and discloses the policies, the business may comply with subdivision (a) by notifying the customer of his or her right to prevent disclosure of personal information, and providing the customer with a cost-free means to exercise that right.").

90 *Id.* § 1798.84(d).

91 *Id.* § 1798.84(d).

92 *Boorstein v. Men's Journal, LLC*, No. CV 12-771 DSF, 2012 WL 2152815, at *2 (C.D. Cal. June 14, 2012).

93 *Id.* at *3.

94 *Id.*

95 *Id.* at *4.

96 *Id.*

In *Miller v. Hearst Communications, Inc.*, the court applied the same analysis in finding that plaintiff lacked standing to sue.[97] Because the plaintiff's claim of statutory injury rested on the assertion that she was statutorily injured because the defendant violated the STL law by failing to properly designate and publicize on its website a location to send STL inquiries, the court found that she did not allege injury sufficient to meet the statutory requirement.[98] The court concluded that "the STL law's remedy provision requires an 'injury' in conjunction with a violation. Because Plaintiff fails to allege a cognizable injury, she lacks statutory standing for her STL claim, regardless of whether her allegations are sufficient to state a violation of the STL law."[99]

In *Boorstein v. CBS Interactive, Inc.*, the plaintiff alleged that he provided personally identifiable information when he subscribed to a website of defendant's; that defendant had shared personal information with third-parties for direct marketing purposes; and therefore was required to meet the notice requirements under STL which it failed to do.[100] Similar to *Boorstein v. Men's Journal, LLC* and *Miller v. Hearst Comunications, Inc.*, the court found that the plaintiff lacked standing to pursue a claim under section 1798.83 because he failed to plead a statutory injury.[101] The court reasoned that section 1798.84(b) requires that a plaintiff must be a "customer" who has been "injured by a violation of this title" to pursue an action for a violation of section 1798.83 and only then can a plaintiff seek any of the remedies provided by section 1798.84.[102] Simply put, alleging a violation of the statute is not enough.

Further, the court opined that the fact that the statute authorizes penalties per violation would suggest that a statutory "violation" is a discrete event which can quantified.[103] "A failure to timely, accurately, or completely respond to a disclosure request is a discrete event; a court can calculate a civil penalty for each failure by counting the number of disclosure requests to which the defendant did not appropriately respond."[104] The court concluded that a failure to post information on a website is a continuing event which cannot easily be quantified and that "a continuing violation of this kind, without more, is not an actionable 'violation of this title.'"[105] Finally, the court stated that to construe a violation as anything less than a company's failure to provide a timely, complete, and accurate response to disclosure requests would eviscerate the safe harbor intended by section 1798.84(d) and invite a "liability trap" which the legislature sought to avoid.[106] "If we interpret the statute as plaintiff suggests, customers could bring suit whether or not they ever tried to contact a business about its privacy policy.

---

97 *Miller v. Hearst Comm'ns, Inc.*, No. CV 12-0733-GHK (PLAx), 2012 WL 3205241, at *5 (C.D. Cal. Aug. 3, 2013).

98 *Id.* at *6.

99 *Id.* at *7.

100 *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 461 (2013).

101 *Id.* at 467.

102 *Id.*

103 *Id.* at 469.

104 *Id.*

105 *Id.* at 470.

106 *Id.* at 471.

Indeed, if the law is interpreted as plaintiff suggests, a customer who made a request for information and received a timely, complete, and accurate response could still sue for an STL violation by challenging the manner in which the company disclosed its contact information on its Web site."[107]

F. Safe Harbor for Record Custodians

Finding that when records containing personal information are abandoned by a business, they often end up in the possession of a storage company or commercial landlord, the legislature created a safe harbor for such a record custodian who properly disposes of the records as required in section 1798.84(f)(1).[108] Accordingly, section 1798.84(f) states a cause action will not stand against a storage company or personal landlord who has come into possession of records containing personal information that have been disposed of by shredding, erasing or otherwise modifying the personal information in the records thereby rendering it unreadable or indecipherable under any means and abandoned by a business for disposing of records containing personal information.[109]

G. Civil Penalties

If a business fails to comply with the statute, it may be subject to fines from $500 up to $3,000 per violation if the violation is deemed willful.[110] The remedies are cumulative to each other and any rights and remedies available and the court may award attorney's fees.[111]

IV. CALIFORNIA CONSUMER PROTECTION AGAINST COMPUTER SPYWARE ACT[112]

The law prohibits any person that is not the authorized user of a computer to knowingly install software on a user's computer in California without providing that user with a detailed notice of what the software is, how it functions, if and how it collects and uses personal information, and a variety of other information about the software. Though "spyware" is not defined in the statute, a person or entity that is not an authorized user[113] is prohibited from (whether with actual knowledge, intentional avoidance of actual knowledge or willfully) causing computer software to be copied onto the computer of a consumer in this state and using the software to do any of the following through intentionally deceptive means:[114]

- Modify settings related to the computer's access to, or use of, the internet, including the page that appears when an authorized user launches an internet browser or similar software program used to access and navigate the internet; the default

---

107 *Id.*

108 Cal. Civ. Code § 1798.84(f)(2).

109 *Id.* § 1798.84(f)(1).

110 *Id.* § 1798.84(c).

111 *Id.* § 1798.84(c)-(h).

112 Cal. Bus. & Prof. Code § 22947.

113 *Id.* § 22947.1.

114 *Id.* § 22947.2.

provider or web proxy the authorized user uses to access or search the Internet; and the authorized user's list of bookmarks used to access web pages.[115]

- Collect personally identifiable information through any of the following: the use of a keystroke-logging function that records all keystrokes made by an authorized user who uses the computer and transfers that information from the computer to another person; tracking all or substantially all of the websites visited by an authorized user if the computer software was installed in a manner designed to conceal from all authorized users of the computer the fact that the software is being installed; or extracting a data element[116] from the consumer's computer hard drive for a purpose wholly unrelated to any of the purposes of the software or service described to an authorized user.[117]

- Prevent, without the authorization of an authorized user, the authorized user's reasonable efforts to disable or block the installation of software, by causing software that the authorized user has properly removed or disabled to automatically reinstall or reactivate on the computer.[118]

- Intentionally misrepresent that software will be uninstalled or disabled by an authorized user's action, with knowledge that the software will not be so uninstalled or disabled.[119]

- Remove, disable, or render inoperative security, antispyware, or antivirus software installed on the authorized user's computer.

In addition, an unauthorized user[120] shall not (whether with actual knowledge, intentional avoidance of actual knowledge or willfully) cause computer software to be copied onto the computer of a consumer in this state and using the software to do any of the following without the authorized user's permission:[121]

- Take control of the consumer's computer by transmitting or relaying commercial electronic mail or a computer virus from the consumer's computer for the purpose of causing damage to the consumer's computer;[122] accessing or using the consumer's

---

115 *Id.* § 22947.2(a)(1-3).

116 "Data element" is defined in Cal. Civ. Code § 22947.1(k)(2), (3), (4) or (5)(A) or (B).

117 Cal. Civ. Code § 22947.2(b)(1-3).

118 *Id.* § 22947.2(c).

119 *Id.* § 22947.2(d).

120 Exempt from the following prohibitions are "any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, repair, authorized updates of software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software . . . " Cal. Civ. Code § 22947.3(d).

121 *Id.* § 22947.3.

122 *Id.* § 22947.3(a)(1).

modem or internet service for the purpose of causing an authorized user to incur financial charges for a service that is not authorized by an authorized user;[123] using the consumer's computer for the purpose of causing damage to another computer, including, but not limited to, launching a denial of service attack;[124] or opening multiple, sequential, stand-alone advertisements in the consumer's Internet browser without the authorization of an authorized user and with knowledge that a reasonable computer user cannot close the advertisements without turning off the computer or closing the consumer's Internet browser;[125]

- Modify any of the following settings related to the computer's access to, or use of, the Internet: an authorized user's security or other settings that protect information about the authorized user for the purpose of stealing personal information of an authorized user; the security settings of the computer for the purpose of causing damage to one or more computers; or[126]

- Prevent an authorized user's reasonable efforts to block the installation of, or to disable, software, by presenting the authorized user with an option to decline installation of software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds, or by falsely representing that software has been disabled.[127]

Finally, a person or entity,[128] who is not an authorized user shall not do any of the following with regard to the computer of a consumer in this state:

- Induce an authorized user to install a software component onto the computer by intentionally misrepresenting that installing software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content.[129]

- Deceptively cause the copying and execution on the computer of a computer software component with the intent of causing an authorized user to use the component in a way that violates any other provision of this section.

---

123 *Id.* § 22947.3(a)(2).

124 *Id.* § 22947.3(a)(3).

125 *Id.* § 22947.3(a)(4).

126 *Id.* § 22947.3(b)(1-2).

127 *Id.* § 22947.3(c)(1-2).

128 Exempt from the following prohibitions are "any monitoring of, or interaction with, a subscriber's Internet or other network connection or service, or a protected computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, repair, authorized updates of software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing software . . . " Cal. Civ. Code § 22947.4(b).

129 Cal. Civ. Code § 22947.4(a)(1).

One of the few cases to be found interpreting or applying this statute is the marital dissolution case *Vertkin v. Vertkin*[130] in which the court upheld plaintiff's cause of action alleging that defendant installed "keystroke" software on her home and office computers and in doing so, obtained plaintiff's personal financial information.[131]

V. CALIFORNIA ONLINE PRIVACY PROTECTION ACT (OPPA)[132]

OPPA requires any operator[133] of a commercial website or online service that collects personally identifiable information about California residents to conspicuously post its privacy policy and comply with its policy's terms.[134] The term "personally identifiable information" means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form including: a first and last name, a home or other physical address, including street name and name of a city or town, an e-mail address, a telephone number, a social security number, any other identifier that permits the physical or online contacting of a specific individual, or information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.[135]

In addition to mandating conspicuous posting of the operator's privacy policy, the statute also requires that the following be included in a privacy policy:[136]

- the categories of personally identifiable information that the operator collects through the website or online service about its users and/or visitors;[137]
- any third parties that the operator may share the personally identifiable information;[138]
- a description of the process for a user or visitor to review and request changes to his or her personally identifiable information collected through the site or service, if the operator maintains such a process;[139]

---

130 *Vertkin v. Vertkin*, 2007 WL 4287512, No. 07-4471 SC (N.D. Cal Dec. 6, 2007).

131 *Id.*

132 CAL. BUS. & PROF. CODE 22575 (2003).

133 "Operator" is defined as "any person or entity that owns a Web site located on the Internet or an online service that collects and maintains personally identifiable information from a consumer residing in California who uses or visits the Web site or online service if the Web site or online service is operated for commercial purposes. It does not include any third party that operates, hosts, or manages, but does not own, a Web site or online service on the owner's behalf or by processing information on behalf of the owner." CAL. CIV. CODE § 22577(c).

134 *Id.* § 22947.4(a)(1).

135 *Id.* § 22577(a).

136 *Id.* § 22575(b).

137 *Id.* § 22575(b)(1).

138 *Id.*

139 *Id.* § 22575(b)(3).

- a description of the process for notifying users and visitors of material changes to the privacy policy;[140]

- an effective date of the privacy policy;[141]

- a disclosure as to how the operator responds to web browser "do not track" signals or other mechanisms that allow consumers to exercise choice regarding the collection of personally identifiable information about an individual consumer's online activities over time and across third-party websites or online services if the operator engages in that type of collection;[142] and

- a disclosure as to whether other parties may collect personally identifiable information about an individual consumer's online activities over time and across different websites when a consumer uses the operator's website or service.[143]

Under CalOPPA, any of the following would suffice to meet the requirement that the operator's privacy policy be "conspicuously posted":

- displayed on the websites homepage or first significant page after entering the website;[144]

- an icon that hyperlinks to a web page on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the Web site, and if the icon contains the word "privacy." The icon shall also use a color that contrasts with the background color of the Web page or is otherwise distinguishable;[145]

- a text link that hyperlinks to a Web page on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the Web site, and if the text link does one of the following: includes the word "privacy," is written in capital letters equal to or greater in size than the surrounding text, is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language, any other functional hyperlink that is so displayed that a reasonable person would notice it, and in the case of an online service, any other reasonably accessible means of making the privacy policy available for consumers of the online service;[146]

---

140 *Id.*

141 *Id.* § 22575(b)(4).

142 *Id.* § 22575(b)(5); an operator may satisfy this requirement by providing " a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the consumer that choice." *Id.* 22575(b)(7).

143 Cal. Civ. Code § 22575(b)(6).

144 *Id.* § 22576(b)(1).

145 *Id.* § 22576(b)(2).

146 *Id.* § 22576(b)(3)(A-C).

- any other functional hyperlink that is displayed such that a reasonable person would notice it;[147] or

- any other reasonably accessible means of making the privacy policy available for consumers of online service.

A. Failure to Comply

If an operator receives notice of non-compliance for failure to post its privacy policy, to post it conspicuously, the operator has a 30-day grace period to comply. An operator shall be in violation of this section if the operator fails to comply with the provisions of section 22575 or with the provisions of its posted privacy policy in either of the following ways: knowingly and willfully or negligently and materially.[148] Hence, an operator who negligently is in material noncompliance with OPPA or with the terms of its privacy policy has violated OPPA. Thus, a non-material (i.e., trivial) but deliberate breach can be a basis for liability, as can minor technical defects in the posting or the contents of a privacy policy.

B. Application

There is almost no California case law applying this statute.[149] One court in holding that the federal Airline Deregulation Act of 1978 preemption provision barred state enforcement of OPPA provided a detailed analysis of the legislative intent of OPPA and noted that OPAA does not provide for a private right of action or public prosecution for violation of any of its provisions.[150]

VI. CONCLUSION

California digital privacy laws have begun to expand the protections afforded to individuals and businesses by establishing a legal framework that sets important standards for the gathering of and use of personal information and by imposing civil and criminal penalties for violations of these laws. As demand for data continues to grow in our post-industrial society, the courts and legislature will no doubt continue to have to navigate the murky waters of privacy, technology and economic demands.

---

147 *Id.* § 22576(b)(4).

148 *Id.* § 22576.

149 Two cases mention OPPA. *See In re Adobe Sys. Inc. Privacy Litig.*, 66 F. Supp. 3d 11973 (2014); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429 (N.D. Cal. April 1, 2015).

150 *People ex rel. Harris v. Delta Air Lines, Inc.,* 247 Cal. App. 4th 884, 888-90 (2016).

FTC PRIVACY AND DATA SECURITY ENFORCEMENT AND GUIDANCE UNDER SECTION 5

By Alexander E. Reicher and Yan Fang[1]

I. INTRODUCTION

Section 5 of the FTC Act does not itself mention privacy or data security, yet it is the legal basis for well over a hundred Federal Trade Commission privacy and data security enforcement actions. The Commission has used the broad language of Section 5—which prohibits "unfair or deceptive acts or practices," among other things—to hold individuals and companies accountable for everything from broken privacy and data security promises to "unfair" collection of personal information. To better understand the contours of the FTC's privacy and data security enforcement under Section 5, this article examines the agency's litigated cases, public settlements, and guidance materials. This article's modest purpose is to serve as an introduction to some of those materials. It proceeds in four sections. The balance of Section I provides an overview of FTC privacy and data security enforcement and guidance. Section II addresses FTC privacy enforcement and guidance under Section 5, including the agency's early privacy actions and those involving social networks, internet tracking, browser toolbars, cookies and behavioral advertising, mobile devices, data brokers, and the misappropriation of consumer data. Section III discusses FTC data security enforcement and guidance under Section 5, including the agency's recent data security litigation and enforcement actions that help define "reasonable" data security. The article concludes in Section IV.

A. Enforcement

In its privacy and data security actions, the Commission has used its Section 5 authority to investigate and file complaints against companies and individuals for privacy and data security violations that are "deceptive," "unfair," or both. Section 5 of the FTC Act states, in relevant part, that the Commission is "empowered and directed to prevent persons, partnerships, or corporations"—excluding certain types of entities, such as banks and credit unions, as well as certain activities such as common carrier activities—"from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[2]

A deceptive act or practice under the FTC Act is (1) a representation, omission, or practice (2) that is likely to mislead consumers acting reasonably in the circumstances and

---

1 Alexander E. Reicher is an associate with Latham & Watkins LLP and served as an attorney in the Federal Trade Commission's Western Regional Office in San Francisco from 2015 to 2016. Yan Fang is a Ph.D. student in the Jurisprudence and Social Policy Program at the University of California, Berkeley. She previously served as an attorney in the Federal Trade Commission's Western Regional Office in San Francisco from 2013 to 2016. The authors thank Thomas Dahdouh for his comments on an earlier version of this article. The views expressed in this article are solely those of the authors.

2 15 U.S.C. § 45(a)(2) (2012).

(3) that is material.[3] An unfair act or practice is one that (1) causes or is likely to cause substantial injury to consumers, (2) is not reasonably avoidable by consumers, and (3) is not outweighed by countervailing benefits to consumers or to competition.[4] Though early privacy and data security cases focused on deception, the FTC has increasingly used its unfairness authority to bring cases in the areas of privacy and data security.[5]

In addition to the FTC Act, the FTC also enforces a number of other privacy and data security laws, including the following (among others):

- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)[6] and the corresponding CAN-SPAM Rule;[7]
- Fair Credit Reporting Act (FCRA)[8] and a number of corresponding rules;
- Gramm-Leach-Bliley Act (GLBA)[9] and the corresponding Privacy of Consumer Financial Information Rule (Financial Privacy Rule)[10] and Standards for Safeguarding Customer Information (Safeguards Rule);[11] and
- The Children's Online Privacy Protection Act (COPPA)[12] and the corresponding Children's Online Privacy Protection Rule.[13]

The FTC investigates companies and individuals whose conduct may violate Section 5 or a specific statute or rule that the agency enforces. In privacy and data security investigations, the Commission has the authority to issue civil investigative demands (CIDs) for documents, interrogatory responses, and "tangible things," and to compel individuals and companies to attend investigational hearings, which are similar to depositions.[14]

FTC investigations may lead to one of several outcomes: (1) the agency's decision to close the investigation, (2) a settlement between the FTC and the target of the investigation, (3) the agency's filing of an administrative complaint, or (4) the agency's

---

3 Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, House Comm. on Energy & Commerce 1-2 (Oct. 14, 1983), *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

4 15 U.S.C. § 45(n); *see also* Letter from FTC Comm'rs to Sen. Wendell H. Ford & Sen. John C. Danforth (Dec. 17, 1980), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

5 *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 599 (2014).

6 15 U.S.C §§ 7701-7713.

7 16 C.F.R. § 316.

8 15 U.S.C. §§ 1681-1681x.

9 15 U.S.C. §§ 6801-6809 and 6821-6827.

10 16 C.F.R. § 313.

11 16 C.F.R. § 314.

12 15 U.S.C. §§ 6501-6506.

13 16 C.F.R. § 312.

14 15 U.S.C. § 57b-1.

filing of a complaint in federal district court. The Commission has resolved the majority of its publicly announced privacy and data security investigations through consent order settlements, but more recently, has filed three complaints, one in federal court and two before its administrative tribunal.

B. Guidance

In addition to enforcement, the Commission has issued a number of reports and guides for businesses on privacy and data security topics. These guidance documents, written by FTC staff and occasionally approved by the FTC's commissioners, outline how to comply with various privacy laws or present the Commission's view of industry best practices.

The Commission's 2012 report *Protecting Consumer Privacy in an Era of Rapid Change*[15] (hereinafter "*Protecting Consumer Privacy*") is among the more significant FTC guidance on privacy and data security matters. Approved by the FTC's commissioners in a 3-1 vote, *Protecting Consumer Privacy* offers a framework "intended to articulate best practices for companies that collect and use consumer data."[16]

The report's privacy framework centers around three principles. First, "[c]ompanies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services"—so-called "privacy by design."[17] Second, "[c]ompanies should simplify consumer choice" when it comes to choices about a company's collection and use of consumer data.[18] Finally, "[c]ompanies should increase the transparency of their data practice."[19] While the report makes specific recommendations under each of these privacy principles, the Commission clarified that these recommendations may go beyond the existing requirements under the privacy laws.[20]

The report also offers guidance on data security, including the recommendation that companies approach privacy by design by creating substantive and procedural protections. Substantive protections center on reasonableness, including reasonableness in the collection and use of data, in its retention and disposal, and in its security.[21] Procedural protections focus on integrating substantive privacy protections into an organization's everyday practices.[22]

---

15 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

16 *Id.* at 1.

17 *Id.* at 22.

18 *Id.* at 35.

19 *Id.* at 60.

20 *Id.* at iii.

21 *Id.* at 23-30.

22 *Id.* at 30-32.

C. Personally Identifiable Information and Sensitive Personal Information

Though some of the Commission's settlements define personally identifiable information or PII,[23] the agency acknowledged in its 2012 *Protecting Consumer Privacy* report that "the traditional distinction between PII and non-PII has blurred" and suggested that "it is appropriate to more comprehensively examine data to determine the data's privacy implications."[24] In that report, the Commission stated that its privacy framework applies to "consumer data that can be reasonably linked to a specific consumer, computer, or other device" rather than to particular categories of PII.[25]

For both privacy and data security, the FTC has stated that it expects businesses to pay particular attention to protecting "sensitive personal information," which it has defined, "at a minimum," as data about children, financial and health information, Social Security numbers, and precise geolocation data.[26] Some of the privacy and data security statutes and rules enforced by the agency also provide specific definitions of protected information. For example, the Children's Online Privacy Protection Rule applies to online contact information, screen names, certain geolocation information, and "persistent identifiers," which can be used to recognize a user over time and across different online services.[27] In recent reports, the FTC has also highlighted that biometric data[28] and data collected through the "Internet of Things"[29] may pose heightened privacy and physical safety concerns.

* * *

---

23 *See, e.g., In re Geocities*, 127 F.T.C. 94, 122 (1999) (decision and order) (defining "Personal identifying information" as information that includes but is not limited to "first and last name, home or other physical address (e.g., school), e-mail address, telephone number, or any information that identifies a specific individual, or any information which when tied to the above becomes identifiable to a specific individual."); *In re Eli Lilly & Co.*, 133 F.T.C. 763, 783 (2002) (decision and order) (defining "Personally identifiable information" and "personal information" as "individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number; (f) an Internet Protocol (IP) address or host name that identifies an individual consumer; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) or any information that is combined with (a) through (g) above" with certain exceptions.).

24 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 19 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

25 *Id.* at 22.

26 *Id.* at 47 n.214, 59.

27 16 C.F.R. § 312.2.

28 Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies iii, 8, 20 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

29 Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 12-13, 30, 50 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

The following sections—"FTC Privacy Enforcement and Guidance Under Section 5" and "FTC Data Security Enforcement and Guidance Under Section 5"—focus on the Commission's actions brought under Section 5 of the FTC Act.

II. FTC PRIVACY ENFORCEMENT AND GUIDANCE UNDER SECTION 5

A. Early FTC Privacy Cases under Section 5

The FTC has been a privacy enforcer for over forty years, beginning with its first case under the FCRA in 1972.[30] As consumer privacy issues moved online, the agency began bringing cases against internet and software companies toward the very end of the 1990s and the early 2000s. This section discusses some of the agency's early privacy cases brought under Section 5 of the FTC Act. Two of these early cases, *In re Geocities* and *In re Microsoft Corporation*, focused on the companies' alleged misrepresentations in privacy policies and elsewhere concerning the purpose or scope of the data collected. The final case in this section, *In re Gateway Learning Corp.*, involved both unfairness and deception counts relating to the company's privacy policy changes.

1. GeoCities

The FTC's 1999 settlement with the web host GeoCities was the agency's first public settlement in the area of internet privacy. GeoCities' members, known as "homesteaders," totaled more than 1.8 million, approximately 200,000 of whom were minors between the ages of three and fifteen.[31] The site was one of the top ten most visited websites at the time.[32] To become a homesteader, all users, including children, were required to complete GeoCities' "New Member Application" form, which required certain information (first and last name, zip code, email address, gender, date of birth, and member name) and solicited, but did not require, other personal information (education level, income, marital status, occupation, and interests).[33]

The Commission alleged that GeoCities deceived consumers, including children, about the purpose of its collection of personal information. Geocities' privacy statements in its New Member Application form and elsewhere indicated that the company would only use the personal information to provide GeoCities members with email ads and product services the members requested.[34] The company also represented that it would only use the optional information it collected "to gain a better understanding of who is visiting GeoCities."[35] The FTC alleged that these privacy representations were false

---

30 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers A-3 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

31 *In re Geocities*, 127 F.T.C. 94, 95 (1999) (complaint).

32 *Id.*

33 *Id.* at 96-97.

34 *Id.* at 97.

35 *Id.*

or misleading because GeoCities shared with advertisers the personal information it collected, including information the company collected from children.[36]

GeoCities also operated an online community for children called GeoKidz Club.[37] GeoCities collected children's information through a sign-up form for the GeoKidz Club and through contest sign-ups.[38] GeoCities represented, the FTC alleged, that GeoCities—not a third party—was the entity collecting children's personal information submitted.[39] The FTC alleged that this representation was deceptive because third parties operated the GeoKidz Club and collected and maintained the children's personal information submitted through the GeoKidz Club membership form.[40] The order settling the case prohibits Geocities from making any misrepresentation about its collection or use of personally identifying information, or about the identity of the party collecting such information, among other things.[41]

2. Microsoft Passport

The FTC's action against Microsoft represents another early case in which the agency alleged that statements in a company's privacy policy were deceptive in violation of Section 5 of the FTC Act. In 1999, Microsoft launched its Passport and Passport Wallet online authentication and wallet services.[42] Passport's privacy policy contained a detailed description of the information the service purportedly collected from and about its users.[43] The policy further stated that Passport participated in the TRUSTe Privacy Program and, as such, users should "expect to be notified of [w]hat personally identifiable information . . . is collected" from them.[44]

Microsoft also offered a children's version of its Passport service called Kids Passport. Microsoft said that Kids Passport would "help[] [parents] conveniently protect and control [their] children's online privacy."[45] The Commission alleged that Microsoft made other statements to the same effect.[46]

The FTC alleged that Microsoft collected personally identifiable information other than that described in the Passport privacy policy, including information about the sites

---

36 *Id.* at 97-98.

37 *Id.* at 98-99.

38 *Id.*

39 *Id.* at 99.

40 *Id.; see also id.* at 122 (defining "Personal identifying information" as information that includes but is not limited to "first and last name, home or other physical address (e.g., school), e-mail address, telephone number, or any information that identifies a specific individual, or any information which when tied to the above becomes identifiable to a specific individual").

41 *Id.* at 123 (1999) (decision and order).

42 *In re Microsoft Corp.*, 134 F.T.C. 709, 710 (2002) (complaint).

43 *Id.* at 714.

44 *Id.*

45 *Id.* at 715.

46 *Id.* at 715-17.

that Passport users signed in to.[47] The Commission also alleged that Microsoft Kids Passport service falsely represented that parents would have control over their children's information.[48] For example, according to the FTC, children could edit their personal information and change account settings set by the parent.[49] Microsoft purportedly also failed to adequately inform parents that some websites outside of the Kids Passport service would have received their children's information.[50] The FTC's complaint also included two counts alleging that Microsoft's representations about Passport's security were false and misleading.[51] In the FTC's settlement with Microsoft, the Commission required the company to, among other things, establish a comprehensive information security program.[52]

3. Gateway

In *In re Gateway Learning Corp.*, another early FTC privacy settlement, the agency focused on a company's changes to its privacy policy. Gateway Learning Corp., the makers of the popular "Hooked on Phonics" learning program, marketed its products through its website, which collected various types of personal information about parents and children in connection with purchases of the company's products.[53]

The company's privacy policy initially stated that Gateway would not "sell, rent or loan" any PII to third parties, and promised to notify consumers online and by email of any "material change" to the policy.[54] Its privacy policy also stated that it would not share information about children under the age of 13 "for any purpose whatsoever."[55] Nevertheless, the FTC alleged, Gateway began renting PII provided by its customers to third party marketers.[56] Gateway subsequently changed its privacy policy to state: "From time to time, we may provide your name, address and phone number (not your e-mail address) to reputable companies whose products or services you may find of interest."[57] The Company did not notify consumers by email of this change.[58]

In its 2004 complaint, the Commission alleged that, contrary to representations in the company's privacy policy, Gateway Learning rented consumers' personal information to third-party marketers without their consent.[59] The company also rented information about children under the age of thirteen, contrary to statements in their privacy policy

---

47 *Id.* at 714-15.

48 *Id.* at 715-17.

49 *Id.* at 717.

50 *Id.*

51 *Id.* at 711-13.

52 *In re Microsoft Corp.*, 134 F.T.C. 709 , 742-43 (2002) (decision and order).

53 *In re Gateway Learning Corp.*, 138 F.T.C. 443, 444 (2004). (complaint).

54 *Id.* at 445.

55 *Id.* at 444-45.

56 *Id.* at 446.

57 *Id.*

58 *Id.* at 447.

59 *Id.* at 449.

that Gateway Learning would not share such information with any third party "for any purpose whatsoever."[60]

The FTC finally alleged an unfairness and a deception count relating to Gateway Learning's change in its privacy policy.[61] The Commission's unfairness count stated that Gateway's "retroactive application of its revised privacy policy caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by the consumer."[62] The Commission's deception count targeted the same privacy policy change, but was based on the company's representation that it would notify consumers of material changes to its privacy policy—which Gateway failed to do.[63]

As part of the settlement, the FTC ordered Gateway to pay $4,608 in redress, which is approximately the amount Gateway earned from the rental of consumers' information collected during the period when Gateway's privacy policy promised not to sell, rent, or loan PII.[64]

B. Social Networks

The FTC's settlements with Google (relating to its Buzz social network) and Facebook represent significant actions that touched on special issues that accompanied the emergence of social networks. In those cases, and in the agency's settlement with Myspace (another social network), the consent orders require the companies to establish "comprehensive privacy program[s]" which require, among other things, designated employees to coordinate the program, a privacy risk assessment, and controls and procedures to identify the risks identified in the risk assessment.[65] This section discusses the agency's complaints against and settlements with Google and Facebook. Both of these cases involved the allegedly unexpected disclosure of previously private information, which the Commission has characterized as a key type of privacy harm.[66]

1. Google Buzz

In early 2010, Google launched the Google Buzz social network within its Gmail product. Buzz was a social network that allowed users to post updates, comments, photos,

---

60 *Id.*

61 *Id.* at 449-50.

62 *Id.* at 449.

63 *Id.* at 450.

64 *In re Gateway Learning Corp.*, 138 F.T.C. 443, 470 (2004) (decision and order).

65 *In re Google Inc.*, 152 F.T.C. 435, 454-55 (Oct. 13, 2011) (decision and order); *In re Myspace LLC*, 2012 WL 4101790, *18 (Aug. 30, 2012) (decision and order); Decision and Order at 5-6, *In re Facebook, Inc.*, No. C-4365 (Aug. 10, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

66 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 8 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

and videos.[67] Buzz users could "follow" and, in turn, be "followed" by other Buzz users.[68] On the day Buzz launched, Gmail users were shown a prompt that purported to allow them to accept or reject enrollment in Buzz.[69] Users who declined to enroll could still be "followed" on Buzz.[70] Users who did enroll were automatically set to follow the Gmail contacts they emailed and chatted with most frequently.[71] Some users complained that these auto-generated lists included "individuals against whom they had obtained restraining orders; abusive ex-husbands; clients of mental health professionals; clients of attorneys; children; and recruiters they had emailed regarding job leads."[72] In some cases, these auto-generated lists were posted on a user's public profile.[73]

Gmail's privacy policy at the time stated that, "Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you."[74] Google's Privacy Policy, which applied to all Google products including Gmail, also stated that "[w]hen you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."[75]

The FTC's complaint alleged two deception counts based on representations in the privacy policies. The Commission alleged that Google used Gmail users' information for purposes other than providing those users with an email service, contrary to representations in the Gmail privacy policy.[76] Specifically, Buzz used Gmail users' contacts to populate its Buzz social network.[77] The FTC's complaint further alleged that Google's failure to seek Gmail users' consent before using their information in this way also contravened the Gmail privacy policy.[78]

The FTC's complaint also alleged a deception count based on options presented to Gmail users to decline enrollment or turn off Buzz. The Commission alleged that users who clicked on these options were still enrolled in certain Buzz features.[79]

The complaint also alleged that Google's offering certain controls that appeared to indicate user control over what information would be made public in their Google public

---

67 *In re Google Inc.*, 152 F.T.C. 435 , 437 (Oct. 13, 2011) (complaint).

68 *Id.*

69 *Id.* at 437-38.

70 *Id.* at 438.

71 *Id.* at 438-39.

72 *Id.* at 441.

73 *Id.* at 439-40.

74 *Id.* at 437.

75 *Id.*

76 *Id.* at 442.

77 *Id.*

78 *Id.*

79 *Id.* at 442-43.

profile was deceptive because in most instances a Gmail users' frequent contacts were made public by default.[80]

Finally, the complaint alleged that Google's self-certification to the Department of Commerce that the company complied with the U.S.-EU Safe Harbor privacy principles and statements in its privacy policy that it adheres to those principles constitute deceptive acts or practices because Google failed to give Gmail users notice and choice at the launch of Buzz.[81]

The Commission's settlement with Google prohibits the company from, among other things, misrepresenting the extent to which it maintains and protects of the privacy of any information Google collects from or about any individual.[82] The consent decree also requires Google to establish a "comprehensive privacy program" and undergo biennial privacy assessments.[83]

2. Facebook

The same year as the FTC's Buzz settlement, the agency also settled privacy-related claims with Facebook. The Commission's eight-count complaint addressed a number of Facebook's information practices at the time, including those related to Facebook's "platform apps" and changes to its 2009 privacy policy.

a. Facebook Platform Apps

The Commission alleged that, through the "Profile Privacy Settings" page, Facebook falsely represented that users could restrict access to their profile information to certain groups (such as Friends or Friends of Friends).[84] In fact, the Commission alleged, applications that a user's friends used on the Facebook platform could access information a user restricted to Friends or Friends of Friends.[85]

The FTC also alleged that platform apps could access far more information than Facebook claimed they could. The Commission alleged, for example, that "a quiz [app] regarding a television show, in many instances could access a user's Relationship Status, as well as the URL for every photo and video that the user had uploaded to Facebook's web site."[86] This kind of access to user information exceeded Facebook's representation that apps would only access profile information they needed to operate, the Commission's complaint alleged.[87]

---

80 *Id.* at 443.

81 *Id.* at 444-45.

82 *Id.* at 453.

83 *Id.* at 454-55.

84 Complaint ¶¶ 10-13, 17, *In re Facebook, Inc.*, No. C-4365 (July 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmpt.pdf.

85 *Id.* ¶¶ 14, 18.

86 *Id.* ¶ 31.

87 *Id.* ¶ 32.

b. 2009 Privacy Policy Changes

The FTC also alleged a deception and an unfairness count relating to Facebook's late 2009 changes to its privacy practices and privacy policy. Specifically, the company made public certain types of information (such as a user's name, profile picture, and friends list) that Facebook users had previously provided the company. The FTC alleged that this change was contrary to Facebook's statements that these changes provided users with "more control" over their information.[88] The FTC also alleged that "Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers."[89]

c. Other Counts and Settlement

The Commission alleged a number of other counts in its complaint against Facebook. The agency charged that the company falsely represented that it would not provide advertisers with information about its users,[90] misrepresented that apps it designated "Verified Applications" met a higher standard of security than other apps,[91] misled consumers as to the effect of deleting or deactivating their Facebook accounts,[92] and failed to adhere to the U.S.-EU Safe Harbor notice and choice privacy principles.[93] Facebook's settlement with the Commission requires, among other things, that the company establish a comprehensive privacy program and undergo biennial assessments by a third-party privacy professional.[94]

C. Tracking Internet Activities

The privacy risks associated with the ever-evolving landscape of internet tracking has been a significant focus of the FTC's enforcement efforts. This section discusses the agency's actions against companies that used browser toolbars, cookies, and other technologies to track consumers' activities. In the case of browser toolbars and tracking applications, the Commission targeted misrepresentations or failures to adequately disclose the scope of the data collected by the browser add-on. In the case of browser cookies and similar browsing tracking technologies, the agency focused on practices that make it more difficult for users to opt out of tracking.

1. Browser Toolbars and Tracking Applications

a. Sears

In 2009, the FTC settled with Sears Holdings Management Corporation, a subsidiary that provides marketing operations to the well-known Sears Roebuck and

---

88 *Id.* ¶¶ 27-28.

89 *Id.*¶ 29.

90 *Id.* ¶¶ 34-42.

91 *Id.* ¶ 43-49.

92 *Id.* ¶¶ 50-55.

93 *Id.* ¶¶ 56-63.

94 Decision and Order at 5-7, *In re Facebook, Inc.*, No. C-4365 (F.T.C. July 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

Kmart department stores and operates sears.com and kmart.com.[95] Sears rolled out an application as part of its "My SHC Community" market research program that, when installed, allegedly tracked nearly all of a user's internet behavior and certain other activities on a user's computer.[96] Users received $10 to keep the tracking application on their computers for at least a month.[97]

To sign up for the My SHC Community, Sears required users to complete a registration page. At the bottom of the registration page, the company displayed a "Privacy Statement and User License Agreement" in a scroll box that displayed only ten lines of text at a time.[98] On the seventy-fifth line of that document, Sears described the types of information the My SHC Community application would collect, including a user's application usage information, "the pace and style with which [the user] enter[ed] information online" and, possibly a user's username, password, credit card and account numbers.[99]

The FTC alleged that this disclosure was not enough. The sole count in the FTC's complaint against Sears alleged that the company failed to disclose adequately that its application would:

- "monitor nearly all of the Internet behavior that occurs on consumers' computers, including information exchanged between consumers and websites other than those owned, operated, or affiliated with [Sears], information provided in secure sessions when interacting with third-party websites, shopping carts, and online accounts, and headers of web-based email";[100]
- "track certain non-Internet-related activities taking place on those computers";[101] and
- "transmit nearly all the monitored information (excluding selected categories of filtered information) to [Sears'] remote computer servers."[102]

Sears' settlement with the FTC requires, among other things, that the company "[c]learly and prominently" display—on a "separate screen" from any privacy policy or license agreement—the types of data Sears will monitor or collect through its tracking applications, how that data will be used, and whether that data will be transmitted to

---

95 Complaint ¶ 1, *In re Sears Holdings Mgmt. Corp,* No. C-4264 (F.T.C. Aug. 31. 2009), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

96 *Id.* ¶¶ 4, 13.

97 *Id.* ¶ 6.

98 *Id.* ¶ 8.

99 *Id.* ¶ 8.

100 *Id.* ¶ 13.

101 *Id.*

102 *Id.*

a third party.[103] The settlement also requires Sears to obtain express consent to the application's data collection.[104]

More recently, the Commission settled with a medical billing services company and its former CEO that, similar to Sears, made important disclosures that a user would only see after scrolling down in text boxes that only showed six lines of text at a time.[105]

b. Upromise

Like *In re Sears Holdings Management Corp.*, the Commission's 2013 settlement with Upromise, Inc. involved an alleged failure to disclose the extent to which the company's tracking application would collect and transmit data. Upromise runs a membership program that rewards its members for purchasing products and services from partner merchants by depositing money into a college savings account.[106] In 2005, Upromise began offering a browser toolbar with an option to receive "personalized offers," which the company said would collect information about a users' browsing history in order to "provide college savings opportunities."[107]

According to the FTC complaint, Upromise failed to disclose that it would collect and transmit extensive information about users' online activities, including, for a period of time, information such as credit card numbers, security codes, card expiration dates, and Social Security numbers.[108] The FTC complaint also alleged that Upromise falsely represented that information collected by the Toolbar would be encrypted in transit and that reasonable measures were employed to protect consumer data from unauthorized access.[109] The agency also alleged that this failure to employ reasonable security methods to protect consumers' information was unfair.[110] The FTC's settlement with Upromise required the company to, among other things, notify customers whose information Upromise collected through the "personalized offers" feature of the toolbar and to provide those customers with instructions to permanently disable the personalized offer feature and uninstall the toolbar.[111]

---

103 *In re Sears Holdings Mgmt. Corp.*, No. C-4264 (F.T.C. Aug. 31, 2009) (decision and order).

104 *Id.* at *7.

105 Complaint, *In re PaymentsMD, LLC,* No. C-4505 (F.T.C. Jan. 27, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150206paymentsmdcmpt.pdf (alleging two counts of deception for failing to adequately inform consumers that the medical billing services company would also seek sensitive health information from third parties); *see also* Complaint, *In re Michael C. Hughes,* No. C-4502 (F.T.C. Jan. 9, 2015), *available* at https://www.ftc.gov/system/files/documents/cases/150206michaelhughescmpt.pdf.

106 Complaint ¶ 3, *In re Upromise, Inc*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf.

107 *Id.*¶¶ 4-6.

108 *Id.* ¶ 15.

109 *Id.* ¶ 16-19.

110 *Id.* ¶ 20.

111 Decision and Order at 5, *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisedo.pdf.

c. Compete, Inc.

The Commission also settled with Compete, Inc., a web analytics company, which, in 2006, launched web browser add-ons called the Compete Toolbar and the Compete Consumer Input Panel.[112] The Compete Toolbar offered users information about the websites they visited, such as the website's popularity.[113] The Compete Consumer Input Panel offered users rewards for sharing their opinions about products and services.[114] The company disclosed that when the Compete Toolbar's "Community Share" feature was engaged it would collect the web pages that users visited in an "anonymously pooled" fashion.[115] Similarly, the company indicated that the Consumer Input Panel would "anonymously transmit[]" aspects of users' browsing behavior to Compete.[116]

The FTC alleged that, contrary to these claims of limited collection, the Toolbar and Input Panel collected and transmitted more extensive information about a consumer's internet behavior and financial transactions, including credit card and Social Security number submitted to third-party websites.[117] The agency alleged that this constituted a deceptive act or practice.[118] The Commission also alleged that Compete falsely represented that it removed all personal information collected through its Toolbar and Consumer Input Panel before transmitting that information to Compete.[119] Finally, the FTC alleged counts for deceptive and unfair security practices.[120]

The Company's settlement with the Commission requires Compete to, among other things, establish a comprehensive information security program.[121]

2. Cookies and Behavioral Advertising

a. Chitika

The FTC's 2011 settlement with Chitika represents the agency's first case against an online advertising network.[122] Chitika tracked users by setting a browser cookie on users' computers.[123] Chitika's privacy policy offered users a button to opt-out of receiving

---

112 *In re Compete, Inc.*, 155 F.T.C. 264 , 265 (Feb. 20, 2013).

113 *Id.*

114 *Id.*

115 *Id.* at 266.

116 *Id.*

117 *Id.* at 270-71.

118 *Id.*

119 *Id.*

120 *Id.* at 271-72.

121 *In re Compete, Inc.*, 155 F.T.C. 264, 294-95 (Feb. 20, 2013) (decision and order).

122 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers A-7 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

123 *In re Chitika, Inc.*, 151 F.T.C. 494, 495-96 (2011) (complaint).

tracking cookies that, when pressed, indicated to the user that "You are currently opted out."[124] Without notice, however, consumers' opt-out preferences expired after ten days, at which point Chitika resumed tracking those users.[125]

The FTC alleged that Chitika's opt-out messaging represented to users that their opt-out preferences would be saved for a "reasonable period of time"—certainly more than ten days.[126] The FTC's complaint alleged that this practice was deceptive in violation of Section 5 of the FTC Act.

b. ScanScout

In re ScanScout, Inc. is another matter that involved an advertising network's tracking technology. ScanScout, Inc. was a video advertising network that employed behavioral advertising technology to select the ads it served users.[127] While many behavioral advertisers use HTTP cookies, which are stored by a users' browser, ScanScout employed Flash cookies, which are stored in a separate location that, at the time, was not managed by a user's browser.[128]

The FTC's 2011 complaint included a single deception count. The agency alleged that ScanScout's privacy policy, which stated that users could change their *browser* settings to "opt out" of receiving a ScanScout cookie, was false and misleading.[129] A browser's cookie settings did nothing to prevent ScanScout from setting a Flash cookie, nor could an operation within a user's browser delete ScanScout's cookies.[130]

c. Epic Marketplace

ScanScout is not the only company to employ other methods of tracking users besides browser cookies. In 2013, the Commission settled with Epic Marketplace Inc. and Epic Media Group, LLC (together, "Epic") based on the agency's complaint that Epic's misleading statements and failure to disclose its "history sniffing" technology violated Section 5 of the FTC Act. Epic served as an internet advertising "intermediary" between website owners and advertisers.[131] It called the network of websites on which it served ads the "Epic Marketplace network."[132] According to the complaint, Epic was able to "history sniff"—that is, determine the websites a consumer had previously visited by accessing a user's browser history.[133] Epic's history sniffing circumvented users' efforts to prevent tracking by deleting cookies, since a browser would retain a user's browsing

---

124 *Id.* at 497.

125 *Id.*

126 *Id.* at 497-98.

127 *In re ScanScout, Inc.*, 152 F.T.C. 1019, 1020 (Dec. 14, 2011) (complaint).

128 *Id.* at 1020-21.

129 *Id.*

130 *Id.* at 1021.

131 *In re Epic Marketplace, Inc.*, 155 F.T.C. 406, 407 (Mar. 13, 2013) (complaint).

132 *Id.*

133 *Id.* at 408.

history even after purging all cookies.[134] History sniffing also allowed Epic to observe users' browsing habits on websites outside of the Epic Marketplace network.[135]

Epic included its history-sniffing code in advertisements displayed on cnn.com, papajohns.com, redcross.com, and orbitz.com, among other websites in the Epic Marketplace network, according to the FTC complaint.[136] The company queried users' browsing histories, which allegedly included some users' visits to webpages relating to "fertility issues, impotence, menopause, incontinence, disability insurance, credit repair, debt relief, and personal bankruptcy."[137]

The FTC alleged that Epic used "history sniffing" to collect information from users about their browsing habits outside of the websites in the Epic Marketplace Network, in conflict with representations that Epic made in its privacy policy.[138] The Commission also alleged that Epic failed to disclose that it was employing history sniffing, which would be material to consumers, and therefore constituted a deceptive act or practice.[139]

d. Google (Safari)

In 2012, the DOJ, on behalf of the FTC, filed a complaint in district court against Google for violating the terms of the 2011 Buzz settlement discussed above.[140] This time the FTC's complaint centered around Google's false representations to Apple Safari browser users that Google would not set tracking cookies or serve targeted ads based on those cookies.[141]

Google uses browser cookies to collect information about users and serve them targeted internet advertisements.[142] The complaint alleged that the company offered users various ways for users to opt-out of targeted advertising, including, for users of Internet Explorer, Firefox, and Chrome browsers, the ability to download a browser plugin to permanently opt-out.[143] Google did not provide a similar plugin for Safari browser users, but stated that Safari's default settings "effectively accomplishes the same thing."[144]

Not so, the Commission alleged. According to the complaint, Google overrode Safari's default settings by first setting a cookie type relating to web form submissions that

---

134 *Id.* at 408-09.

135 *Id.* at 411.

136 *Id.* at 408.

137 *Id.*

138 *Id.* at 411.

139 *Id.*

140 *See supra* Section II(B)(1).

141 Complaint ¶ 12, *United States v. Google Inc.*, No. 5:12-cv-04177-HRL (N.D. Cal. Aug. 8, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809googlecmptexhibits.pdf.

142 *Id.* ¶ 23.

143 *Id.* ¶ 35.

144 *Id.* ¶¶ 36, 37.

Safari would accept even under the default settings.[145] Thereafter, Safari would accept other types of cookies from Google, including cookies that allowed the company to serve targeted ads.[146]

The three counts of the complaint alleged violations of the Buzz consent order for misrepresenting the extent to which users could control Google's collection of their information and for misrepresenting Google's compliance with the Network Advertising Initiative's Self-Regulatory Code of Conduct.[147] For violations of the 2011 Buzz consent order, Google was subject to civil penalties of up to $16,000 per individual violation.[148] The company settled with the Commission for $22,500,000.[149]

D. Mobile

Ubiquitous mobile devices pose a number of privacy risks that the FTC has addressed through its enforcement actions and guidance. Some of the agency's enforcement actions have focused on adequate user notice and consent, which are important in the mobile context just as they are elsewhere.[150] Moreover, as the FTC outlined in a 2013 staff report, mobile devices present at least three unique privacy challenges. First, mobile devices are typically associated with a single individual, typically always with that person, and typically always on.[151] Second, mobile devices function at the center of a number of data-collecting entities, including wireless providers, mobile OS providers, app developers, analytics companies, and advertisers.[152] Finally, mobile devices—in contrast to desktop computers—may be used to collect a user's geolocation information to build a record

---

145 *Id.* ¶¶ 42-43.

146 *Id.* ¶¶ 46, 48.

147 *Id.* ¶¶ 49-57.

148 *See* 15 U.S.C. § 45(l), as modified by 28 U.S.C. § 2461; *see also* 16 C.F.R. § 1.98(c).

149 *See* Order Approving Stipulated Order for Permanent Injunction and Civil Penalty Judgment at 3, *United States v. Google Inc.*, No. 5:12-cv-04177-HRL (N.D. Cal. Nov. 16, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/11/121120googleorder.pdf.

150 *See, e.g.,* Complaint, *In re General Workings Inc.*, No. C-4573 (F.T.C. Apr. 26, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1604vulcuncmpt.pdf (alleging an unfairness count based on respondents' installation, without adequate notice or consent, of a Chrome browser extension on users' PCs that then force-installed apps onto that user's mobile Android device); Complaint, *FTC v. Frostwire LLC*, No. 1:11-cv-23643 (S.D. Fl. Oct. 7, 2011) (alleging unfair design of the company's mobile file-sharing app that caused users to unknowingly share files on their mobile devices).

151 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 2 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also, e.g.,* Complaint, *In re Nomi Tech., Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (discussed *infra* Section II(D)(3)).

152 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 2-3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also, e.g.,* Complaint, *In re Nomi Tech. , Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (discussed *infra*)).

of an individual's movements.[153] This section discusses some of the FTC enforcement actions and guidance literature addressing these and other issues.

1. Path

In 2013, the DOJ, on behalf of the FTC, filed a complaint against Path, Inc., a social network, for its false and misleading disclosures relating to its automatic collection of users' mobile device contact information. The Path app for Apple's iOS devices offered users the ability to "Find friends from your contacts."[154] However, even if a user never selected that option, the app automatically collected contacts stored on a mobile device each time the user launched the app and signed in, the complaint alleged.[155] Path's privacy policy also stated that the company automatically collected "certain information . . . such as your Internet Protocol (IP) address, your operating system, the browser type, the address of a referring site and your activity on our site."[156]

The complaint alleged that "Find friends from your contacts" amounted to a representation that Path would collect users' mobile device contacts only if the user selected that option.[157] Because Path automatically collected that information regardless, that representation amounted to a deceptive act or practice.[158] The complaint also alleged that Path's automatic collection of users' mobile device contacts exceeded what the company disclosed in its privacy policy.[159]

Finally, the complaint alleged that Path collected information from children in violation of the COPPA Rule.[160] The company's settlement required Path to pay $800,000 for its violations of the COPPA Rule.[161]

---

153 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 3 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; *see also, e.g.,* Complaint, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf (discussed *infra*); Complaint, *In re Nomi Tech., Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf (discussed *infra*); Complaint, *Goldenshores Tech., LLC*, No. C-4446 (F.T.C. Mar. 31, 2014) (alleging that company failed to adequately disclose that Android flashlight app would transmit precise geolocation information third-party advertising networks).

154 Complaint ¶ 12, *United States v. Path, Inc.*, No. 3:13-cv-0448 (N.D. Cal. Jan. 31, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathinccmpt.pdf.

155 *Id.* ¶¶ 13-14.

156 *Id.* ¶ 16.

157 *Id.* ¶¶ 30-31.

158 *Id.* ¶ 31.

159 *Id.* ¶¶ 32-33.

160 *Id.* ¶¶ 34-38.

161 Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief ¶ 18, *United States v. Path, Inc.*, No. 3:13-cv-0448 (N.D. Cal. Feb. 8, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/02/130201pathincdo.pdf.

2. Snapchat

In 2014, the FTC settled with Snapchat, Inc., a mobile app that marketed itself as a way to send photo and video "snaps" that "disappear[] forever" after a pre-designated amount of time.[162] Despite this claim, the FTC alleged that there were a number of ways that a snap might not "disappear[] forever": users could access and save video files by connecting a mobile device to a computer, could use third-party apps available on Apple's and Google's app stores to save snaps, or could easily take a screen shot of the snap using a method that was not detected by the Snapchat app.[163] Consequently, the Commission's complaint alleged that Snapchat's representation that messages would "disappear forever" was false and misleading.[164] The Commission's complaint further alleged that Snapchat's representation that Snapchat users would be notified if a "snap" recipient took a screenshot of the message (to preserve it) was false and misleading because users could easily prevent the app from sending this notification.[165]

The Commission's complaint also alleged that a number of other aspects of Snapchat's service violated Section 5 of the FTC Act. In its privacy policy, Snapchat represented that it would "not ask for, track, or access any location-specific information from your device at any time while you are using the Snapchat application."[166] Despite this, the FTC said that Snapchat collected location information from users of the Android version of its application.[167] The FTC alleged that this was false or misleading in violation of Section 5 of the FTC Act.[168]

Snapchat's app offered to assist users in finding other friends on Snapchat. The app prompted users to enter a mobile phone number to search for a Snapchat account associated with that number.[169] When a user entered a phone number, however, the Snapchat app collected the names and phone numbers of *all* contacts on the user's mobile device.[170] The FTC alleged that Snapchat collected more personal information through its "Find Friends" feature than both its user interface and its privacy policy represented.[171]

Finally, the Commission alleged that the company's failure to verify the owner of the phone number that users entered into its application and failure to secure its API did not constitute reasonable security measures to protect personal information that Snapchat represented it offered in its privacy policy.[172]

---

162 Complaint ¶¶ 6-7, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf.

163 *Id.* ¶¶ 9-15.

164 *Id.* ¶¶ 16-17.

165 *Id.* ¶¶ 15, 18-19.

166 *Id.* ¶¶ 20-21.

167 *Id.* ¶¶ 23-24.

168 *Id.* ¶ 24.

169 *Id.* ¶ 25.

170 *Id.* ¶ 26.

171 *Id.* ¶¶ 28-33.

172 *Id.* ¶¶ 43-44.

The FTC's settlement requires Snapchat to, among other things, implement a comprehensive privacy program.[173]

3. Nomi

In 2015, the FTC settled with Nomi Technologies, a company that provides retailers with the ability to silently collect and track information about the mobile devices that consumers carry into their stores.[174] Nomi's privacy policy promised to allow consumers to opt out of retailer tracking "on its website as well as at any retailer using Nomi's technology."[175]

The Commission's complaint alleged that Nomi had promised both to give consumers notice when a retailer was using Nomi's technology and to provide a means of opting out of tracking at those retail locations.[176] Nomi's failure to provide users with this notice and opportunity to opt out amounted to deceptive acts or practices, the Commission alleged.[177]

The Commission approved the complaint and settlement by a three to two vote. FTC Chairwoman Ramirez, along with Commissioners Brill and McSweeny, issued a statement in support of the complaint and consent order. They wrote: "This case is simply about ensuring that when companies promise consumers the ability to make choices, they follow through on those promises."[178] Commissioner Ohlhausen issued two dissenting statements emphasizing that Nomi had no obligation to offer an opt-out as a "third party contractor collecting no personally identifiable information,"[179] and was therefore being "punishe[d]" for offering "more transparency and choice than legally required.[180] Commissioner Ohlhausen expressed her concern that this settlement would "undermine the FTC's own established privacy goals" and "diminish companies' incentives to be transparent about their privacy practices."[181] Commissioner Wright also dissented on the basis that penalizing Nomi "sends a dangerous message to firms weighing the costs and

---

173 Decision and Order at 3, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.

174 Complaint ¶¶ 3-5, *In re Nomi Tech., Inc.*, No. C-4538 (F.T.C. Sept. 3, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.

175 *Id.* ¶ 12.

176 *Id.* ¶¶ 14, 16.

177 *Id.* ¶¶ 14-17.

178 Statement of Chairwoman Ramirez, Comm'r Brill, and Comm'r McSweeny 3-4, *In re Nomi Tech., Inc.*, No. C-4538 (Apr. 23, 2015), *available at* https://www.ftc.gov/public-statements/2015/04/statement-chairwoman-ramirez-commissioner-brill-commissioner-mcsweeny.

179 Dissenting Statement of Comm'r Maureen K. Ohlhausen 1, *In re Nomi Tech., Inc.*, No. C-4538 (Apr. 23, 2015), *available at* https://www.ftc.gov/system/files/documents/public_statements/638361/150423nomiohlhausenstatement.pdf.

180 Dissenting Statement of Comm'r Maureen K. Ohlhausen 1, *In re Nomi Tech., Inc.*, No. C-4538 (Aug. 28, 2015), *available at https://www.ftc.gov/public-statements/2015/08/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-nomi*.

181 *Id.*

benefits of voluntarily providing information and choice to consumers."[182] Moreover, in his view the Commission had not shown that Nomi's representation that consumers could opt out at retail locations was material—a required element of deception.[183] Commissioner Brill also wrote separately in support of the settlement and to address Commissioner Ohlhausen's concern that Nomi's settlement would deter companies from offering privacy choices. In her view, the settlement would incentivize companies "to periodically review statements they make to consumers" and to "make sure their practices line up with those statements."[184]

4. FTC Guidance on Mobile Privacy Issues

The FTC has issued a number of studies and business guidance documents on mobile privacy issues. In the 2013 staff report *Mobile Privacy Disclosures*, FTC staff set forth best practices for privacy disclosures for mobile platforms, app developers, app trade associations, and advertising networks and other third parties that provide app services. The report notes that "platforms, such as Apple, Google, Amazon, Microsoft, and Blackberry are gatekeepers to the app marketplace and possess the greatest ability to effectuate change with respect to improving mobile privacy disclosures."[185] FTC staff suggest that mobile platforms should: (1) offer consistent privacy disclosures across apps; (2) exert more oversight and control over the apps offered in their app stores; (3) make clear the extent to which the platform reviews apps before offering apps for download on their app stores; and (4) develop a do-not-track mechanism to provide users with a means of preventing companies from tracking their behavior across apps.[186]

FTC staff also provide recommendations for app developers in that report. Staff recommend that developers: (1) make their privacy policies available through the app stores in which they offer the app; (2) provide "just-in-time" disclosures and obtain express consent when their apps collect sensitive information outside of the platform's API or when they share such sensitive information with third parties; and (3) better coordinate with the ad networks and other third parties so that developers' privacy-related disclosures to consumers are truthful and accurate.[187] The report also encourages app developers to participate in self-regulatory programs, trade associations, and industry organizations in pursuit of "uniform, short-form privacy disclosures."[188]

---

182 Dissenting Statement of Comm'r Joshua D. Wright 4, *In re Nomi Tech., Inc.*, No. C-4538 (Apr. 23, 2015), *available at* https://www.ftc.gov/public-statements/2015/04/dissenting-statement-commissioner-joshua-d-wright-matter-nomi-technologies.

183 *Id.*

184 Statement of Comm'r Julie Brill 1, *In re Nomi Tech., Inc.*, No. C-4538 (Aug. 28, 2015), *available at* https://www.ftc.gov/public-statements/2015/08/statement-commissioner-julie-brill-matter-nomi-technologies-inc.

185 Fed. Trade Comm'n, Mobile Privacy Disclosures: Building Trust Through Transparency 14 (2013), *available at* https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

186 *Id.* at 14-21.

187 *Id. at 22-24.*

188 *Id.* at 24.

For advertising networks and other third parties, the report recommends that these entities make clear the function of the code they are supplying to app developers (to provide advertising services, for example).[189] The report also recommends that these third parties work with platforms to implement a do-not-track system.[190]

Finally, the staff report recommends that app trade associations work to: (1) develop standard icons to depict an app's privacy practices; (2) develop privacy "badges" to standardize privacy disclosures within apps or app advertisements; and (3) standardize within app privacy policies.[191]

In addition, the FTC has published *Marketing Your Mobile App*,[192] which is a short guide for businesses on common advertising, privacy, and data security issues faced by even the smallest mobile app startups. The guide makes the point that "[l]aws that apply to established businesses apply to [small companies], too, and violations can be costly."[193] Finally, two reports—*Paper, Plastic . . . or Mobile?* and *What's the Deal?*—focus on a host of consumer protection issues, including privacy, relating to mobile payments and mobile shopping apps.[194]

E. Data Brokers: Renting or Selling Data

Several FTC enforcement actions and policy initiatives have focused on companies that buy, rent, or sell consumer information. These companies, sometimes called "data brokers," often produce marketing, risk mitigation, or people-searching products, which can help other companies better market their goods, verify identities and detect fraud, or research individuals.[195] The Commission has recognized how consumers benefit from data brokers, but it has also identified some of the risks that such entities pose to consumers. This section discusses some of the agency's enforcement actions, studies, and guidance on data brokers.

---

189 *Id.*

190 *Id.* at 25.

191 *Id.* at 25-27.

192 Fed. Trade Comm'n, Marketing Your Mobile App (2013), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf.

193 *Id.* at 1.

194 Fed. Trade Comm'n, What's the Deal? An FTC Study on Mobile Shopping Apps (2014), *available at available at* https://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf; Fed. Trade Comm'n, Paper, Plastic . . . or Mobile? (2013), *available at https://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf.*

195 Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 23-35 (2014), *available at* https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

1. CartManager

In 2005, the FTC settled with Vision I Properties, LLC d/b/a CartManager International ("CartManager"). According to the FTC's complaint, CartManager licensed online shopping cart software to small online merchants who, in turn, incorporated the software into their own websites to look like other pages on the merchant's site.[196] When consumers complete their orders using these shopping carts, CartManager receives the information, including name, billing and shipping addresses, phone number, email, credit card information, and information about the customer's purchase.[197] CartManager would then transmit this information to the merchant to fill the order.[198]

Some merchants using CartManager's shopping cart software published privacy policies stating that they would not rent or sell personal information collected from consumers to third parties, the FTC alleged.[199] Nevertheless, in 2003, CartManager began selling personal information it collected through the check-out process to third-party marketers.[200] The FTC alleged that CartManager did so "knowing that such practices were contrary to merchant privacy policies."[201] The Commission alleged that this constituted an unfair act or practice in violation of Section 5 of the FTC Act.[202]

2. LeapLab

Nine years after the agency's action against CartManager, the FTC filed a complaint in federal district court against another company, SiteSearch Corporation, along with SiteSearch's founder, chairman, and former CEO, LeapLab, LLC, and Leads Company, LLC. The defendants in this case collected and sold payday loan applications, which are applications for short-term loans often used to obtain an advance on an upcoming paycheck.[203] The FTC alleged that the defendants in this case sold these applications, which contain consumers' personal financial information (such as account and Social Security numbers), to non-lenders—entities that were not in the business of offering these consumers a payday loan.[204]

One of defendants' non-lender customers included Ideal Financial. Using data acquired from defendants and other sources, Ideal Financial processed over $47 million in unauthorized charges to consumers' accounts.[205] The FTC's complaint alleged that defendants' sale of consumer payday loan applications to non-lenders that had "no

---

196 *Vision I Properties, LLC*, 139 F.T.C. 296, 297 (2005).

197 *Id.*

198 *Id.*

199 *Id.* at 297-98.

200 *Id.* at 298.

201 *Id.* at 299.

202 *Id.*

203 Complaint ¶¶ 12-13, *FTC v. Sitesearch Corp., dba LeapLab*, No. 2:14-cv-02750-NVW (D. Ariz. Dec. 22, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf.

204 *Id.* ¶¶ 13, 15, 19.

205 *Id.* ¶ 36.

legitimate need for this sensitive personal information" constituted an unfair act or practice in violation of Section 5 of the FTC Act.[206] The FTC settled with LeapLab, LLC and John Ayers for $4,124,710 and with Leads Company LLC for $1,651,682.[207] The Court entered a default judgment against SiteSearch Corp. for $4,124,710.[208]

3. Bayview Solutions[209]

In 2014, the same year as the FTC's action against the LeapLab defendants, the FTC filed a complaint in federal district court against Bayview Solutions, LLC and two individuals for publicly disclosing consumers' sensitive financial information on an online debt collection marketplace.[210] Such marketplaces serve as forums for debt sellers to advertise their debt portfolios to buyers.[211] The FTC alleged that the defendants posted partially-redacted debt portfolios in unencrypted Excel format, which included sensitive information such as consumers' first name, date of birth, city, state, email address, employer name, bank, bank account number, bank routing number, and driver's license number.[212]

While defendants partially redacted last names, street addresses, or phone numbers from the portfolios, the FTC alleged that the remaining, unredacted information, such as a user's email address, made it all too easy to re-identify the rest of the consumer's information. For example, since email addresses are commonly a combination of a consumer's first and last names, the partially redacted information could allow someone to figure out a consumer's last name.[213] The agency's complaint alleged that this exposed the personal information of more than 28,000 consumers.[214] Consumers "would be unlikely to know that Defendants possess, and are openly disclosing their information" and could not therefore "protect themselves from the harms and potential harms the disclosures cause, including possible identity theft and concomitant account fraud, invasion of privacy, and job loss."[215] The FTC alleged that defendants' public disclosure of consumer information constituted an unfair act or practice in violation of Section 5

---

206 *Id.* ¶¶ 44-46.

207 Press Release, Fed. Trade Comm'n, Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers (Feb. 18, 2016) (collecting settlements), *available at* https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive.

208 Final Judgment and Order for Injunctive and Other Relief at 6, *FTC v. Sitesearch Corp.*, No. 2:14-cv-02750-NVW (D. Ariz. Dec. 11, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/160218leaplabsitesearch.pdf.

209 The FTC filed another complaint against Cornerstone and Company and its manager for similar conduct. *See* Complaint, *FTC v. Cornerstone and Co.*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/enforcement/cases-proceedings/142-3211-x150005/cornerstone-company-llc.

210 Complaint ¶¶ 11-12, 31, *FTC v. Bayview Sols., LLC*, No. 1:24-cv-01830-RC (D.D.C. Oct. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf.

211 *Id.* ¶ 11.

212 *Id.* ¶ 20.

213 *Id.* ¶ 21.

214 *Id.* ¶ 18.

215 *Id.* ¶ 25.

of the FTC Act.[216] Defendants stipulated to a permanent injunction that requires, among other things, that they establish a comprehensive information security program.[217]

4. FTC Guidance for Data Brokers and Big Data

The FTC has also issued guidance on the privacy issues peculiar to data brokers and so-called "big data." In its 2014 report *Data Brokers: A Call for Transparency and Accountability*, the FTC reported the findings of its study of nine data brokers and offered legislative recommendations to Congress and best practices recommendations to data brokers. The Commission reaffirmed the recommendations it made to data brokers in its *Protecting Consumer Privacy* report,[218] including its recommendation that data brokers consider privacy at every stage of product development—the "privacy by design" principle.[219] The FTC suggested that it is "particularly important" for data brokers to collect only the data they need and dispose of the data they do not.[220] In addition, the agency called on data brokers to improve their efforts to avoid collecting information from children and teens.[221] Finally, the Commission encouraged data brokers to take "reasonable precautions" to make sure that their customers—those who use their data—do not use it for eligibility determinations or unlawful discriminatory purposes.[222]

While the FTC's 2014 data brokers report recommends that companies ensure the appropriate use of consumer data, its focus is primarily on data collection, compilation, and analytics issues. In contrast, the Commission's 2016 report *Big Data: A Tool for Inclusion or Exclusion?* focuses predominantly on how data gets used after it is collected—including the consumer protection and equal employment laws that apply to big data use.[223] Finally, the FTC's business guidance for debt brokers, *Buying or selling debts? Steps for keeping data secure*, offers a collection of common-sense practices for securing debt-related information.[224]

---

216 *Id.* ¶¶ 31-33.

217 Stipulated Final Order for Permanent Injunction at 3, *FTC v. Bayview Sols., LLC*, No. 1:24-cv-01830-RC (D.D.C. Apr. 20, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150421bayviewstip.pdf.

218 *See supra* Section I(B).

219 Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability 54 (2014), *available at* , https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

220 *Id.* at 55.

221 *Id.*

222 *Id.*

223 Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

224 Fed. Trade Comm'n, Buying or selling debts? Steps for keeping data secure (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0202_buying-selling-debt.pdf.

F. Misappropriation of Consumer Data

The FTC has brought several cases against companies that misappropriate consumer data, either through undisclosed monitoring of consumers or unauthorized means. This section discusses three of these cases.

1. DesignerWare and Related Rent-to-Own Cases

In 2013, the FTC settled with several companies and individuals involved with software installed on rented computers that allowed the rental company to take screenshots, log keystrokes, and use the computers' webcams to take pictures—all without the renters' knowledge. DesignerWare, LLC developed the software at issue, called PC Rental Agent, which it licensed to stores that offer rent-to-own computers.[225]

The program had a Detective Mode, which enabled the computer rental companies to silently monitor a computer user's activities and take pictures surreptitiously using the PC's webcam.[226] According to the complaint, one of the owners of DesignerWare stated that Detective Mode works "like many spyware/malware programs" in that it is "not detectable by antivirus programs" and "hooks the screen, keyboard, and mouse so it can 'Spy' on the user and gather information."[227] The agency alleged that Detective Mode had been used to capture pictures of children, naked individuals, and couples engaged in sexual activities.[228]

Using Detective Mode, rental companies could also prompt a renter's computer to display a fake registration window for a software program such as Windows, Internet Explorer, Office, or Yahoo! Messenger.[229] The registration window collected a user's name and contact information, which the software program then transmitted to DesignerWare's servers, which in turn emailed the information to the rent-to-own store.[230]

Finally, the Commission alleged that PC Rental Agent logged, for a period of time, all of the Wi-Fi hotspots the rented computer detected or connected to.[231] The software would then transmit that information to DesignerWare's servers, which would then provide the computer rental companies with a list of the physical locations of the Wi-Fi hotspots the rented computer detected or connected to.[232] This information could be used to pinpoint a rented computer's location and, if aggregated, could track the movements of computer renters.[233]

---

225 *In re DesignerWare, LLC*, 155 F.T.C. 421, 422 (Apr. 11, 2013) (complaint).

226 *Id.* at 424.

227 *Id.*

228 *Id.* at 425.

229 *Id.* at 427.

230 *Id.* at 427.

231 *Id.* at 426.

232 *Id.*

233 *Id.*

The Commission included three counts against DesignerWare in its complaint. First, the Commission alleged that the company's surreptitious monitoring and geophysical location tracking constituted an unfair act or practice in violation of Section 5 of the FTC Act.[234] Second, the Commission alleged that DesignerWare had provided rent-to-own computer stores with the means and instrumentalities to engage in an unfair practice by providing them with PC Rental Agent and by transmitting information improperly acquired from computer rental consumers.[235] Finally, the FTC alleged that DesignerWare's fake registration windows that purported to be from "trusted software providers" were deceptive.[236]

The FTC settled with DesignerWare, two of its principals, and seven rent-to-own companies in April of 2013,[237] and with the national rent-to-own retailer Aaron's, Inc. in March of 2014.[238]

2. Jerk.com

In re Jerk, LLC was one of the agency's few privacy matters to proceed to litigation. In 2014, the Commission filed an administrative complaint against Jerk, LLC and its principal, John Fanning. Respondents operated a social network (www.jerk.com and other URLs) where users could "Post a Jerk" by creating a profile of another person with buttons that allowed users to vote the person a "Jerk" or "not a Jerk."[239] The website contained an estimated 70+ million profiles, which purported to be generated by users, the complaint alleged.[240] By paying a $30 membership fee, users could obtain "additional paid premium features," including, the FTC alleged, the ability to dispute information posted on the website.[241]

The Commission alleged two counts of deception. First, Jerk represented that content on the website was generated by Jerk users and reflected their views when, in fact, the vast majority of Jerk profiles were taken, without users' consent, from Facebook.[242] Second, Jerk represented that consumers who paid the membership fee would receive additional benefits, including the ability to dispute the information posted

---

234 *Id.* at 428-29.

235 *Id.* at 429-30.

236 *Id.* at 430-31.

237 Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Software and Rent-to-Own Companies Accused of Computer Spying (Apr. 15, 2013) (collecting settlements), *available at* https://www.ftc.gov/news-events/press-releases/2013/04/ftc-approves-final-order-settling-charges-against-software-and.

238 Decision and Order, *In re Aaron's, Inc.*, No. C-4442 (F.T.C. Mar. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140311aaronsdo.pdf.

239 Complaint ¶¶ 4, 6, *In re Jerk, LLC*, No. 9361 (F.T.C. Apr. 2, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140407jerkpart3cmpt.pdf.

240 *Id.* ¶ 4.

241 *Id.* ¶¶ 8, 12.

242 *Id.* ¶¶ 15-16.

on the website, when, in fact, consumers often received nothing in return for paying the membership fee.[243]

In March 2015, the Commission granted summary judgment for FTC complaint counsel. The Commission found for the FTC on both deception counts and found John Fanning individually liable.[244] Fanning, but not Jerk, LLC, appealed the Commission's decision to the First Circuit, which upheld the Commission's finding of liability.[245]

3. Craig Brittain

In 2016, the FTC settled with an individual, Craig Brittain, who owned and ran the so-called "revenge porn" websites www.isanybodydown.com and www.obamanudes.com. According to the complaint, Brittain posted nude photographs along with the subject's full name, date of birth, town and state, phone number, and a link to the subject's Facebook profile.[246] Brittain compiled the photos and information through anonymous submissions, by asking for others to send him nude photographs and through a "bounty" system on the website where users could ask others to post nude photos of a specific person in exchange for a reward.[247] In many instances, Brittain did not remove the photos in response to requests.[248] According to the complaint, Brittain, posing as an independent entity called "Takedown Hammer" and "Takedown Lawyer," advertised content removal services on the website and charged users $200-500 to remove photos that he himself had posted.[249]

The FTC alleged that Brittain's posting of nude photographs, along with the personal information of the subjects, constituted an unfair act or practice in violation of Section 5 of the FTC Act. The agency also alleged that Brittain had represented that the photos submitted to him would be used solely for his private use.[250] The Commission said that posting those photos and their personal information therefore constituted a deceptive act or practice.[251]

The FTC privacy enforcement actions and guidance discussed above help define the boundaries of Section 5 liability for companies and individuals. While technological developments—particularly those that involve the collection or use of consumer data—will always create uncertainty, these past FTC privacy actions should help individuals, companies, and the attorneys that advise them to predict whether particular data practices amount to deceptive or unfair acts or practices under Section 5.

---

243 *Id.* ¶¶ 17-18.

244 Opinion of the Commission at 2, *In re Jerk, LLC*, No. 9361 (F.T.C. Mar. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150325jerkopinion_0.pdf.

245 *Fanning v. FTC*, 821 F.3d 164, 168 (1st Cir. 2016).

246 Complaint ¶ 5, *In re Craig Brittain*, No. C-4564 (F.T.C. Dec. 28, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/160108craigbrittaincmpt.pdf.

247 *Id.* ¶¶ 5-7.

248 *Id.* ¶ 9.

249 *Id.* ¶ 10.

250 *Id.* ¶ 15.

251 *Id.* ¶ 16.

III. FTC DATA SECURITY ENFORCEMENT AND GUIDANCE UNDER SECTION 5

The FTC's data security enforcement actions and guidance play a similar role in outlining the contours of Section 5 liability for particular data security practices. This section discusses some of those cases and materials.

A. FTC's Data Security Enforcement Authority under Section 5

Since 2002, the agency has brought dozens of data security actions under Section 5 theories of deception and unfairness.[252] Like its privacy cases, the FTC's early data security actions focused on companies' violations of their express or implied promises about their data security practices. Later ones alleged unfairness and deception or unfairness alone.[253]

The vast majority of FTC data security actions have concluded in settlements. Two cases, however, have proceeded to litigation: *FTC v. Wyndham Worldwide Corp.* in federal court and *In re LabMD, Inc.* before the FTC's administrative tribunal.[254] Both the *Wyndham* and *LabMD* actions addressed the FTC's unfairness authority under Section 5 to bring data security enforcement actions. In these cases, the defendants argued that the FTC lacks authority to bring such actions under an unfairness theory and that the agency failed to provide fair notice of the data security standards that the companies must follow under Section 5. This section addresses the FTC's two litigated cases, its settlements, and its guidance.

1. Wyndham

In *Wyndham*, the FTC alleged that the hospitality chain engaged in both deceptive and unfair practices under Section 5 by "fail[ing] to maintain reasonable and appropriate data security for consumers' sensitive personal information,"[255] including failing to remedy known security vulnerabilities, allowing software to be configured inappropriately, and failing to employ reasonable measures to detect and prevent unauthorized access to the company's network.[256] Wyndham moved to dismiss the complaint, challenging on two grounds the FTC's authority to bring data security under an unfairness theory. First, Wyndham argued that the passage by Congress of specific laws relating to data security, such as the FCRA, GLBA, COPPA, and the Health Insurance and Portability and

---

252 *In re Eli Lilly & Co.*, 133 F.T.C. 763 (2002) (complaint) was the agency's first data security action. *See* Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers A-3 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

253 *See supra* Section I(A) (citing Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583 (2014)).

254 *F.T.C v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz.); *In re LabMD, Inc.*, No. 9357 (F.T.C.).

255 First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 1, 44-49, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

256 *Id.* at 24.

Accountability Act of 1996 (HIPAA), implies that Section 5, alone, does not authorize the agency to regulate data security under an unfairness theory.[257] Second, Wyndham argued that due process and fair notice principles require the agency to issue rules or regulations on data security before bringing enforcement actions.[258] The court rejected both arguments. It held that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme,"[259] and that the FTC Act's statutory three-part test for unfairness, as well as the agency's public complaints and consent orders, provide sufficient notice of what is prohibited under Section 5.[260]

On appeal, the Third Circuit affirmed the district court's decision. First, it upheld the FTC's data security authority under the unfairness prong, reasoning that Congress's passage of topic-specific statutes, such as the FCRA, GLBA, and COPPA, are consistent with the FTC already having "some authority" to regulate data security through Section 5.[261] Second, it held that Wyndham had fair notice that the company's data security practices could constitute an unfair practice.[262] "While far from precise," Section 5 still informs parties that the relevant inquiry is a "cost-benefit, analysis" that considers "the probability and expected size of reasonably unavoidable harms . . . given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[263] The court also found that the FTC's 2007 business guidance, *Protecting Personal Business Information: A Guide For Business*, counseled against many of the practices alleged against Wyndham, and that the agency's published complaints can help companies to "apprehend the possibility that their cybersecurity could fail as well."[264] In December of 2015, Wyndham agreed to settle the FTC's charges.[265]

2. LabMD

LabMD involved similar challenges to the FTC's Section 5 unfairness authority to bring data security cases. In this administrative litigation, the FTC alleged that a medical testing laboratory failed to reasonably protect the security of consumers' personal data, including medical information, by failing to use appropriate measures to prevent employees from installing on company computers applications and files that employees did not need to perform their jobs.[266] LabMD filed a motion to dismiss—and subsequently, a motion for summary judgment—arguing (1) that Section 5 does not

---

257 *F.T.C v. Wyndham Worldwide Corp.,* 10 F. Supp. 3d 602, 610-11 (D.N.J. Apr. 7, 2014).

258 *Id.* at 616.

259 *Id.* at 613.

260 *Id.* at 620-21.

261 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 248 (3d Cir. 2015) (explaining that the topic-specific statutes require, rather than merely authorize, the FTC to issue regulations).

262 *Id.* at 255.

263 *Id.*

264 *Id.* at 256-57.

265 Stipulated Order for Injunction, *FTC v. Wyndham Worldwide Corp.*, 2:13-cv-01887-ES-JAD (D.N.J. Dec. 11, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf.

266 Complaint ¶ 10, *In re LabMD, Inc.*, No. 9357 (F.T.C. Aug. 29, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

expressly authorize the FTC to regulate data security practices; (2) that HIPAA removes the agency's ability to apply Section 5 to unfair practices involving health information; and (3) that the agency cannot regulate data security under Section 5 on a case-by-case basis. The Commission rejected all three arguments. First, the Commission held that Congress delegated broad authority to determine what practices were unfair, citing the three-part test unfairness set in Section 5, the legislative history of the FTC Act, as well as federal case law deeming as "unfair" a wide range of acts and practices that were never expressly authorized under Section 5.[267] Next, the Commission held that neither HIPAA, nor any other "targeted" statute, such as the HITECH provision of the American Recovery and Reinvestment Act of 2009, forecloses the Commission from challenging data security measures that it has reason to believe are unfair acts or practices.[268] Finally, the Commission held that conducting an administrative adjudication without first conducting a rulemaking comports with due process—emphasizing that "complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development," rather than general regulations.[269]

After an administrative trial, the Chief Administrative Law Judge of the FTC issued an initial decision dismissing the FTC's complaint for failing to prove that Wyndham's conduct caused, or was likely to cause, substantial consumer injury.[270] FTC complaint counsel appealed the ALJ's decision to the Commission, which reversed and found LabMD's data security practices unfair under Section 5.[271] LabMD has appealed the Commission's order to the Eleventh Circuit.[272]

B. Enforcement Actions and Guidance

While *Wyndham* and *LabMD* focused on unfairness, the FTC has brought data security actions under both the deception and unfairness prongs of the FTC Act. The majority of FTC enforcement actions are settlements leading to consent orders that require the settling company, among other things, to establish and maintain a "comprehensive security program" or "information security program" that requires designated employees

---

267 Order Denying Respondent LabMD's Motion to Dismiss at 4, *In re LabMD, Inc.*, No. 9357 (F.T.C. Jan. 16, 2014), *available at https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf*; *see also* Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. May 19, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140520labmdmotion.pdf.

268 Order Denying Respondent LabMD's Motion to Dismiss at 11, *In re LabMD, Inc.*, No. 9357 (F.T.C. Jan. 16, 2014), *available at https://www.ftc.gov/sites/default/files/documents/cases/140117labmdorder.pdf*; *see also* Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. May 19, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140520labmdmotion.pdf.

269 Order Denying Respondent LabMD's Motion to Dismiss at 16, *In re LabMD, Inc.*, No. 9357 (F.T.C. Jan. 16, 2014); *see also* Order Denying Respondent LabMD, Inc.'s Motion for Summary Decision at 9, *In re LabMD, Inc.*, No. 9357 (F.T.C. May 19, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140520labmdmotion.pdf.

270 Initial Decision, *In re LabMD, Inc.*, No. 9357 (F.T.C. Nov. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.

271 Opinion of the Commission at 1, *In re LabMD, Inc.*, No. 9357 (F.T.C. July 29, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf.

272 Petition for Review, *LabMD, Inc. v. FTC, No. 16-16270 (11th Cir. Oct. 7, 2016).*

to coordinate the program, a privacy risk assessment, and safeguards to control the identified risks.[273] Such security programs also generally require the company to obtain biennial independent assessments of the appropriateness and effectiveness of the program.[274] Most orders also prohibit the settling company from mispresenting the extent to which it, or its products and services, protect(s) the "privacy, security, confidentiality, or integrity" of consumer personal information.[275]

---

273 *See, e.g.,* Stipulated Final Order for Permanent Injunction at 3-4, *FTC v. Cornerstone and Co.*, No. 1:14-cv-01479-RC (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150421cornerstonestip.pdf (comprehensive information security program); Decision and Order at 3-4, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf (comprehensive information security program); Decision and Order at 3-4, *In re Fandango, LLC,* No. C-4481 (F.T.C. Aug. 13, 2014), available at https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf (comprehensive security program); *In re HTC America Inc.,* 155 F.T.C. 1617, 1631-33 (2013) (decision and order) (comprehensive security program); Decision and Order at 2-3, *In re EPN, Inc.,* No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf (comprehensive information security program); Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 8-9, *United States v. RockYou, Inc.,* No. CV-12-1487 (N.D. Cal. Mar. 28, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf (comprehensive information security program); *In re CardSystems Sols, Inc.,* 142 F.T.C. 1019, 1025-26 (2006) (decision and order) (comprehensive information security program).

274 *See, e.g.*, Stipulated Final Order for Permanent Injunction at 5-6, *FTC v. Cornerstone and Co*., No. 1:14-cv-01479-RC (D.D.C. Apr. 21, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150421cornerstonestip.pdf; Decision and Order at 4-5, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf; Decision and Order at 4-5, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf; *In re HTC America Inc.*, 155 F.T.C. 1617, 1631-35 (2013) (decision and order); Decision and Order at 4, *In re EPN, Inc.*, No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf; Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 9-11, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 28, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf; *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1026-28 (2006) (decision and order).

275 *See, e.g.,* Decision and Order at 3, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf (prohibiting misrepresentations of "the extent to which respondents use, maintain, and protect the privacy, confidentiality, security, or integrity of personal information collected from or about consumers."); Decision and Order at 2, *In re Fandango, LLC*, No. C-4481 (Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf (prohibiting misrepresentations of "the extent to which respondent or its products or services maintain and protect the privacy, security, confidentiality, or integrity of any covered information.)"; *In re HTC America Inc.*, 155 F.T.C. 1617, 1631 (2013) (decision and order) (prohibiting misrepresentations of "the extent to which respondent or its products or services, including any covered devices, use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of any covered information from or about consumers."); Decision and Order at 2, *In re EPN, Inc.*, No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epndo.pdf (prohibiting misrepresentations of "the extent to which respondent maintains and protects the privacy, confidentiality, or security of any personal information collected from or about consumers."); Consent Decree and Order for Civil Penalties, Injunction and Other Relief at 7, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 28, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf (prohibiting misrepresentations of the "the extent to which [Defendant and its officers, agents, representatives, and employees] maintain and protect the privacy, confidentiality, security, or integrity of consumer personal information collected from or about consumers.").

Although the requirements in the consent orders apply only to the companies under order, the inadequacies and failures alleged in the FTC's public complaints associated with these settlements provide insight into the agency's approach to data security enforcement, as do the various reports, business guides, and blogs that the agency has issued.

For data security, one of the agency's key pieces of guidance is *Start with Security*, which identifies ten important lessons culled from the FTC's dozens of data security enforcement actions.[276] Another informative guide is *Protecting Personal Information*, which provides a practical checklist of actions for creating and implementing a sound data security plan.[277] Although FTC reports and business guides generally do not distinguish between practices required under Section 5 and best practices that go beyond existing legal requirements, the materials nevertheless provide concrete advice on many of the practices that the FTC has alleged to be unfair or deceptive in its public complaints. Indeed, in *FTC v. Wyndham*, the Third Circuit cited *Protecting Personal Information* as a helpful source of notice about companies' data security obligations under Section 5.[278]

The next sections discuss the FTC enforcement actions as well as its guidance, synthesizing key principles and practices from both areas of agency activity.

C. Reasonable Data Collection, Use, Retention, and Disposal

The Commission has stated that "reasonableness" is the "touchstone" of the agency's approach to data security: "'[A] company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities.'"[279] In its guidance, the agency calls on companies to "limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by

---

276 Fed. Trade Comm'n, Start with Security (2015), *available at* , https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

277 Fed. Trade Comm'n, Protecting Personal Information (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

278 According to the court, guidance materials "that are neither regulations nor 'adjudications on the merit'" can satisfy fair notice principles. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257-59 (3d Cir. 2015). The court also noted that "consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to [Wyndham] in trying to understand the specific requirements imposed by [Section 5]." *Id.* at 257 n.22.

279 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? 22-23 (2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 24 n.108 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n on Opportunities and Challenges in Advancing Health Info. Tech. Before the Subcomm. on Info. Tech. and the Subcomm. on Health, Benefits, and Admin. Rules of the Oversight and Gov't Reform Comm., United States House of Representatives (Mar. 22, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/941063/160322commtestimonyhealthinfo.pdf; Fed. Trade Comm'n, Data Security, https://www.ftc.gov/datasecurity (last visited March 13, 2016).

law."[280] The agency also recommends a closely related principle of data minimization—the idea that companies should limit the data they collect, use, and retain to that which is needed to serve a legitimate business purpose.[281] Consistent with its guidance, the FTC has brought numerous actions against companies for failing to establish reasonable policies or procedures regarding the collection, use, retention, and disposal of consumer information.

1. Reasonable Collection

In *United States v. RockYou*, the FTC alleged that the online game operator collected users' email passwords as part of the website registration process, even though the passwords were not needed by the business.[282] The company's unnecessary collection of consumers' email passwords, among several other alleged failures in its storage and protection of consumer information, led the FTC to charge that RockYou broke its promises to "use[] commercially reasonable physical, managerial, and technical safeguards" and to "make[] commercially reasonable efforts to ensure the security of our systems."[283]

The lesson from *RockYou* comports with the FTC's guidance that companies avoid the use and collection of sensitive personal information that does not serve a legitimate business need.[284] For example, the agency counsels against using social security numbers as employee or customer identification numbers.[285] It also recommends adjusting settings on credit card-reading software so that credit card information is not retained permanently.[286] If a company must keep information for business reasons, the agency

---

280 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 27 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

281 *See, e.g.*, Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iv, 21, 34 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

282 Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶¶ 14, 16, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 26, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf.

283 *Id.* ¶¶ 15-16.

284 *See, e.g.*, Fed. Trade Comm'n, Start with Security 2 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iv, 21, 34 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Fed. Trade Comm'n, Protecting Personal Information 6-7 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

285 Fed. Trade Comm'n, Protecting Personal Information 6 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

286 *Id.* at 7.

recommends developing a written records retention policy to identify what information must be kept, how it long it is to be kept, and how it is to be secured and disposed.[287]

2. Reasonable Use

The agency has also taken actions against companies for unreasonable use of consumer data, including unnecessary use of real consumer information. In *In re Accretive Health*, the FTC alleged that the medical billing company used real people's personal information in employee training sessions and then failed to remove that information from employees' computers once the training ended.[288] Similarly, in *In re GeneLink*, the Commission alleged that a nutritional supplements and skincare products company gave sensitive consumer data to outside service providers that were developing software for the company, even though the service providers had no need for such sensitive data to develop the software.[289] In both cases, the FTC alleged that the practices were unfair, and, in *In re GeneLink*, alleged that the practices were also a violation of the company's promises.[290]

To avoid the unnecessary risk of exposing consumers' sensitive personal information, the agency advises that companies use fictitious information for training or application development purposes.[291]

3. Reasonable Retention

The FTC has also brought actions against companies for retaining consumer information beyond the time necessary to serve a legitimate business purpose. In *In re Life is Good*, the FTC alleged that the retailer violated its privacy policies by indefinitely storing consumer information, including credit card numbers, expiration dates, and security codes, without a business need.[292] Likewise, in *In re BJ's Wholesale Club*, the FTC alleged as unfair the retailer's practice of retaining customers' credit and debit card information used to process transactions for up to 30 days, which was long after the transactions were complete.[293] The *BJ*'s case shows that even a relatively short retention period in absolute terms may be considered unreasonable if a company retains information for longer than the time needed to serve business reasons.

The agency has stated that the reasonableness of a retention period depends, in part, on the type of relationship a company has with a consumer, as well as how the

---

287 *Id.* at 7.

288 Complaint ¶ 6(d), *In re Accretive Health, Inc.*, No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf.

289 Complaint ¶¶ 29(D), 30, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf.

290 Complaint ¶ 9, *In re Accretive Health, Inc.*, No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf; Complaint ¶¶ 31-33, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf.

291 Fed. Trade Comm'n, Start with Security 3 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

292 *In re Life Is Good, Inc.* 145 F.T.C. 192, 194 (2008) (complaint).

293 *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 467-68 (2005).

company uses the information.[294] Companies that have a direct relationship with consumers, for example, may be justified in retaining data for an extended period, while companies engaged in a one-time transaction with consumers may not have a basis to hold information beyond the time needed to process the transaction.[295] In its guidance on this issue, the agency has offered several examples of contexts in which appropriate lengths of data retention will vary. A consumer's mortgage company, for example, may need to maintain data for the life of the mortgage to ensure accurate payment tracking.[296] Likewise, a consumer's auto dealer may need to retain customer data for longer periods of time in order to manage service records.[297] By contrast, however, the agency has stated that "online behavioral advertising data often becomes stale quickly and need not be retained long."[298]

The reasonableness of a retention period also depends on the type of information at issue. The FTC advises that companies consider the nature of the data they collect when they decide how long to retain data.[299] Companies that collect data on children and teens, on consumers' real-time locations, or on consumers' biometrics may want to dispose of such data more quickly.[300]

---

294 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 28 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

295 *See id*.

296 *Id*.

297 *Id*.

298 *Id.; see also*, Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security ("[I]f you offer a location-based mobile game, get rid of the location data when it's no longer relevant."); Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies ii (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf ("[I]f a consumer creates an account on a website that allows her to virtually 'try on' eyeglasses, uploads photos to that website, and then later deletes her account on the website, the photos are no longer necessary and should be discarded.").

299 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 27 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

300 *Id*. at 29; Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies ii, 11-12, 18 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

4. Reasonable Disposal

The agency has pursued several actions against companies for claims that they failed to securely dispose of consumers' personal information.[301] For example, in *In re Rite Aid*, the FTC alleged that the use of open dumpsters by some pharmacies to discard consumers' and employees' personal information, including pharmacy labels and job applications, was unfair and contrary to the company's data security claims.[302] Similarly, in *In re CVS Caremark Corp.*, the agency alleged that the pharmacy engaged in unfair practices when it failed to obscure or redact consumers' and employees' personal information before disposing that information in publicly accessible dumpsters.[303]

The agency has also settled with companies for failing to properly dispose of consumer information when selling computer equipment containing such information. In *In re Goal Financial*, the FTC alleged that the student loan originator and servicer failed to live up to its data security promises when, among other things, its employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text.[304]

The FTC has offered a significant amount of guidance on secure disposal practices.[305] When disposing of old computers and portable storage devices, for example, the FTC recommends using available technology to wipe the devices.[306] For paper records, the agency recommends shredding, burning, or pulverizing.[307]

---

301 *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief ¶¶ 16-18, *United States v. PLS Fin. Servs., Inc.*, No. 1:12-cv-08334 (N.D. Ill. Oct. 17, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107plspaydaycmpt.pdf (payday loan and check cashing store's inadequate disposal procedures alleged to be contrary to company's claims); Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 11-14, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (mortgage broker's disposal of consumers' personal financial records in a publicly-accessible dumpster alleged to be contrary to company's claims); *In re Nations Title Agency, Inc.* 141 F.T.C. 323, 325, 327 (2006) (complaint) (failure to implement reasonable policies and procedures in key areas, such as the collection, handling, and disposal of personal information, contradicted company's claims).

302 *In re Rite Aid Corp.*, 150 F.T.C. 694, 697 (2010) (complaint).

303 Complaint ¶¶ 7, 8, *In re CVS Caremark Corp.*, No. C-4259 (F.T.C. June 18, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf.

304 *In re Goal Fin., LLC*, 145 F.T.C. 142, 144 (2008) (complaint).

305 *See, e.g.*, Fed. Trade Comm'n, Protecting Personal Information 16, 20-21 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

306 Fed. Trade Comm'n, Start with Security 14 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 21 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

307 Fed. Trade Comm'n, Protecting Personal Information 21 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

D. Reasonable Security Measures

The FTC has stated that it assesses the reasonableness of a company's data security practices based on the sensitivity and volume of consumer information the company holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities, among other things.[308]

1. Assessments of Information Sensitivity and Risks

The FTC has stated that it expects companies to assess their security vulnerabilities, including inventorying what consumer information they have, which employees or third parties have access to that information, and the life cycle of that information as it "moves into, through, and out of a business."[309] To protect sensitive and other consumer information, the agency advises that companies inventory all computers, mobile devices, flash drives, and other equipment to determine where data is stored.[310] It also advises talking to staff throughout the company, as well as to outside service providers, to understand how the personal information flows.[311] Depending on particular circumstances, "appropriate assessments may range from having a knowledgeable employee run off-the-shelf security software to having an independent professional conduct a full-scale security audit."[312]

---

308 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; Fed. Trade Comm'n, Big Data: A Tool for Inclusion or Exclusion? 22-23 (Jan. 2016), *available at* https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 24 n.108 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n on Opportunities and Challenges in Advancing Health Info. Tech. Before the Subcomm. on Info. Tech. and the Subcomm. on Health, Benefits, and Admin. Rules of the Oversight and Gov't Reform Comm., United States House of Representatives (Mar. 22, 2016), *available at* https://www.ftc.gov/system/files/documents/public_statements/941063/160322commtestimonyhealthinfo.pdf; Fed. Trade Comm'n, Data Security, https://www.ftc.gov/datasecurity (last visited March 13, 2016).

309 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; *see also* Fed. Trade Comm'n, Protecting Personal Information 4-5 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies ii, 10 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

310 Fed. Trade Comm'n, Protecting Personal Information 5-6 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

311 *Id.*

312 *Id.* at 10.

a. Information Sensitivity

The FTC considers the sensitivity of the collected information when evaluating whether a company has implemented reasonable data security measures. Dozens of FTC data security actions have involved personal information relating to finances,[313] health,[314] and minors.[315] The FTC has also provided guidance for companies that collect or use sensitive personal information, including blogs for businesses that use health data.[316]

b. Risk Scope and Control

Failure to identify potential security risks to consumer information or to implement measures to control for such risks has been a significant focus in FTC enforcement actions.[317] The agency has pursued several cases alleging that companies compromised consumers' personal information by failing to assess the risks posed by peer-to-peer (P2P) file-sharing software that employees install on their networks. In *In re EPN, Inc.*, the FTC charged as unfair the debt collector's failure to "[a]ssess risks to the consumer

---

313 *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR, 2013 WL 1222491 (D. Ariz. Mar. 25, 2013); *In re Goal Fin., LLC*, 145 F.T.C. 142 (2008); *FTC v. Cornerstone and Co.*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* http:// www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf; *FTC v. Bayview Sols.,* Case 1:14-cv-01830-RC (D.D.C. Aug. 27, 2014), *available at* http:// www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf; *In re Credit Karma, Inc.*, No. C-4480, 2014 WL 4252397 (F.T.C. Aug. 13, 2014); *In re Fandango, LLC*, No. C-4481, 2014 WL 4252396 (F.T.C. Aug. 13, 2014); *United States v. PLS Fin. Servs., Inc.*, No. 1:12-cv-08334 (N.D. Ill. 2012); *In re EPN, Inc.*, No. C-4370, 2012 WL 2150217 (F.T.C. June 7, 2012); *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012); *In re Dave & Buster's, Inc.*, 149 F.T.C. 1450 (2010); *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. filed Dec. 30, 2008); *In re Premier Capital Lending, Inc.*, No. C-4241, 2008 WL 4892987 (F.T.C. Nov. 6, 2008); *In re Life Is Good, Inc.* 145 F.T.C. 192 (2008); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019 (2006); *In re DSW, Inc.*, 141 F.T.C. 117 (2006); *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga.) (settlement entered Feb. 15, 2006), *available at* http:// www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf; *In re Nations Title Agency, Inc.*, 141 F.T.C. 323 (2006); *In re Superior Mortgage Corp.*, 140 F.T.C. 926 (2005); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

314 *See, e.g.*, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C.); *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C.); *In re Accretive Health, Inc.*, No C-4432 (F.T.C.); *In re Henry Schein Practice Solutions, Inc.*, No. C-4575 (F.T.C.); *In re LabMD, Inc.*, No. 9357 (F.T.C.); *In re CBR Systems, Inc.*, 155 F.T.C. 841 (2013); *In re EPN, Inc*, No. C-4370 (F.T.C.); *In re Rite Aid Corp.*, 150 F.T.C. 694 (2010); *In re CVS Caremark Corp.*, No. C-4259 (F.T.C.); *In re Eli Lilly & Co.*, 133 F.T.C. 763 (2002).

315 *In re GMR Transcription Services, Inc.*, No. C-4482 (F.T.C.); *In re TrendNET*, No. C-4426 (F.T.C.); *In re CBR Systems, Inc.*, 155 F.T.C. 841 (2013); *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal.); *In re Upromise, Inc.*, No. C-4351 (F.T.C.); *In re Microsoft Corp.*, 134 F.T.C. 709 (2002).

316 *See, e.g., Cora Han, Using Consumer Health Data?,* FTC Bus. Blog (Apr. 27, 2015 9:32 AM), https:// www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data; Cora Han, *Using Consumer Health Data: Some Considerations for Companies,* FTC Bus. Blog (Apr. 28, 2015 9:52 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/04/using-consumer-health-data-some-considerations-companies.

317 *See, e.g.*, *In re Goal Fin., LLC*, 145 F.T.C. 142, 144, 146 (2008) (complaint) (failure to adequately assess risks to information collected and stored in paper files and on computer network alleged to be contrary to company's claims); Complaint ¶¶ 7, 9-10, *In re CVS Caremark Corp.*, No. C-4259 (F.T.C. June 18, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf (failure to employ a reasonable process for discovering and remedying risks in disposal of personal information alleged to be unfair and contrary to company's claims); Complaint at 325, *In re Nations Title Agency, Inc.* 141 F.T.C. 323 (2006) (failure to assess risks to consumer information collected and stored online and offline alleged to be contrary to company's claims).

personal information it collected" and to "[a]dopt an information security plan that was appropriate for its networks and the personal information processed and stored on them."[318] The complaint alleged that EPN failed to use "reasonable measures to assess and enforce compliance with its security policies and procedures, such as scanning networks to identify unauthorized [P2P] file sharing applications" or to use "reasonable methods to prevent, detect, and investigate unauthorized access to personal information on its networks, such as by adequately logging network activity and inspecting outgoing transmissions to the Internet."[319] These and other failures allegedly led to the disclosure of company files containing personal financial and health information about thousands of debtors, including social security numbers, employer addresses, and in the case of healthcare clients, physician name, insurance number, and diagnosis code, on a P2P network.[320] Similarly, in *In re Franklin's Budget Car Sales, Inc.,* the FTC charged that the auto dealer's failure to assess risks to consumer information it collected and failure to adopt an appropriate security plan led to the exposure of personal information about thousands of consumers on a P2P network.[321]

c. Secure Design

The agency has also brought actions against companies for failing to design their products securely. In *In re Snapchat,* discussed in Section II(D)(2), the FTC alleged that the mobile messaging company failed to securely design its application, which would allow an individual to create an account using another consumer's phone number and to enable that individual to send and receive messages with the consumer's phone number.[322] According to the FTC's complaint, numerous consumers complained that their numbers had been misappropriated to create unauthorized Snapchat accounts.[323]

The agency has also taken action against companies that failed to verify the performance of advertised privacy and security features. In *In re TRENDnet*, the FTC charged that the electronics company failed to test the efficacy of its password protection option on the live internet feed of the company's IP cameras.[324] The FTC charged that the setting did not reasonably prevent unauthorized access to the live feeds and was therefore unfair.[325] The agency further alleged that the company's failure to "perform security review and testing" of the software through measures such as a security architecture review or software vulnerability and penetration testing was contrary to the company's

---

318 Complaint ¶ 6, *In re EPN, Inc.*, No. C-4370 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf.

319 *Id.*

320 *Id.* ¶¶ 4, 8.

321 Complaint ¶¶ 8-10, *In re Franklin's Budget Car Sales, Inc.*, No. C-4371 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf.

322 Complaint ¶¶ 34-36, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf (discussed *supra* Section II(D)(2)).

323 *Id.* ¶ 36.

324 Complaint ¶¶ 7, 8, *In re TRENDnet, Inc.*, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

325 *Id.* ¶ 18.

promises that it took reasonable steps to ensure security.[326] The agency has brought actions alleging comparable failures in *In re Snapchat*,[327] *In re ASUSTeK Computer*,[328] *In re Oracle*,[329] and *In re Upromise*.[330]

As the agency has stated in its guidance, reviewing and testing the functionality of security features is especially important because such practices help companies—and their service providers—to identify if there are "backdoors" to gaining control over personal information.[331]

2. Authentication and Access Limitations

The FTC has brought numerous cases against companies for failing to limit personnel and third-party access to consumer information.[332] Here, the agency's assessment of reasonableness has focused on whether individuals and organizations have a legitimate business need to access the information, as well as the types of measures implemented to exclude those without a valid need.

---

326 *Id*. ¶¶ 8, 14-17.

327 Complaint ¶¶ 3-19, *In re Snapchat, Inc.*, No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatcmpt.pdf (mobile messaging app over-promised that its messages would "disappear forever" and that "snap" sender would be immediately notified if a recipient took a screenshot of the snap) (discussed *supra* Section II(D)(2)).

328 Complaint ¶¶ 30, 37-46, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (hardware manufacturer's failure to use readily available secure protocols, to perform reasonable and appropriate software code review and testing, and to implement readily available, low-cost protections against well-known and reasonably foreseeable vulnerabilities alleged to be unfair and contrary to company's representations).

329 Complaint ¶¶ 20-22, *In re Oracle Corp.*, No. C-4571 (F.T.C. Mar. 28, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160329oraclecmpt.pdf (software company's failure to disclose, or to disclose adequately, that Java updates did not fully protect computers from malware alleged to be deceptive).

330 Complaint ¶ 14(b), *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf (failure to test company's toolbar before distributing it or to monitor the toolbar's operation for compliance with company policies alleged to be unfair and contrary to company's claims) (discussed *supra* Section II(C)(1)(b)).

331 Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii, 28-29 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; *see also* Fed. Trade Comm'n, Start with Security 10 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

332 *See, e.g.*, Complaint ¶¶ 20(c), 41-43, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (failure to limit access to personal information to employees and vendors needing access alleged to be deceptive in light of company's claims); Complaint ¶¶ 6(b), 9, *In re Accretive Health, Inc.,* No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf (medical billing company's failure to adequately restrict access to personal information based on employee need alleged to be unfair); *In re Dave & Buster's, Inc.*, 149 F.T.C. 1450, 1451-52 (2010) (complaint) (restaurant chain's failure to adequately restrict a third-party credit card processor's access to company network—for example, by restricting connections to specified IP addresses or granting temporary, limited access—alleged to be unfair).

a. Employee and Third-Party Access

In *In re Goal Financial*, the FTC alleged that the student loan originator and servicer's failure to restrict employee access to personal information stored in paper files and on its network was deceptive in light of the company's promises.[333] According to the agency's complaint, as a result of this and other lax practices, a group of employees transferred, without authorization, more than 7,000 consumer files containing sensitive information to third parties.[334]

The FTC also brought a case against Twitter for the social media company's failure to limit access to key administrative systems. The complaint alleged that the company granted almost all of its employees administrative control over Twitter's system, which allowed any employee to reset Twitter users' account passwords, to view users' nonpublic tweets, and to send tweets on users' behalf.[335] The agency alleged that this failure increased the risk that the misappropriation of a single employee's credentials could result in a serious breach, thereby contravening Twitter's representations to consumers about its security.[336]

The FTC has also entered into settlements with businesses that sold or provided consumer information without verifying the identities of their clients or the legitimacy of those clients' purposes in acquiring the information. In *United States v. ChoicePoint Inc.*, the FTC alleged violations of the Fair Credit Reporting Act and the FTC Act against the consumer reporting agency for accepting subscribers without verifying the identities or qualifications of those subscribers.[337] For example, ChoicePoint allegedly accepted, without further inquiry, "facially contradictory" information on subscriber applications, such as articles of incorporation that reflected that the business was suspended.[338] In addition to claimed violations of the FCRA, the FTC alleged that the company's lack of reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers was unfair under Section 5 and contrary to the company's representations that it implemented reasonable and appropriate measures to prevent unlawful access to consumers' information.[339] ChoicePoint agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle the charges.[340]

The agency alleged similar violations against Rental Research Services, a company that, according to the Commission, used sensitive financial data from other consumer reporting agencies to create reports that property owners use to assess potential

---

333 *In re Goal Financial, LLC*, 145 F.T.C. 142 , 144, 146 (2008) (complaint).

334 *Id.* at 144.

335 *In re Twitter, Inc.*, 151 F.T.C. 162, 164, 167 (2011) (complaint).

336 *Id.* at 167-69.

337 Complaint ¶¶ 15-32, *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf.

338 *Id.* ¶ 13(c).

339 *Id.* ¶¶ 15-32.

340 Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4, 17, *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. Feb. 15, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

renters.[341] In addition to alleging violations of the FCRA,[342] the FTC charged as unfair the company's failure to verify or authenticate the identities and business purposes of prospective customers.[343] According to the complaint, the company gave identity thieves posing as property owners an account with unlimited online access to consumers' credit reports, which the unauthorized parties used to access at least 318 reports.[344] The company, and the named officer, agreed to pay $500,000 in civil penalties to settle the complaint.[345]

In its guidance, the agency has stated that it expects companies to limit the access of employees, third parties, and customers according to the legitimate business needs of those parties.[346]

b. Network Segmentation

Reasonable restriction of access may also require a company to segment its network, which limits the ability of computers on a system to communicate with each other.[347] In *In re DSW*, the FTC alleged that the shoe retailer's failure to segment its network allowed hackers to use one in-store network to access personal information on other in-store and corporate networks—resulting in the breach of sensitive information relating to more than more than 1.4 million credit card and debit card accounts and nearly one hundred thousand checking accounts and driver's license numbers.[348] According to the complaint, this failure was unfair under Section 5.[349] Similarly, in *FTC v. Wyndham*, the FTC alleged deception and unfairness counts against the hospitality chain for failing to use "readily

---

341 Complaint for Civil Penalties, Injunctive and Other Equitable Relief ¶ 9, *United States v. Rental Research Servs., Inc.*, No. 0:09-CV-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrscmpt.pdf.

342 *Id.* ¶¶ 18-26.

343 *Id.*¶¶ 13, 17, 28-29.

344 *Id.* ¶ 15.

345 Stipulated Final Judgment and Order for Civil Penalties, Permanent Injunction, and Other Equitable Relief at 4, No. 0:09-CV-00524-PJS-JJK (D. Minn. Mar. 5, 2009), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2009/03/090305rrsorder.pdf.

346 Fed. Trade Comm'n, Start with Security 9 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 5 (2011) *available at*, https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

347 *See, e.g.*, Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶¶ 16, 29-30, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 26, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf (failure to segment servers alleged to be contrary to company's claims); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1021-22 (2006) (complaint) (failure to use readily available security measures to limit access between computers on network and between such computers and the internet alleged to be unfair).

348 *In re DSW Inc.*, 141 F.T.C. 117, 120 (2006) (complaint).

349 *Id.* at 119.

available security measures," such as firewalls, to limit access among the chain's property management systems, corporate network, and the internet.[350]

These actions are consistent with the agency's guidance that companies should protect particularly sensitive data by housing it in a separate, secure place on a company's network.[351]

c. Strong Authentication

Strong authentication procedures are also an important component of reasonable security. The FTC has initiated several cases against businesses for lacking adequate password policies and systems.[352] In *In re Twitter*, the FTC alleged that Twitter let employees use common dictionary words—as well as passwords they were already using for other accounts—as administrative passwords.[353] According to the complaint, Twitter's failure to require employees to use unique or complex passwords left the company vulnerable to hackers who could use password-guessing tools or passwords stolen from other services to access Twitter's system.[354]

The FTC has also taken action against companies that failed to protect their authentication systems from outsider bypass. In *In re ASUSTeK Computer Inc.*, the agency alleged that design flaws in the computer hardware maker's router allowed unauthorized individuals to access a consumer's "private personal cloud" account by sending a specific command or entering a specific URL in a web browser, thereby bypassing the need to use the consumer's login credentials.[355] Similarly, in *In re Lookout Services, Inc.*, the FTC alleged that outsiders could bypass login requirements and access the company's sensitive

---

350 First Amended Complaint 10, ¶ 24(a), *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

351 Fed. Trade Comm'n, Start with Security 7 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

352 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶ 24(f), *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (allowing use of easily guessed passwords to access systems alleged to be unfair and contrary to company's claims); Complaint ¶¶ 18, 30, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (allowing consumers to retain the same default login credentials on every router, along with other security design flaws, alleged to be unfair and contrary to company's claims); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1021-22 (2006) (complaint) (failure to use strong passwords, along with other security failures, alleged to be unfair); *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 534, 536-37 (2011) (complaint) (failure to require strong user passwords alleged to be unfair and contrary to company's claims); *In re Nations Title Agency, Inc.,* 141 F.T.C. 323, 325, 327-28 (2006) (complaint) (failure to implement reasonable access controls, such as strong passwords, to prevent unauthorized access to stored personal information alleged to be deceptive in light of company's claims).

353 *In re Twitter, Inc.*, 151 F.T.C. 162, 167-68 (2011) (complaint).

354 *Id.* at 168-69.

355 Complaint ¶¶ 7, 10, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf.

employee information by typing a URL into a web browser.[356] The FTC charged that these failures were unfair and contrary to the company's promises.[357]

Strong authentication may also require implementing measures to guard against brute force attacks, which employ software programs to repeatedly guess different combinations of user login IDs and passwords in an attempt to gain access to a system. In its actions against Lookout Services and Twitter, the FTC alleged as unfair and deceptive the companies' failure to suspend or disable user credentials even after the companies' systems experienced a number of unsuccessful login attempts.[358] And in *FTC v. Wyndham*, the FTC alleged as unfair and deceptive Wyndham's failure to defend against brute-force attacks seeking access to an administrator account.[359]

The FTC has offered a variety of concrete tips for strengthening passwords and authentication procedures.[360] For example, it recommends that companies require employees and users to choose complex passwords and to instruct them not to use the same or similar passwords across multiple accounts.[361] It also recommends companies adopt policies and procedures to suspend or disable accounts after repeated failed login attempts and consider additional forms of protections, such as two-factor authentication.[362] But as the agency has noted, data security is an evolving process. In a recent blog post, the FTC's Chief Technologist discussed research showing that mandatory password changes may offer less security benefits than previously thought, in part because users forced to regularly change passwords tend to create passwords that follow predictable patterns—enabling attackers to more easily guess the next password.[363] The bottom line is that companies should continually re-evaluate their authentication methods as risks, technologies, and the latest thinking on security continue to evolve.

---

356 *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 534-35 (2011) (complaint).

357 Complaint ¶¶ 37-46, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf; *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 536-37 (2011) (complaint).

358 *Id*. at 534-37); *In re Twitter, Inc.*, 151 F.T.C. 162, 167-69 (2011) (complaint).

359 First Amended Complaint for Injunctive and Other Equitable Relief ¶ 26, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

360 *See, e.g.* Fed. Trade Comm'n, Start with Security 5 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 12-13 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

361 Fed. Trade Comm'n, Protecting Personal Information 12 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; Fed. Trade Comm'n, Start with Security 5 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

362 Fed. Trade Comm'n, Protecting Personal Information 5 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

363 Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, Tech@FTC Blog (Mar. 2, 2016, 10:55 AM), https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes.

3. Security for Information throughout Its Life Cycle

Through its enforcement actions and guidance, the FTC has made clear that personal information in all formats must be reasonably secured throughout its life cycle.[364]

a. Encryption

Securing information in an electronic format will often require some form of encryption. The FTC has brought several cases against companies alleged to have failed to encrypt or to adequately secure consumer data. In *In re Henry Schein Practice Solutions, Inc.*, a dental software company purportedly represented that it used industry-standard encryption and that its product helped to protect patient data as required by HIPAA.[365] Instead of using encryption, however, the business used a less complex method of data masking that did not meet the National Institute of Standards and Technology (NIST) standard recommended by the Department of Health and Human Services for companies seeking to comply with HIPAA.[366] In its proposed complaint, the FTC alleged that the company's inadequate data obfuscation was deceptive in light of the company's claims.[367] The settlement requires the company to pay $250,000 as an equitable remedy and to notify customers that its software uses a less complex encryption than the standard recommended by the NIST.[368]

The agency has also taken action against companies that allegedly failed to properly configure the encryption they employed. In *In re Fandango* and *In re Credit Karma*, the FTC alleged that the companies used SSL encryption in their mobile apps, but turned off a critical security process known as "SSL certificate validation" without implementing any compensating security measures.[369] This failure made the companies' applications vulnerable to man-in-the-middle attacks in which unauthorized third parties position themselves between the online service and an application by presenting an invalid

---

364 Fed. Trade Comm'n, Start with Security 6-7, 13 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 30 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

365 Complaint ¶¶ 5, 9, 12, *In re Henry Schein Practice Sols., Inc.*, No. C-4575, *available at* https://www.ftc.gov/system/files/documents/cases/160523hspscmpt.pdf.

366 *Id.* ¶¶ 8, 10.

367 *Id.* ¶¶ 19-22.

368 Decision and Order at 4, 5, *In re Henry Schein Practice Sols., Inc.,* No. C-4575 (Jan. 5, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160523hspsdo.pdf.

369 Complaint ¶¶ 17, 19, 21(a), *In re Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint ¶¶ 16, 18, 19(a), *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

certificate to the application.[370] The FTC alleged that Fandango and Credit Karma's failures contravened their privacy and security promises.[371]

(1) Transmission

The FTC's data security cases involving the transmission of consumer data have focused on a number of different means of data transmission. Some of the FTC's cases in this area have centered around companies' alleged failures to secure the technology devices used by their employees to transport consumer information.[372] Other cases have focused on an alleged failure to use encryption (or adequate encryption) during the transmission of consumer information.[373] In *FTC v. Rennert* and *In re TRENDnet*, the FTC alleged that the companies' failures to use secure connections when transmitting consumer information contradicted the companies' representations.[374] The FTC also alleged as unfair TRENDnet's transmission of user login credentials in clear, readable text, despite the availability of free software that would have enabled the company to secure such transmissions.[375]

Even within a company, encryption of personal information during transmission may be necessary. In *In re Superior Mortgage Corp.*, the FTC alleged that, although the company used SSL encryption to secure the transmission of sensitive personal information between a customer's web browser and the company's website server, the company's third-party service provider decrypted the information once it reached Superior Mortgage's server and subsequently emailed the decrypted information in clear, readable text to the

---

370 Complaint ¶ 11, *In re Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint ¶ 10, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

371 Complaint ¶¶ 27, 30, *In re Credit Karma, Inc.*, No. C-4480 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmacmpt.pdf; Complaint ¶ 25, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

372 *See, e.g.*, Complaint ¶¶ 6(a), 7, 9 *In re Accretive Health, Inc.*, No C-4432 (F.T.C. Feb. 5, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140224accretivehealthcmpt.pdf (employee's leaving a laptop containing more than 600 files with information related to 23,000 patients in locked passenger compartment of a car, which was then stolen, alleged to be unfair); *In re CBR Sys., Inc.*, 155 F.T.C. 841, 844-45 (2013) (complaint) (employee's leaving unencrypted backup tapes, laptop, and an external hard drive with sensitive information in car alleged to be deceptive in light of company's promises).

373 *See, e.g.*, Complaint ¶¶ 20(a), 38-40, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (transmitting and storing personal information in clear, readable text violated company's representations).

374 Complaint ¶ 34, *FTC v. Rennert*, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm; Complaint ¶ 8, *In re TRENDnet*, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

375 Complaint ¶ 8, *In re TRENDnet*, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

company's headquarters and branch offices.[376] According to the complaint, this practice contradicted the company's data security claims.[377]

(2) Storage

The FTC has taken action against companies for claims that the companies employed inadequate or no encryption to protect stored information.[378] The Commission has also settled with companies that allegedly put portfolios of consumer debt containing highly sensitive personal and financial information on public websites for purposes of selling those portfolios.[379]

(3) Remote Access

Failure to ensure that computers with remote access to company networks have appropriate endpoint security has also been an area of significant FTC enforcement.[380] In *FTC v. Premier Capital Lending*, the FTC alleged that a mortgage lender's failure to assess a business client's security before activating a remote login account for that client was contrary to the company's claim that it "maintain[ed] physical, electronic, and

---

376 *In re Superior Mortgage Corp.*, 140 F.T.C. 926, 930 (2005) (complaint).

377 *Id.*

378 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 24(b), 47-49, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (storage of payment card information in clear, readable text alleged to be unfair); Complaint ¶ 8, *In re TrendNET*, No. C-4426 (Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf (storage of user login credentials in clear, readable text, despite existence of free software enabling securing of stored credentials, alleged to be unfair and contrary to company's claims); *In re Ceridian Corp.*, 151 F.T.C. 514, 516 (2011) (complaint) (indefinite storage of personal information in clear, readable text without a business need alleged to be unfair and contrary to company's claims); Complaint ¶¶ 20(a), 38-40, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (transmitting and storing personal information in clear, readable text alleged to be contrary to company's claims); *In re Guess?, Inc.*, 136 F.T.C. 507, 512-13 (2003) (complaint) (storage of consumers' personal information, including credit card numbers, in clear, readable text alleged to be contrary to company's claims); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102, 106 (2005) (complaint) (failure to maintain sensitive information in an encrypted format alleged to be contrary to to company's claims); Complaint ¶¶ 34, 43-44 *FTC v. Rennert*, No. CV-S-00-0861-JBR (D. Nev. July 12, 2000), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2000/07/ftc.gov-iogcomp.htm (failure to encrypt customer information alleged to be contrary to company's claims).

379 *See, e.g.*, Complaint for Permanent Injunction and Other Equitable Relief ¶¶ 28-30, *FTC v. Cornerstone and Company, LLC*, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf (online posting of consumers' bank account and credit card numbers, birth dates, contact information, employers' names, and debt-related information alleged to be unfair); Complaint for Permanent Injunction and Other Equitable Relief ¶¶ 22, 31-33, *FTC v. Bayview Sols.*, LLC, Case 1:14-cv-01830-RC (D.D.C. Oct. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf (online posting of unencrypted documents containing consumers' names, addresses, credit card numbers, bank account numbers, and debt-related information alleged to be unfair) (discussed *supra* Section II(E)(3)).

380 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 24(c), 44-49, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (allowing hotels to connect to network without ensuring that they implemented adequate information security policies and procedures alleged to be unfair and contrary to company's claims).

procedural safeguards that comply with federal standards."[381] When hackers accessed the client's system, they stole its remote login credentials and used those to obtain consumers' sensitive personal information.[382]

Similarly, in the agency's first action against LifeLock, the FTC alleged that the business's failure to install antivirus programs on computers that employees used to remotely access Lifelock's network was inconsistent with the company's claim that it used "highly secure physical, electronic, and managerial procedures."[383] The consent order in *In re Lifelock* requires the company, and its two co-founders, to establish a comprehensive information security program and to obtain independent third-party assessments every two years.[384] In 2015, the FTC filed a contempt action against LifeLock for violating the 2010 settlement by, among other things, failing to establish and maintain a comprehensive information security program and falsely advertising that it protected consumers' sensitive data with the same high-level safeguards as financial institutions.[385] Lifelock settled the action, agreeing to pay $100 million in equitable monetary relief.[386]

The FTC recommends that companies consider using encryption if they allow remote access to the computer network by employees or by service providers.[387]

(4) Sensitive Information

Through its guidance and enforcement actions, the FTC has identified several types of information that benefit from strong encryption during storage or transmission. Passwords and credentials, for example, must be stored securely.[388] Biometric data may

---

381 Complaint ¶¶ 1, 19-21, *In re Premier Capital Lending, Inc.*, No. C-4241 (F.T.C. Dec. 10, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081206pclcmpt.pdf.

382 *Id.*

383 Complaint ¶¶ 19(f), 20(f), 35-37, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf.

384 Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendants Lifelock and Davis §§ II, III, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 9, 2010), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockstip.pdf; Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief as to Defendant Maynard §§ II, III, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 9, 2010), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309maynardstip.pdf.

385 Notice of Lodging Proposed Documents Under Seal at 1-2, *FTC v. LifeLock, Inc.*, 2:10-cv-00530-MHM (D. Ariz. July 21, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/150721lifelocknotice.pdf.

386 Amended Order at 4, *FTC v. LifeLock, Inc.*, 2:10-cv-00530-MHM (D. Ariz. Jan. 4, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160105lifelockorder.pdf.

387 Fed. Trade Comm'n, Protecting Personal Information 15 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

388 *See, e.g.*, Complaint ¶¶ 10(e), 14, *In re Reed Elsevier Inc.*, No. C-4226 (F.T.C. July 29, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801reedcomplaint.pdf (allowing customers to store user credentials in a vulnerable format alleged to be unfair); *In re Guidance Software, Inc.*, 143 F.T.C. 532, 535-36 (2007) (complaint) (storing network user credentials in clear, readable text alleged to be deceptive in light of company's claims).

also require some form of protection.[389] FTC guidance also makes clear that companies should encrypt sensitive information that is sent to third parties over public networks and should consider encrypting sensitive information stored on internal computer networks, disks, or portable storage devices.[390] For mobile applications, the agency recommends transit encryption for usernames, passwords, and other important data, such as application programming interface (API) keys.[391]

b. Physical Security

The physical security of information is also an important component of reasonable security. In *In re Lifelock*, the agency alleged that the company's practice of leaving faxed documents containing consumers' personal information in an open and easily accessible area contradicted the company's security representations.[392] Similarly, in *In re Gregory Navone*, the FTC charged that the mortgage broker's storage of sensitive consumer information in boxes in his garage, among other practices, violated the FCRA and contradicted the company's claims.[393]

The FTC has stated that it expects companies and their employees and service providers to take measures to protect paper and other physical materials containing personal information.[394] The agency recommends that paper documents containing personal information be stored in a locked room or container, and that access to the locked areas and containers be limited to employees with a legitimate business need.[395] As for the physical security of laptops and portable devices, the agency advises that they be stored in a secure place.[396] If a company stores consumer data on other portable devices, it

---

389 Fed. Trade Comm'n, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies 17 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf ("[E]ven if a company does not itself intend to implement facial recognition technologies, it should consider putting protections in place that would prevent unauthorized scraping of the publicly available images it stores in its online database.").

390 Fed. Trade Comm'n, Protecting Personal Information 10 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

391 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security ("If you use HTTPS, use a digital certificate and ensure your app checks it properly.").

392 Complaint ¶¶ 20(h), 35-37, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf.

393 Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 12-14, 15-16, 19-25, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf.

394 Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement 1 (Jan. 31, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf; Fed. Trade Comm'n, Start with Security 13 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 8-9 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

395 Fed. Trade Comm'n, Protecting Personal Information 8-9 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

396 *Id* . at 13.

may also want to consider adding an "auto-destroy" function so that any data on a stolen device will be destroyed if an unauthorized individual tries to use it.[397]

4. Ongoing Monitoring

The FTC has stated that it expects companies to implement security on an ongoing basis.[398] Indeed, the agency has brought numerous actions against companies for failing to monitor the security of its service providers, activity on their networks, and security issues reported by consumers, researchers, or other third parties.

a. Network Activity

The FTC has brought numerous actions in which companies allegedly increased the risk or scope of a data breach by failing to monitor activity on their networks or to employ sufficient measures to detect unauthorized access.[399] In *In re Dave & Busters*, the FTC alleged that the company's failure to use an intrusion detection system and to monitor system logs for suspicious activity was unfair.[400] According to the complaint, an intruder was able to connect numerous times to the company's networks, to install unauthorized software, and to intercept personal information in transit from in-store networks to the company's credit

---

397 Fed. Trade Comm'n, Protecting Personal Information 13 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

398 *See, e.g.*, Fed. Trade Comm'n, Start with Security 8 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

399 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶¶ 24(g), 27, *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012) *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (failure to employ reasonable measures to detect and prevent unauthorized access to network or to conduct security investigations alleged to be unfair and contrary to company's claims); Complaint ¶ 6, *In re EPN, Inc.*, No. C-4370 (F.T.C. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf (failure to scan networks to identify unauthorized P2P file sharing applications on networks and failure to adequately log network activity and inspect outgoing transmissions alleged to be unfair); *In re Ceridian Corp.*, 151 F.T.C. 514, 516 (2011) (failure to employ reasonable measures to detect and prevent unauthorized access to personal information alleged to be unfair and contrary to company's claims); *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 535 (2011) (complaint) (failure to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as by employing an intrusion detection system and monitoring system logs, alleged to be unfair and contrary to company's claims); *In re Life Is Good, Inc.*, 145 F.T.C. 192, 194 (2008) (complaint) (failure to use readily available security measures to monitor and control connections from network to the internet and failure to employ reasonable measures to detect unauthorized access alleged to be contrary to company's claims); *In re CardSystems Sols., Inc.*, 142 F.T.C. 1019, 1021 (2006) (complaint) (failure to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations alleged to be unfair); *In re Nations Title Agency, Inc.*, 141 F.T.C. 323, 325, 327 (2006) (complaint) (failure to employ reasonable measures to detect and respond to unauthorized access to personal information or to conduct security investigations alleged to be contrary to company's claims); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465, 467 (2005) (complaint) (failure to employ sufficient measures to detect unauthorized access or conduct security investigations alleged to be unfair); *In re Microsoft Corp.*, 134 F.T.C. 709, 712 (2002) (complaint) (failure to implement reasonable and appropriate procedures to detect possible unauthorized access, failure to monitor system for potential vulnerabilities, and failure to record and retain system information sufficient to perform security audits and investigations alleged to be contrary to company's claims) (discussed *supra* Section II(A)(2)).

400 *In re Dave & Buster's, Inc.*, 149 F.T.C. 1449, 1451-52 (2010) (complaint).

card processing company—all of which allegedly led to several hundred thousand dollars of fraudulent charges on consumers' credit and debit cards.[401]

As these cases make clear, companies should monitor for unusual activity, including multiple failed login attempts from unknown users or computers and higher-than-average traffic.[402] The FTC also recommends that companies use an intrusion detection system and maintain a central log file of security-related information, which can help identify compromised computers if there is an attack.[403]

b. Service Providers and Clients

The FTC has stated that it expects companies to retain service providers that are capable of maintaining reasonable security and to monitor or verify that those service providers are indeed complying with the company's security requirements.[404] In *United States v. ChoicePoint Inc.*, the agency alleged as deceptive and unfair the data broker's failure to identify unauthorized activity by subscribers, even after receiving subpoenas from law enforcement authorities alerting the company to fraudulent subscriber accounts.[405] Similarly, in *In re Premier Capital Lending*, the agency alleged that the mortgage lender's failure to use readily available information to review access requests made by one account, such as spikes in the number of requests or blatant irregularities in the information used to make the requests, contradicted Premier Capital's representations that it used reasonable and appropriate data security measures.[406]

The FTC has brought several actions against companies for failing to include contractual provisions that require a service provider to adopt reasonable security precautions.[407] In *In re GMR Transcription Services*, the company hired service providers to transcribe sensitive audio files, but failed to require those providers to take reasonable

---

401 *Id.*

402 Fed. Trade Comm'n, Protecting Personal Information 16 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

403 *Id.*

404 Fed. Trade Comm'n, Start with Security 11 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

405 Complaint ¶¶ 14, 25-32, *United States v. ChoicePoint Inc.*, No. 06-CV-0198 (N.D. Ga. Jan. 30, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf.

406 Complaint ¶¶ 14(c), 19-21, *In re Premier Capital Lending, Inc.*,, No. C-4241 (F.T.C. Dec. 10, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/12/081206pclcmpt.pdf.

407 *See, e.g.*, Complaint ¶¶ 29(B), 31-33, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf (failure to require, by contract, that service providers implement and maintain appropriate safeguards for consumers' personal information alleged to be unfair and contrary to company's claims); Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 11, 17-18, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (failure to enter into agreements requiring service providers to safeguard information alleged to be contrary to company's claims).

security measures, which enabled hackers to post on the internet many files containing consumers' confidential health-related information.[408]

The FTC has also taken action against companies that failed to verify that their service provider actually complied with security requirements.[409] For example, in *In re Upromise*, the company purportedly claimed that its toolbar, which collected consumers' browsing information, would use a filter to remove any personally identifiable information before transmission.[410] According to the FTC, however, Upromise failed to verify that the service provider hired to create the toolbar actually implemented the promised security.[411] As a result, the toolbar collected sensitive personal information, including financial account numbers, and transmitted that information in clear text.[412] The agency alleged that this failure was unfair and contrary to Upromise's representations that it encrypted information transmitted by consumers using the toolbar and that it took other reasonable measures to protect consumer data.[413] For additional discussion of the case, see *supra* Section II(C)(1)(b).

In its guidance, the FTC recommends investigating a service provider's data security practices, for example, by visiting their facilities.[414] It also advises that companies consider requiring service providers to give notification of any security incidents, even if the incident may not have led to an actual compromise of company data.[415]

---

408 Complaint ¶¶ 11-13, 17-21, *In re GMR Transcription Servs., Inc.*, No. C-4482 (F.T.C. Aug. 14. 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.

409 *See, e.g.*, Fed. Trade Comm'n, Start with Security 11 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Complaint ¶¶ 29(C), 30, 31-33, *In re Genelink, Inc.*, Nos. C-4456, C-4457 (F.T.C. May 8, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140512genelinkcmpt.pdf (failure to provide reasonable oversight of service providers, for instance by requiring that they implement simple, low-cost, and readily available defenses to protect consumers' personal information, alleged to be unfair and contrary to company's claims); *In re Nations Title Agency, Inc.* 141 F.T.C. 323, 325, 327-28 (2006) (complaint) (failure to provide reasonable oversight of service providers' handling of personal information alleged to be unfair and contrary to company's claims).

410 Complaint ¶¶ 5, 14(d), *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf.

411 *Id.* ¶¶ 10, 14(a).

412 *Id.* ¶¶ 16-21.

413 *Id.* ¶¶ 16-21.

414 Fed. Trade Comm'n, Protecting Personal Information 19 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

415 *Id.*

c. Security Complaints and Reports

Companies that lack a process for receiving and addressing security-related reports and complaints also been the subject of FTC enforcement.[416] In *In re TRENDnet*, the company allegedly failed to implement any process to monitor security vulnerability reports from third parties such as researchers and academics, despite the availability of free tools to conduct such monitoring.[417] In *In re Fandango*, the company relied on its general customer service system to respond to warnings about security risks, which led to a report from a security researcher being incorrectly marked as "resolved" without being flagged for further review.[418]

The FTC recommends that companies review and address complaints and reports of security vulnerabilities, and that they use a dedicated email address, like "security@yourcompany.com," to receive such submissions.[419]

5. Addressing Common Vulnerabilities

Companies' failures to test for and address commonly known and reasonably foreseeable vulnerabilities have led to FTC enforcement. For example, in *In re Lookout Services*, the FTC charged that the company failed to adequately test its web application for widely known security flaws, including one called "predictable resource location," which enables users to easily predict patterns and manipulate URLs in order to gain access to secured web pages.[420] As a result, a hacker could bypass the web application's authentication screen and gain unauthorized access to the company's databases.[421]

In other actions, the FTC alleged that companies failed to assess their applications for well-known vulnerabilities, such as Structured Query Language (SQL) injection attacks

---

416 *See, e.g.*, Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Complaint ¶ 30(e), *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf (failure to maintain an adequate process for receiving and addressing security vulnerability reports from third parties alleged to be unfair and contrary to company's claims); *In re HTC America Inc.*, 155 F.T.C. 1617, 1619 (2013) (complaint) (lack of process for receiving and addressing reports about security vulnerabilities alleged to be unfair and contrary to the company's claims).

417 Complaint ¶ 8(c), No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

418 Complaint ¶ 17, *In re Fandango, LLC*, No. C-4481 (F.T.C. Aug. 13, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

419 Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

420 *In re Lookout Servs., Inc.*, 151 F.T.C. 532, 535 (2011) (complaint).

421 *Id.* at 534-536.

or Cross-Site Scripting (XSS) attacks.[422] In *In re Guess*, the FTC alleged that the retailer failed to protect against SQL injection and other commonly known attacks by failing to test or otherwise assess its website's vulnerability to such attacks.[423]

a. Industry-Tested and Accepted Methods

Failure to use industry-tested and accepted methods is a factor in assessing the reasonableness of a company's data security practices.[424] For example, in *In re ValueClick*, the FTC alleged that the company stored sensitive customer information collected online in a database that used non-standard encryption.[425] Unlike widely accepted encryption algorithms that are extensively tested, ValueClick's method allegedly used a simple alphabetic substitution system that was subject to significant vulnerabilities.[426] The agency charged that the use of this weaker method, among other practices, was inconsistent with the company's representation that it used industry-standard security measures.[427] The FTC further alleged that ValueClick violated the CAN-SPAM Act by sending consumers emails with deceptive subject headers.[428] ValueClick agreed to pay a $2.9 million civil penalty to settle the charges.[429]

Failure to use inexpensive, readily available tools to improve security is another factor in assessing reasonableness. In *In re Petco* and in *In re Life is Good*, the FTC alleged that the companies' respective failures to use simple, readily available, and low-cost defenses that would have blocked SQL injection attacks was contrary to the companies'

---

422 *See, e.g.*, *In re Life Is Good, Inc.*, 145 F.T.C. 192, 194 (2008) (complaint) (failure to adequately assess the vulnerability of web application and network to SQL injection attacks alleged to be inconsistent with company's representations); *In re Cardsystems Sols., Inc.*, 142 F.T.C. 1019, 1021 (2006) (complaint) (failure to adequately assess the vulnerability of web application and computer network to SQL injection attacks alleged to be unfair); *In re Ceridian Corp.*, 151 F.T.C. 514, 516 (2011) (failure to protect network from SQL attacks alleged to be unfair and contrary to the company's claims); Complaint for Civil Penalties, Permanent Injunction, and Other Relief ¶ 16, *United States v. RockYou, Inc.*, No. CV-12-1487 (N.D. Cal. Mar. 26, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf (failure to protect website from commonly known or reasonably foreseeable attacks such as SQL injection attacks or XSS attacks contradicted company's claims).

423 *In re Guess?, Inc.*, 136 F.T.C. 507, 510, 512 (2003) (complaint).

424 *See, e.g.*, Complaint ¶ 8, *In re Henry Schein Practice Sols., Inc.*, No. C-4575 (F.T.C. May 20, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160105scheincmpt.pdf (use of data masking, instead of encryption, contradicted company's claim that it used industry-standard encryption and that its product helped to protect patient data as required by HIPAA).

425 Complaint for Civil Penalties, Permanent Injunction, and Other Equitable Relief ¶¶ 41, 47-48, *United States v. ValueClick, Inc.*, No. CV08-01711MMM(RZx) (C.D. Cal. Mar. 13, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317complaint.pdf.

426 *Id.*

427 *Id.* ¶¶ 38-39.

428 *Id.* ¶¶ 33, 55-56.

429 Stipulated Final Judgment for Civil Penalties and Permanent Injunctive Relief at 8, *United States v. ValueClick, Inc.*, No. CV08-01711MMM(RZx) (C.D. Cal. Mar. 13, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/03/080317judgment.pdf.

data security claims.[430] Similarly, in *In re HTC*, the agency alleged that the mobile device manufacturer not only used less secure methods for protecting communications, but also failed to use simple code to fix its device vulnerabilities.[431] The agency alleged that these practices, among others, were unfair and contrary to HTC's claims.[432] The consent order requires HTC to develop security patches to fix its various security vulnerabilities and to notify consumers about the availability of the patches.[433]

Consistent with its enforcement actions, FTC guidance recommends that companies use methods for addressing security vulnerabilities that experts already have tested and found to be effective.[434]

b. Platform Guidelines and Settings

The extent to which a company follows platform guidelines or security protections built into operating systems may also be a factor in assessing the reasonableness of a security practice. The FTC's complaints in *In re Fandango* and *In re Credit Karma* also charged the companies with failing to follow iOS and Android security guidelines for developers.[435] Likewise, in *In re HTC*, the agency alleged that the company undermined the Android operating system's permissions-based model by pre-installing an app that, if exploited, would give any third-party app access to the phone's microphone.[436] According to the complaint, HTC also pre-installed another app that could download and install apps outside of the normal Android permission process.[437]

The FTC recommends that companies understand and follow platform guidelines and security protections built into operating systems.[438] Where necessary, companies may have to implement security measures beyond those offered by the platform.[439]

---

430 *In re Life Is Good, Inc.*, 145 F.T.C. 192, 194 (2008) (complaint); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102, 105-06 (2005) (complaint).

431 *In re HTC America Inc.*, 155 F.T.C. 1617, 1620-21, 1625 (2013) (complaint).

432 *Id.* at 1627-28.

433 *In re HTC America Inc.*, 155 F.T.C. 1617, 1631-35 (2013) (decision and order).

434 Fed. Trade Comm'n, Start with Security 6 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

435 *See supra* Section III(D)(3)(a).

436 *In re HTC America Inc.*, 155 F.T.C. 1617, 1620-21 (2013) (complaint).

437 *Id.*

438 Fed. Trade Comm'n, Start with Security 10 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

439 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

c. Third-Party Software

The FTC has taken action against companies that failed to update and patch third-party software.[440] In *In re TJX Companies*, the FTC alleged that the retailer failed to patch or update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the company's defenses.[441] An intruder allegedly exploited this and other failures, compromising tens of millions of consumer credit and debit payment cards.[442]

The FTC recommends that companies establish a reasonable process to regularly update and patch third party software.[443] Such a process may involve regularly checking expert websites and software vendors' websites for alerts about new vulnerabilities, as well as implementing policies for installing vendor-approved patches.[444] Companies may also want to follow general and library-specific mailing lists and create a plan for shipping security updates to consumers, if necessary.[445] In the context of the Internet of Things (IOT), the FTC has asked companies to pay particular attention to patching known vulnerabilities where feasible.[446] As the agency explained, many "[IOT] devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date [IOT] devices that are vulnerable to critical, publicly known security or privacy bugs."[447]

---

440 *See, e.g.*, Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; Fed. Trade Comm'n, Protecting Personal Information 10, 17 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; Complaint ¶¶ 20(d), 35-37, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530-MGM (D. Ariz. Mar. 8, 2010), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2010/03/100309lifelockcmpt.pdf (failure to use readily available security measures to routinely prevent unauthorized access to personal information, such as by installing patches and critical updates on its network, contradicted company's security claims).

441 Complaint ¶ 8(e), *In re TJX Cos., Inc.*, No. C-4227 (F.T.C. July 29, 2008), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.

442 *Id.* ¶¶ 9-11.

443 Fed. Trade Comm'n, Start with Security 12 (2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

444 Fed. Trade Comm'n, Protecting Personal Information 10 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

445 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

446 Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World iii (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

447 *Id.* at 31.

6. Planning for Security Incidents

The agency has brought several actions against companies for failing to establish a plan for responding to security incidents.[448] In *In re EPN, Inc.*, the agency alleged as unfair the debt collector's failure to adopt an appropriate information security plan, including any type of "incident response plan."[449] These failures, among others, allegedly led to the disclosure of files containing financial and health information about thousands of debtors, including social security numbers, employer addresses, and in the case of healthcare clients, physician names, insurance numbers, and diagnosis codes, on a public P2P network.[450]

Planning for security incidents may also require establishing policies and procedures for notifying affected consumers. The FTC brought an action against ASUSTeK Computer for failing to notify customers of firmware updates until well after the company learned of the issues.[451] The agency alleged that the failure was unfair and contrary to ASUSTeK's data security promises.[452]

The FTC recommends that companies create a plan for responding to security incidents that includes investigating security incidents immediately, closing off vulnerabilities and threats to personal information, knowing whom to notify in the event of an incident, and designating a senior employee to coordinate and implement the plan.[453]

7. Training and Designating People

In many ways, the lynchpin to implementing reasonable data security is people—people who design, create, and update products and services, people who interact with consumer information, and people who establish and carry out policies and procedures needed to effect sound security. The centrality of people to sound security helps to

---

448 *See, e.g.*, First Amended Complaint for Injunctive and Other Equitable Relief ¶ 24(i), *FTC v. Wyndham Worldwide Corp.*, No. 2:12-cv-01365-PGR (D. Ariz. Aug. 9, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf (failure to follow proper incident response procedures, including failing to monitor computer network for malware used in a previous intrusion, alleged to be unfair and contrary to company's claims); Complaint ¶ 8(b), *In re Franklin's Budget Car Sales, Inc.*, No. C-4371 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf (failure to adopt an incident response plan alleged to be deceptive in light of company's claims).

449 Complaint ¶¶ 6, 11 *In re EPN, Inc.*, No. C-4370 (F.T.C. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf.

450 *Id.* ¶¶ 8, 10.

451 Complaint ¶ 13, *In re ASUSTeK Comput. Inc.*, No. C-4587 (F.T.C. July 18, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/1607asustekcmpt.pdf.

452 *Id.* ¶ 30(g).

453 Fed. Trade Comm'n, Protecting Personal Information 22-23 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf; *see also* Fed. Trade Comm'n, Start with Security 1 (2015), *available at* ,https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

explain why the FTC has taken action against companies for failing to adequately train employees and service providers on data security.[454]

Some cases highlight the importance of employee training in secure information disposal.[455] Other cases make clear the importance of offering training in secure coding. In *In re TRENDnet*, the FTC alleged as unfair and deceptive the company's failure to implement reasonable guidance or training to employees responsible for testing, designing, and reviewing the security of its IP cameras and related software.[456] Similarly, in *In re HTC America*, the FTC alleged as unfair and deceptive the company's failure to implement adequate privacy and security guidance or training for its engineering staff.[457] This purportedly contributed to the company's failure to implement readily available secure communication mechanisms in its logging applications, which allowed malicious third-party apps to communicate with the logging application and placed consumers' text messages, location data, and other sensitive information at risk.[458]

---

454 *See, e.g.*, Complaint ¶¶ 8, 13-14, *In re Franklin's Budget Car Sales, Inc.*, No. C-4371 (F.T.C. Oct. 3, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026franklinautomallcmpt.pdf (failure to adequately train employees about information security alleged to be deceptive in light of company's claims); Complaint ¶¶ 6, 11 *In re EPN, Inc.*, No. C-4370 (F.T.C. June 7, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf (failure to adequately train employees about security alleged to be unfair); Complaint ¶¶ 14(c), 18-20, *In re Upromise, Inc.*, No. C-4351 (F.T.C. Mar. 27, 2012), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf (failure to ensure that employees responsible for information collection program received adequate training about security risks and policies alleged to be unfair and contrary to company's claims) (discussed *supra* Section II(C)(1)(b)); Complaint for Civil Penalties, Injunction, and Other Equitable Relief ¶¶ 11, 13, 15-16, *FTC v. Navone*, No. 2:08-cv-01842 (D. Nev. Dec. 30, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/01/090121navonecmpt.pdf (failure to alert employees or third parties to sensitivity of consumer information, or to instruct them to take precautions with information, alleged to be contrary to company's claims); *In re MTS, Inc.*, 137 F.T.C. 444, 448 (2004) (complaint) (failure to provide appropriate training and oversight for employees regarding application vulnerabilities and security testing alleged to be contrary to company's claims); *In re Eli Lilly & Co.*, 133 F.T.C. 763, 767-68 (2002) (failure to adequately train employees regarding consumer privacy and information security and failure to properly oversee and to assist an employee who sent out an email containing email addresses of 669 people who used Prozac.com alleged to be contrary to company's claims).

455 *See, e.g.*, *In re Rite Aid Corp.*, 150 F.T.C. 694, 696-97 (2010) (complaint) (failure to adequately train employees to dispose personal information securely alleged to be unfair and contrary to the company's claims); Complaint ¶¶ 7, 9-11, *In re CVS Caremark Corp.*, No. C-4259 (F.T.C. June 18, 2009), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2009/06/090623cvscmpt.pdf (failure to adequately train employees to dispose personal information securely alleged to be unfair and contrary to the company's claims); Complaint ¶¶ 5, 11-13, *In re Nations Title Agency, Inc.* (F.T.C. June 19, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf (failure to implement reasonable policies and procedures in employee training about handling of personal information alleged to be contrary to company's claims).

456 Complaint ¶ 8(d)(ii), *In re TrendNET*, No. C-4426 (Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

457 *In re HTC America Inc.*, 155 F.T.C. 1617, 1619 (2013) (complaint).

458 *Id.* at 1621-23.

The FTC has offered several points of guidance on employee training.[459] One is to create a "culture of security" by implementing a regular schedule of training for staff.[460] Such training could include updates about new security risks and vulnerabilities, explanations of why passwords should not be shared, and explanations of why sensitive personal data should not be transmitted via unsecured email.[461] If an employee fails to attend trainings, companies should consider blocking that person's access to the network.[462]

The FTC also recommends that companies designate persons(s) responsible for security, including those at appropriate levels of responsibility within an organization.[463] In the mobile app context, for example, the agency recommends that a developer team include at least one person responsible for considering security at every stage of an app's development.[464]

The agency also offers a series of free, plain-language videos discussing tips and lessons from the agency's law enforcement actions.[465] Companies can use these videos, as well as FTC reports, guides, and blogs, to help employees understand how to implement reasonable data security throughout the organization.

---

459 Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 30 (2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf; Fed. Trade Comm'n, Internet of Things: Privacy & Security in a Connected World 29 (2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; *see also* Fed. Trade Comm'n, Start with Security 9 (2015), *available at* ,https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf Fed. Trade Comm'n, Protecting Personal Information 18 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

460 Fed. Trade Comm'n, Protecting Personal Information 18 (2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

461 *Id.* at 12-13, 18.

462 *Id.* at 18.

463 *Id.*

464 Fed. Trade Comm'n, Mobile App Developers: Start with Security (2013), *available at* http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security.

465 The videos are available at the FTC's webpage for the Start with Security initiative. Fed. Trade Comm'n, *Start with Security*, https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Mar 22, 2016).

IV. CONCLUSION

The FTC's litigated cases, public settlements, and guidance materials are key to understanding the agency's Section 5 privacy and data security enforcement. This article provided an introductory framework to sketch the boundaries of Section 5 liability in this area. Sections II and III offered a bird's-eye view of a number of relevant FTC enforcement actions involving a wide variety of privacy and data security issues. There is of course no substitute for consulting the complaints, consent orders, guidance, and other materials—almost all of which are available online at www.ftc.gov.

BIOMETRIC PRIVACY LITIGATION: IS UNIQUE PERSONALLY IDENTIFYING INFORMATION OBTAINED FROM A PHOTOGRAPH BIOMETRIC INFORMATION?

By Natasha Kohne and Kamran Salour[1]

I. FACIAL RECOGNITION TECHNOLOGY: THE ABILITY TO PERSONALLY IDENTIFY SOMEONE FROM A PHOTOGRAPH

A. Social Media Sites Store Millions of Individualized Faceprints Generated From Photographs

Millions of people upload their photographs to social media sites such as Google and Facebook every day.[2] Google Photos touts more than 200 million monthly active users.[3] Shutterfly's ThisLife database stores roughly 18 billion images.[4] And Facebook claims that it has already uploaded 250 billion user photos, with 350 million more uploads daily.[5]

But in today's technological world, with only a mathematical algorithm, any person's face from a photograph can be analyzed and converted into an individualized "faceprint"—a unique identifying tag analogous to a fingerprint.[6] Creating a faceprint is surprisingly simple: typically, an algorithm measures the relative position, size, or shape of the eyes, nose, cheekbones, and jaw; these measurements are then compared with an existing database of images to determine a match.

Though simple, these algorithms are remarkably effective. Google's FaceNet algorithm reportedly identifies faces with 99.63 percent accuracy. Facebook's DeepFace operates at a reported 97.25 percent accuracy rate. Both algorithms significantly outperform the FBI's facial recognition program, which reports an 85 percent success rate.[7] To appreciate the effectiveness of these algorithms consider this: if you present

---

1 Natasha Kohne co-heads Akin Gump's cybersecurity, privacy and data protection practice and is licensed to practice in New York. Ms. Kohne is a partner in Akin Gump's San Francisco office (practicing under the supervision of Akin Gump's California partners) and in Abu Dhabi. Kamran Salour is counsel in Akin Gump's Los Angeles office and is a member of the firm's cybersecurity, privacy and data protection practice. The views expressed in this article are those of the authors and do not necessarily represent the views of Akin Gump Strauss Hauer & Feld LLP, its lawyers, or its clients.

2 Ben Sobol, *Facial recognition technology is everywhere. It may not be legal.,* WASH. POST, (June 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/.

3 Kia Kokalitcheva, *Google Photos Has Added Millions of New Users,* FORTUNE (May 18, 2016), http://fortune.com/2016/05/18/google-photos-200-million/.

4 Ricardo Bilton, *Shutterfly buys ThisLife in an attempt to create the perfect photo service, VENTURE BEAT (Jan. 7, 2013), http://venturebeat.com/2013/01/07/shutterfly-buys-thislife/.*

5 Jam Kotenko, *Facebook reveals we upload a whopping 350 million photos to the network daily,* DIGITAL TRENDS (Sept. 18, 2013), http://www.digitaltrends.com/social-media/according-to-facebook-there-are-350-million-photos-uploaded-on-the-social-network-daily-and-thats-just-crazy/.

6 Avi Asher-Schapiro, *Facial Recognition Technology Is Big Business—And It's Coming For You,* VICE NEWS (Aug. 13, 2015), https://news.vice.com/article/facial-recognition-technology-is-big-business-and-its-coming-for-you.

7 *Id.*

a person with two pictures, that person can tell at around a 97 percent accuracy rate whether the same person is in each photograph.[8]

As is evident from these comparative statistics, a company can generate readily a faceprint and identify a previously unknown individual from that faceprint with facial recognition technology with astonishing precision.

B. Faceprints Raise Potential Biometric Privacy Issues

Both Google and Facebook have amassed considerable faceprint databases. So far, Google Photos has applied automatically more than 2 trillion identifying tags to photographs in its database.[9] Facebook has not disclosed the size of its faceprint database, but it has called its repository "the biggest dataset in the world."[10]

But facial recognition technology sparks a series of privacy discussion points. First, it raises the topic of consent: "Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a [greater] distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere—on a lamp post, attached to an unmanned aerial vehicle or, now, integrated into the eyewear of a stranger."[11]

Second, facial recognition technology raises the topic of safeguarding. Biometric information is unlike other unique personal information such as social security or credit card numbers that if lost or stolen, can be replaced. Biometric information is biologically unique to an individual; if compromised, such information is irreplaceable. Therefore, it is important to know for what purpose biometric information will be collected, how it will be used, and how (and for how long) it will be stored before being destroyed.

Yet another question surrounding biometrics in the facial recognition context—and this article's primary focus—is does information derived from facial recognition technology constitute biometric information? Principally, must a facial recognition scan take place in-person, or does one capture biometric data by simply scanning a photograph?

As is often the case, technology outpaces the law, so the answer to this question remains unsettled. To compound matters, there is no federal statute that governs biometric privacy. And without a federal statute, states are left to create their own statutes to protect their citizens' biometric information. Only two states, Illinois and Texas, have statutes directed to biometric privacy. Texas' biometric statute, Capture or Use of Biometric Identifier (CUBI)[12], has not been the subject of judicial interpretation, while

---

8 Russell Brandom, *Why Facebook is beating the FBI at facial recognition,* The Verge (July 7, 2014), http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

9 Kokalitcheva, *supra* note 3.

10 Sobol, *supra* note 2.

11 Press Release, Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People (Feb. 5, 2014), https://www.franken.senate.gov/?p=press_release&id=2699.

12 Tex. Bus. & Com. Code Ann. § 503.001 (2009).

judicial interpretation of Illinois' biometric statute, Biometric Information Privacy Act (BIPA)[13] has yielded results that are seemingly at odds with BIPA's plain text.

***

Part One of this Article discusses BIPA's origins, the obligations BIPA imposes on individuals and companies, and key BIPA-defined terms. **Part Two** analyzes how federal courts have interpreted BIPA's scope; specifically, whether under BIPA information derived from photographs constitutes biometric information. **Part Three** identifies common jurisdictional and constitutional defenses to BIPA claims and discusses their relative success. **Part Four** explores proposed amendments to BIPA and whether existing and proposed biometric statutes in other states consider unique identifying information derived from photographs to be biometric information. **Part Five** concludes with a discussion on how the existing uncertain biometric legal landscape has taken the focus off of protecting biometric information and instead given savvy plaintiffs' lawyers license to assert multi-million dollar class action suits against companies alleging BIPA violations but devoid of allegations that an individual's biometric information has been compromised.

II. PART ONE: THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

A. BIPA Was Enacted to Safeguard the Biometric and Corresponding Financial Data of Illinois Residents

In 2008, the Illinois legislature faced a dilemma: Pay By Touch, a California-based company that allowed people to pay for goods and services with only a swipe of a finger,[14] was in bankruptcy, and the California bankruptcy court had just approved the sale of Pay By Touch's database.[15] This was no ordinary database, however. This database housed the fingerprint and financial data of all of Pay By Touch's former customers. Importantly for the Illinois legislature, this database included the fingerprint and corresponding financial data of thousands of Illinois citizens; Illinois had served as a pilot testing site for new applications of biometric-facilitated financial transactions, including Pay By Touch's finger-scan technology. Pay By Touch's bankruptcy posed a serious risk to Illinois citizens whom were left wondering what would happen to their fingerprint and financial data stored in Pay By Touch's database.

Illinois recognized that its citizens needed their biometric information protected.[16] "Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once

---

13 740 Ill. Comp. Stat. § 14/1, et seq. (2008).

14 Shubha, *Failure Story: What Happened to Pay By Touch?,* Let's Talk Payments (Apr. 20, 2015), https://letstalkpayments.com/failure-story-what-happened-to-pay-by-touch/.

15 *Pay By Touch Fades into History As Lenders Buy Core Assets,* Digital Transactions (Apr. 7, 2008), http://www.digitaltransactions.net/news/story/Pay-By-Touch-Fades-into-History-As-Lenders-Buy-Core-Assets.

16 *See* IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249 (May 30, 2008) (Statement of Rep. Kathleen A. Ryg).

compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."[17]

The Illinois Legislature responded by enacting BIPA,[18] the first state statute focused on the regulation of biometric information in consumer financial transactions. Put broadly, BIPA aims to set "collection and retention standards while prohibiting the sale of biometric information."[19]

From its 2008 enactment until 2015, BIPA remained largely unnoticed, if not altogether unknown. Then, in 2015, three Illinois residents sued Facebook alleging that Facebook's "Tag Suggestions" feature collects, stores, and uses biometric information (*i.e.*, faceprints) in violation of BIPA.[20] Though seemingly divorced from the discrete intent of BIPA to secure biometric information used in financial transactions,[21] this suit sparked several more putative class actions against various social media companies' alleged use of photographic-based facial recognition technology.

B. An Individual's or Company's Obligations under BIPA

BIPA proclaims that "[t]he public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[22]

To achieve this purpose, BIPA makes it unlawful for a ***private entity*** to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's ***biometric identifiers*** or ***biometric information***, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative."[23]

If a private entity fails to comply with these requirements, it is subject to civil suit and, at minimum, statutory penalties, ***per each violation***. In particular, BIPA authorizes any person aggrieved by a BIPA violation to file suit against an offending party, and the prevailing party may recover, among other things, $1,000 for each negligent violation, $5,000 for each intentional violation, and reasonable attorneys' fees.[24]

---

17 740 Ill. Comp. Stat. § 14/1, et seq. (2008).

18 *Id.*

19 *See IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249.*

20 *In re Facebook Biometric Information Privacy Litigation,* No. 15-cv-03747-JD, ___ F. Supp. 3d ___, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016).

21 Stephanie N. Grimoldby, *Ill. facial recognition law leads to wave of class actions against Facebook, others,* Legal NewsLine (July 6, 2016), http://legalnewsline.com/stories/510954980-ill-facial-recognition-law-leads-to-wave-of-class-actions-against-facebook-others.

22 740 Ill. Comp. Stat. § 14/5(g) (2008).

23 *Id.* § 14/15(b).

24 *Id.* § 14/20.

In short, under BIPA, a private entity must: (1) inform the subject in writing that it collects or stores the subject's biometric identifiers or biometric information; (2) inform the subject in writing of the specific purpose and duration that the biometric identifiers or biometric information will be used, collected, or stored; and (3) obtain the subject's written consent.[25] A failure to comply could subject a private entity to civil suit seeking thousands in civil penalties for each alleged violation. For companies like Snapchat and Shutterfly, the number of alleged violations easily rises to the millions.

C. BIPA's Defined Terms Appear to Exclude from BIPA's Scope Photographs and Information Derived from Photographs

To understand BIPA's scope, one must understand three central defined terms: (1) private entity; (2) biometric identifiers; and (3) biometric information. BIPA defines each of these terms as follows:

- **Private entity** "means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.[26]

- **Biometric identifier** "means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. ***Biometric identifiers do not include writing samples, written signatures, photographs,*** human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."[27]

- **Biometric information** "means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information ***does not include information derived from items or procedures excluded under the definition of biometric identifiers*** [*i.e.*, writing sample, written signature, photographs] excluded under the definition of biometric identifiers."[28]

---

25 Among its other requirements, BIPA demands a publicly available retention and destruction schedule that establishes a retention schedule and guideline for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. *See id.* § 14/10.

26 *Id.*

27 *Id.* (emphasis added).

28 *Id.* (emphasis added).

Defined Term Under BIPA	Includes	Excludes
Private Entity	Individuals and Companies	Illinois Government Agency
Biometric Identifier	Retina/iris scan; voiceprint; fingerprint; scan of hand or face geometry	Photographs
Biometric Information	Any information based on an individual's biometric identifier used to identify an individual	Information derived from photographs

BIPA's plain text, it would seem, excludes from BIPA's purview ***photographs*** *and any information an individual or company about an individual* ***derived from a photograph.*** *Not everything is as it seems, however.*

III. PART TWO: WHETHER A PLAINTIFF CAN STATE A CAUSE OF ACTION UNDER BIPA WHEN THE ALLEGED BIOMETRIC INFORMATION AT ISSUE WAS DERIVED SOLELY FROM A PHOTOGRAPH

Suits alleging a company's facial recognition technology violates BIPA follow a similar and predictive pattern, the defendant company: (1) allegedly conducted a scan of a photograph of the plaintiff's face; (2) extracted from that photograph the plaintiff's unique geometric data; (3) used that extracted data to create a faceprint of the plaintiff; and (4) compared that faceprint with an existing faceprint database to identify the plaintiff—all without the plaintiff's knowledge or consent.

Two district courts have held that a plaintiff can state a cause of action under BIPA even though the purported biometric information was derived solely from a photograph.[29]

29 *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015); *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD, ___ F. Supp. 3d ___, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016).

A. The *Shutterfly* Suit

On December 29, 2015, the Northern District of Illinois issued what is believed to be the first judicial interpretation of BIPA.[30] In that case, the plaintiff Brian Norberg sued Shutterfly, a photo-service company that allows its users to store and organize their photos. In his suit, Norberg, a non-Shutterfly user, claimed that an unnamed Shutterfly user uploaded Norberg's photo while creating a wedding invitation. Norberg alleged that when a Shutterfly user uploads a photo, Shutterfly then scans that photograph for faces, extracts geometric data relating to the unique points and contours of each extracted face, and then uses that data to create and store a template of each face.[31] Shutterfly, therefore, according to Norberg, collected and stored his face template without his informed written consent, in violation of BIPA.[32]

Shutterfly sought to dismiss the complaint for lack of personal jurisdiction[33] and for failure to state a claim.[34] Relying on BIPA's plain text, Shutterfly argued that Norberg cannot state a cause of action because "BIPA clearly and unequivocally states that photographs—and any information derived from photographs—are not within the scope of the law."[35]

At first glance, the court appeared to agree with Shutterfly's interpretation of BIPA. The court noted that BIPA defines a biometric identifier as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry," but excludes "writing samples, signatures, ***photographs***, biological samples, demographic data, tattoos, or physical descriptions."[36] The court noted further that BIPA's definition of biometric information does not include information derived from items excluded from the above definition (*i.e.*, photographs).[37] Nonetheless, the court denied Shutterfly's motion to dismiss and held that Norberg did state a cause of action for BIPA:

> Here, [Norberg] alleges that [Shutterfly is] using his personal face pattern to recognize and identify [him] in photographs posted to [Shutterfly's photo sharing websites]. [Norberg] avers that he is not now nor has he ever been a user of [Shutterfly's photo sharing websites], and that he was not presented with a written biometrics policy nor has he consented to have his biometric identifiers used by [Shutterfly]. As a result, the Court finds that Plaintiff has plausibly stated a claim for relief under the BIPA.[38]

---

30 *Norberg,* 152 F. Supp. 3d at 1103.

31 First Amended Class Action Complaint ¶¶ 26-28, *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-05351 (N.D. Ill. June 23, 2015), ECF No. 6.

32 *Id.* ¶¶ 48-51.

33 *See* Part Three, *infra.*

34 *Norberg,* 152 F. Supp. 3d at 1104.

35 Memorandum in Support of Defendants' Motion to Dismiss, Norberg v. Shutterfly, Inc., No. 1:15-cv-05351 (N.D. Ill. April 12, 2016), ECF No. 26.

36 *Norberg*, 152 F. Supp. 3d at 1106.

37 *Id.*

38 *Id.*

Whether Norberg would have prevailed at trial will remain unknown. Ultimately, the parties entered into a settlement agreement and Norberg dismissed the complaint with prejudice.[39]

B. The *Original Facebook* Suit

On May 5, 2016, the Northern District of California similarly held that the plaintiffs could state a cause of action under BIPA even though the purported biometric information was derived from photographs.[40] In 2015, Adam Pezen, Carlo Licata, and Nimesh Patel each brought separate putative class actions in the Northern District of Illinois against Facebook.[41] Those three suits were subsequently consolidated and transferred to the Northern District of California.[42] The class action plaintiffs alleged that Facebook's Tag Suggestions feature—which allegedly scans photographs uploaded by a Facebook user and then identifies faces appearing in those photographs—violates BIPA because it extracts a Facebook user's facial geometry without that user's knowledge or consent.[43]

Facebook argued that BIPA does not apply to its "Tag Suggestions" feature because BIPA excludes photographs and information derived from photographs, and Facebook's feature derived the purported biometric information at issue exclusively from uploaded photographs.[44]

The court denied Facebook's motion and held that the plaintiffs stated a cause of action under BIPA.[45] BIPA regulates the collection, retention, and disclosure of personal biometric identifiers such as the scan of hand or face geometry. "Plaintiffs allege that Facebook scans user-uploaded photographs to create a 'unique digital representation of the face . . . based on geometric relationship of their facial features.' That allegation falls within the scan of face geometry stated in the statute."[46]

The court addressed Facebook's BIPA interpretation as well. The court opined that Illinois legislature enacted BIPA to address emerging biometric technology, such as Facebook's face recognition software, without including physical identifiers that are more qualitative and non-digital in nature.[47] The court went on to interpret photographs to mean physical photographs only: "'Photographs' is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet. Consequently, the court will not read the statute to categorically exclude

---

39 Stipulation of Dismissal With Prejudice, *Norberg v. Shutterfly*, Inc., No. 1:15-cv-05351 (N.D. Ill. April 12, 2016), ECF No. 91.

40 *In re Facebook Biometric Information Privacy Litigation,* No. 15-cv-03747-JD, ___ F. Supp. 3d ___, 2016 WL 2593853 (N.D. Cal. May 5, 2016).

41 *Id.* at *1-2.

42 *Id.*

43 *Id.*

44 *Id.* at *11.

45 *Id.*

46 *Id.* at *12.

47 *Id.*

from its scope all data collection processes that use images. And to read that categorical exclusion into the statute would substantially undercut it because the scanning of biometric identifiers is often based on an image or photograph."[48]

To date, two separate district courts that have interpreted BIPA, and each such court has held that a plaintiff can state a cause of action under BIPA even if the alleged biometric information is derived solely from photographs. Neither decision is precedential, however.[49]

C. The *Google* Suit

Despite two federal courts refusing to dismiss a BIPA claim on the basis that the purported biometric information was derived from photographs—and therefore is neither a biometric identifier nor biometric information under BIPA—Google has advanced this same argument in defense of a photo-based facial recognition BIPA class action suit.

Plaintiff Lindabeth Rivera sued Google in the Northern District of Illinois.[50] She alleges that Google Photos violates BIPA. "Specifically, Google has created, collected and stored, in conjunction with its cloud-based 'Google Photos' service, millions of 'face templates' (or 'face prints')—highly detailed geometric maps of the face—from millions of Illinois residents, many thousands of whom are not even enrolled in the Google Photos service. Google creates these templates using sophisticated facial recognition technology that extracts and analyzes data from the points and contours of faces that appear in photos taken on Google 'Droid' devices and uploaded to the cloud-based Google Photos service. Each face template that Google extracts is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person."[51] Rivera does not have a Google Photos account.[52]

Another individual, Joseph Weiss also sued Google under a virtually identical theory.[53] Unlike Rivera, however, Weiss does have a Google Photos account.[54]

On June 17, 2016, Google filed a single motion to dismiss both the Rivera and Weiss complaints. Google maintains that the putative class action should be dismissed for

---

48 *Id.*

49 *See Klein v. Depuy, Inc.,* 476 F. Supp. 2d 1007, 1023 (N.D. Ind. 2007) ("Although federal courts are bound to state court precedents in interpreting state law, there is no authority that requires a district court that is attempting to predict how the highest state court would rule to follow the decision of federal courts sitting in that state."), *aff'd* 506 F.3d 553 (7th Cir. 2007).

50 *See* First Amended Complaint by Lindabeth Rivera, *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), ECF No. 40.

51 *See id.* ¶ 5.

52 *See id.* ¶ 7.

53 *See* First Amended Complaint by Joseph Weiss ¶ 5, *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), ECF No. 41.

54 *See id.* ¶ 27.

failure to state a claim because BIPA expressly precludes from its scope photographs and information derived from photographs.[55]

Google's motion also attacks the prior decisions in *Norberg* and *Facebook*. Google maintains that "[t]he decision in *Norberg* contains hardly any reasoning at all, and does not even attempt to explain how BIPA can be read to cover information derived from photographs." Google argues that "[t]he court in *Facebook,* for its part, adopted an interpretation of 'photographs' that neither party before it had advanced, construing the term to refer only to 'paper prints of photographs, not digitized images.'" Google argues further that this " . . . interpretation of BIPA would lead to absurd results—among them that just *taking* a digital photograph would constitute a 'scan of . . . face geometry,' because such a photograph would no longer fall within the exclusion for 'photographs.'"[56]

Google's motion to dismiss is pending. It remains to be seen whether the *Google* court will follow the prior decisions of the *Norberg* and *Facebook* courts, and whether it will address Google's criticisms of those rulings. The *Google* court's decision could open the floodgates to additional putative class actions alleging BIPA violations based on photographic facial recognition.

IV. PART THREE: COMMON JURISDICTIONAL AND CONSTITUTIONAL DEFENSES TO BIPA CLAIMS

A. Courts Have Reached Different Holdings Whether an Interactive Website Is Sufficient to Establish Personal Jurisdiction

Given the uncertainty as to what constitutes biometric information under BIPA, companies facing suit under BIPA have advanced defenses other than personally identifying information derived from a photograph does not constitute biometric information. These defenses have achieved varied success.

One such defense is a lack of personal jurisdiction. At a basic level, a court can only exercise personal jurisdiction (*i.e.,* jurisdiction over the parties to the suit) if there have been sufficient minimum contacts between the defendant and the forum state.[57] If personal jurisdiction does not exist, a court does not have authority to preside over the suit, and the case is dismissed.

In August 2015, an Illinois resident, William Gullen, sued Facebook "resulting from the illegal actions of Facebook in collecting, storing and using Plaintiff's and other similarly situated individuals' biometric identifiers and biometric information . . . without informed written consent in violation of BIPA."[58] Like the suit against Facebook that preceded it, Gullen claims that Facebook's "Tag Suggestions," relies on proprietary facial recognition technology to scan every user-uploaded photo for faces,

---

55 *See* Memorandum by Google, Inc. in Support of Motion to Dismiss for Failure to State a Claim, *Rivera v. Google, Inc.*, No. 1:16-cv-02714 (N.D. Ill. May 27, 2016), ECF No. 49.

56 *Id.*

57 *International Shoe Co. v. State of Wash., Office of Unemployment Comp. and Placement,* 326 U.S. 310, 316 (1945).

58 Complaint ¶ 1, *Gullen v. Facebook.com, Inc.*, No. 1:15-cv-07681 (N.D. Ill. Aug. 31, 2015), ECF No. 1.

extract geometric data relating to the unique points and contours of each face, and then uses that data to create and store, without consent, a template of each face.[59] Gullen does not and has never had a Facebook account.[60]

Facebook filed a motion to dismiss in November 2015. Facebook's motion to dismiss advanced two reasons for dismissal: (1) The Court lacked personal jurisdiction over Facebook; and (2) Gullen could not state a claim under BIPA since his claim rests entirely upon the collection, storage, and use of biometric information that was derived from *photographs* uploaded to Facebook.[61] Facebook argued that to establish personal jurisdiction, Gullen must establish a sufficient "relationship among the defendant, the forum, and the litigation," but Gullen cannot establish the requisite sufficient relationship as he alleges he does not have a Facebook account and has never interacted with Facebook.[62]

On January 21, 2016, the court dismissed Gullen's claim with prejudice.[63] Gullen based his personal jurisdiction claim on the allegation that Facebook "target[s] its facial recognition technology to millions of users who are residents of Illinois."[64] But the court stated that Facebook does not target exclusively its facial recognition technology on Illinois residents; Gullen's complaint alleges that Facebook uses this technology on every user-uploaded photograph.[65] Therefore, Gullen's personal jurisdiction claim is based on the notion that Facebook operates an interactive website, which is insufficient by itself to establish personal jurisdiction.[66]

Conversely, under nearly identical facts, the *Shutterfly* court held that personal jurisdiction did exist. To establish jurisdiction, Norberg, a non-Shutterfly user, alleged that "[t]here are likely tens of thousands of individuals who, while residing in Illinois, had their photos uploaded to Shutterfly."[67]

The *Shutterfly* court found that allegation sufficient to establish personal jurisdiction. The court reasoned that: (1) Shutterfly operates a number of websites that provide digital photo storage and sharing services that are available in all fifty states; (2) Shutterfly is accused of violating is an Illinois statute and stems out of its contact with Illinois

---

59 *Id.* ¶ 22.

60 *Id.* ¶ 8.

61 Defendant Facebook, Inc.'s Memorandum of Law in Support of its Motion to Dismiss, *Gullen v. Facebook.com, Inc.,* No. 1:15-cv-07681 (N.D. Ill. Aug. 31, 2015), ECF No. 20.

62 *Id.*

63 Order on Motion to Dismiss, *Gullen v. Facebook.com, Inc.,* No. 1:15-cv-07681 (N.D. Ill. Jan. 1, 2016), ECF No. 37.

64 Complaint ¶ 10, *Gullen v. Facebook.com, Inc.,* No. 1:15-cv-07681 (N.D. Ill. Aug. 31, 2015), ECF No. 1.

65 *Id.* ¶ 22.

66 *Illinois v. Hemi Grp. LLC*, 622 F.3d 754, 760 (7th Cir. 2010) (stating operation of interactive website insufficient to create specific jurisdiction). The Court never determined whether Gullen could state a claim for relief under BIPA, leaving companies guessing.

67 First Amended Class Action Complaint ¶10, *Norberg v. Shutterfly, Inc.*, No. 1:15-cv-05351 (N.D. Ill. June 23, 2015), ECF No. 6.

residents; and (3) because Norberg is a private Illinois resident, there is a strong interest in adjudicating the matter locally.

The Shutterfly decision stands in sharp contrast to the Facebook decision and Seventh Circuit precedent, which has rejected the notion that an online merchant's operation of an interactive site is sufficient to confer specific jurisdiction on it in every state from which the site can be accessed.

B. The Supreme Court's Recent Ruling in Spokeo May Slow the Growth of BIPA Class Action Suits

1. The *Smarte Carte* Suit

Another defense is lack of subject matter jurisdiction. At a high-level, subject matter jurisdiction refers to the court's authority to hear a particular case. In federal court, a plaintiff must establish Article III standing. Without it, the federal court does not have subject matter over the case.

The Supreme Court recently clarified a plaintiff's requirement to establish Article III standing. In *Spokeo, Inc. v. Robins*, the Supreme Court held that to establish Article III standing, a plaintiff must allege "concrete" harm—which the Supreme Court described as harm that is "real" and "not abstract."[68] The Ninth Circuit held previously that a "statutory violation automatically establishes standing," but the Supreme Court held that the allegation of a statutory violation does not by itself suffice to meet the "real" harm standard. *Spokeo* thus holds that a plaintiff has standing to bring a statutory claim only when the asserted violation encompasses an allegation of concrete harm—either because (1) an element of the cause of action requires proof of such a harm, and the plaintiff alleges facts sufficient to establish that element; or (2) the plaintiff separately alleges facts establishing a concrete harm.[69]

The Northern District of Illinois relied recently on *Spokeo* to dismiss a putative BIPA class action.[70] That suit concerns Smarte Carte's alleged collection, storage, and use of biometric data without consumer consent in violation of BIPA.[71] The complaint alleges that in 2008, Smarte Carte introduced electronic lockers for rent. Unlike traditional rental lockers that require a key, Smarte Carte's electronic lockers scan, collect, and record the renter's fingerprint at the time of rental; the renter unlocks the locker using that recorded fingerprint.[72] The plaintiff McCollough allegedly used and paid for an electronic locker five times in 2015.[73] She contends that, in violation of BIPA, Smarte Carte did not inform renters in writing that their biometric identifiers or biometric information was being collected or stored, for how long such information would be

---

68 *Spokeo, Inc. v. Robins,* 136 S. Ct. 1540, 1548 (2016).

69 *Id.* at 1549-50.

70 *McCollough v. Smarte Carte, Inc.,* No. 16-cv-03777, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

71 *Id.* at *1.

72 *Id.*

73 *Id.*

stored, or make available a written policy disclosing when such information will be destroyed permanently.[74]

Smarte Carte filed a motion to dismiss and argued that the court lacked subject matter jurisdiction.[75] Principally, Smarte Carte argued that "[n]owhere in the Complaint does Plaintiff contend that she suffered any harm, loss or injury."[76] Plaintiff's alleged BIPA violations, without more, are insufficient to confer standing under Article III of the U.S. Constitution.[77]

The Court agreed. "This Court finds that plaintiff has alleged the sort of bare procedural violation that cannot satisfy Article III standing."[78] McCollough did not allege any harm that resulted from the alleged violation.[79] "Even without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, this Court finds it difficult to imagine, without more, how this retention could work a concrete harm."[80] The court went on to ask: "How can there be an injury from the lack of advance consent to retain the fingerprint data beyond the rental period if there is no allegation that the information was disclosed or at risk of disclosure?"[81]

2. The *Original Facebook* Suit and The *Take-Two* Suit

Facebook, after failing to dismiss the Plaintiffs' putative class action suit on 12(b)(6) grounds,[82] filed in June 2016 a motion to dismiss for lack of standing based on *Spokeo*. According to Facebook, Plaintiffs allege that Facebook violated BIPA because it failed to develop a written policy governing the retention and destruction of documents and failed to notify and obtain informed written consent from the individuals whose biometric information Facebook purportedly collected. But, Plaintiffs did not allege that they have been harmed by these supposed technical violations of BIPA.[83] Facebook's motion to dismiss for lack of subject matter jurisdiction is still pending.

Take-Two is advancing a similar argument in its defense of a BIPA class action filed against it. Take-Two develops and publishes basketball-themed video games NBA 2K15

---

74 *Id*. at *2.

75 *Id*. at *2-3.

76 Defendant Smarte Carte, Inc.'s Memorandum of Law in Support of Motion to Dismiss at 2, *McCollough v. Smarte Carte, Inc.*, No. 16-cv-03777 (N.D. Ill. May 6, 2016), ECF No. 13.

77 "Any person ***aggrieved*** by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal court against an offending party." 740 Ill. Comp. Stat. § 14/20 (2008) (emphasis added).

78 *McCollough,* 2016 WL 4077108, at *3.

79 *Id*.

80 *Id*. at *4.

81 *Id*. The Court also found that the Plaintiff failed to state a claim under BIPA. BIPA provides that "[a] ny person aggrieved" has a right of action. The Court interpreted "aggrieved" to require a showing of injury; since McCollough has not alleged any facts showing that her rights have been adversely affected by the purported BIPA violations, she has not stated a claim.

82 *See* Part Two, *supra*.

83 Motion to Dismiss for Lack of Subject Matter Jurisdiction, *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD (N.D. Cal. June 29, 2016), ECF No. 129.

and NBA 2K16. Each game contains a "MyPlayer" feature which allows users to create a personalized basketball avatars by taking a photograph.[84]

In *Take-Two,* Plaintiffs Ricardo Vigil and his sister Vanessa Vigil sued Take-Two for BIPA violations. They allege that this process violates BIPA: "Take-Two has created, collected and stored 'scans of face geometry' (or 'face templates')–highly detailed geometric maps of the face–from thousands of Illinois residents. Both the NBA 2K15 and NBA 2K16 video games are equipped with software that, in combination with a camera attached to a personal computer or a game console, operates to extract and analyze data from the points and contours of the face of an individual playing the game, and thereafter creates a virtual player with a personally identifying facial rendition. Each face template, on which each rendition is based, is unique to a particular individual, in the same way that a fingerprint or voiceprint uniquely identifies one and only one person."[85]

Take-Two's motion is predicated not on whether Take-Two violated BIPA, but whether the plaintiffs can establish that they have been harmed by any purported violations. To support a damages claim, Ricardo Vigil claims he would not have purchased the NBA 2K15 video game if he knew that one of the games features violates BIPA. Both Ricardo and his sister allege that Take-Two misappropriates valuable biometric data and that they face an increased risk that their biometric data may be compromised in the future. Take-Two denounces that any of these allegations can support standing under Article III, or even state a claim for relief under BIPA itself, as neither plaintiff can demonstrate he or she is an aggrieved party as BIPA requires.[86] Take-Two's motion to dismiss for lack of subject matter jurisdiction is also pending.

If district courts follow *Smarte Carte,* then BIPA class action suits may be limited as plaintiffs will be required to allege concrete harm resulting from the alleged BIPA violation, and not merely a BIPA violation itself.

3. The Arbitration Agreement Defense?

Snapchat became the latest social media company purportedly using facial recognition technology to face suit under BIPA. Plaintiffs Jose Luis Martinez and Malcolm Neal, both Snapchat users, filed suit in California state court May 2015.[87] They alleged that: (i) Snapchat's "Lenses" feature relies on facial recognition technology to allow users to add real-time special effects and sounds to photographs; (ii) scans a user's face each time he or she uses Lenses; and (iii) collects, stores, and uses geometric data

---

84 Memorandum of Law of Defendant Take-Two Interactive Software, Inc. in Support of Motion to Dismiss the Second Amended Complaint, *Santana v. Take-Two Interactive Software, Inc.*, No. 1:15-cv-08211-JGK (S.D.N.Y. July 29, 2016), ECF No. 49.

85 Second Amended Complaint ¶ 5, *Santana v. Take-Two Interactive Software, Inc.*, No. 1:15-cv-08211-JGK (S.D.N.Y. July 15, 2016), ECF No. 43.

86 Memorandum of Law of Defendant Take-Two Interactive Software, Inc. in Support of Motion to Dismiss the Second Amended Complaint, *Santana v. Take-Two Interactive Software, Inc.*, No. 1:15-cv-08211-JGK (S.D.N.Y. July 29, 2016), ECF No. 49.

87 Complaint, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. May 23, 2016), ECF No. 1-1.

relating to the unique points and contours (*i.e.,* biometric identifiers) of each face without consent, in violation of BIPA.[88]

In July, Snapchat removed the case to the Central District of California,[89] presumably to be able to assert an Article III challenge following *Spokeo.* In August, Snapchat filed a motion to compel arbitration, arguing that all Snapchat users, including plaintiffs, expressly agreed under Snapchat's Terms of Use to individually arbitrate all claims and disputes arising in connection with their use of any Snapchat service.[90]

Snapchat's arbitration notice includes a waiver to participate in class-action lawsuits or classwide arbitrations.[91] Snapchat's motion to compel arbitration also noted that Lenses does not use facial recognition technology to place these special effects. "Instead it uses object recognition technology, which allows Lenses to identify a nose as a nose or an eye as an eye, but does not—and cannot—identify a nose or an eye, let alone a whole face, as belonging to any specific person."[92] On August 30, 2016, plaintiffs voluntarily dismissed their complaint without prejudice.[93]

Just eight days after Snapchat filed its motion to compel arbitration, asserting that the plaintiffs expressly waived their right to class-action litigation and classwide arbitration, the plaintiffs dismissed their suit voluntarily. Because the *Snapchat* suit was dismissed voluntarily, it is unknown how the Court would have ruled on Snapchat's motion to compel arbitration. Clearly, however, if a plaintiff cannot file a class action, then the appeal of BIPA to plaintiffs' lawyers, and the per violation statutory penalties BIPA provides, dwindles.

V. PART FOUR: THE RISE OF CLASS ACTION SUITS AGAINST SOCIAL MEDIA COMPANIES BASED ON THEIR ALLEGED SCANS OF PHOTOGRAPHS AND ITS POTENTIAL IMPACT ON BIOMETRIC LEGISLATION

A. The Proposed Amendments to BIPA

On May 26, 2016, in response to the floodgates of photograph-based facial recognition BIPA class action suits, Illinois Senator Terry Link filed a proposed amendment to BIPA.[94]

---

88 *Id.* ¶ 33.

89 Notice of Removal, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. July 14, 2016), ECF No. 1.

90 Motion to Compel Arbitration, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. Aug. 22, 2016), ECF No. 21.

91 *Id.*

92 *Id.*

93 Notice of Voluntary Dismissal, *Martinez v. Snapchat, Inc.*, No. 2:16-cv-05182-SVW (C.D. Cal. Aug. 30, 2016), ECF No. 29.

94 Linn Foster Freedman, *Proposed amendment to Illinois biometrics privacy law introduced then stalled,* DATA PRIVACY + SECURITY INSIDER (June 2, 2016), https://www.dataprivacyandsecurityinsider.com/2016/06/proposed-amendment-to-illinois-biometrics-privacy-law-introduced-then-stalled/.

In pertinent part, Senator Link's proposed amendments sought two main changes. First, it expressly excluded both physical and digital photographs from BIPA's definition of "biometric identifier." Second, it added a new defined term, "scan," and limited the definition of "scan" to in-person scans.

TERM	BIPA	PROPOSED AMENDMENT
"Biometric Identifier"	**"Biometric identifier"** means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."	**"Biometric identifier"** means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, <u>physical or digital</u> photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color."
"Biometric Information"	**"Biometric information"** means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers."	**"Biometric information"** means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. "Biometric information" and "biometric identifier" do ~~Biometric information does~~ not include information derived from items or procedures excluded under the definition of biometric identifiers."
"Scan"	**N/A**	**"Scan"** means data resulting from an in-person process whereby a part of the body is traversed by a detector or an electronic beam.

By excluding from the definition of "biometric identifier" physical and digital photographs and clarifying that the term "scan" must occur in-person, the proposed BIPA amendment would have effectively abrogated BIPA claims related to the collection of user faceprints by online services. Not surprisingly, the proposed BIPA amendment sparked debate.

Critics of the proposed BIPA amendment were angered by the timing, substance, and intent behind the proposed amendment. Senator Link made his proposal just before the Memorial Day weekend and attached the bill to the end of an unrelated bill regarding unclaimed property. Critics also believed the proposed amendment would nullify biometric protections. It is common in biometrics for scanning to be of an image or photograph. The proposed amendment "retroactively removes the consumer protections of [BIPA] and renders the Act effectively null," by changing the technical definition of biometric scans as to render BIPA inapplicable to actual biometrics.[95] "To purposefully and specifically exclude photographs and digital photographs, as the proposed amendment does, means BIPA will essentially not apply to biometrics due to how biometric analytical processes work."[96] Critics believed further that the proposed BIPA amendment was not intended to secure biometric data, but was instead submitted in response to lobbying efforts from social media companies such as Facebook and Google:

> We suspect that the proposed Amendments were introduced in an effort to immunise Facebook, Google, and others, from liability in the lawsuits they are facing. That's because two federal courts have looked at whether BIPA regulates facial recognition technology as applied to uploaded photographs (in cases against Shutterfly and Facebook) and both federal courts have held that the statute unambiguously regulates the activity. It appears that the proposed Amendments are an effort to achieve through new legislation what these social media companies have been unable to achieve through the courts. Absent a retroactively applied amendment to BIPA, the pending lawsuits against Facebook and Google should proceed to trial. An 'in person scan' using a 'detector' or 'electronic beam' is not how companies are actually obtaining consumers' biometric data in the real world. If the intermediation of a photograph excused all subsequent processing into a biometric identifier, as the Amendments would have done, then practically all biometric data gathered and stored against consumers' wishes would be free from regulation and thus wholly permitted. Simply stated, the Amendments would have entirely swallowed the rule against unauthorised collection of biometric identifiers, rendering the statute and its promises of protection entirely hollow.[97]

Proponents of the amendment argue that Senator Link's proposal did nothing more than clarify BIPA's intent. Senator Link's proposed amendment merely adds the words "physical or digital" to the word "photograph" to make it clear that photographs are

---

95 Letter from Abraham Scarr, Dir. of Ill. Public Interest Research Grp., to Sen. Bliss (May 27, 2016), https://www.eff.org/files/2016/06/07/2016-05-27_letter_-_il-pirg_against_il_hb_6074_0.pdf.

96 Letter from Pam Dixon, Exec. Dir. of World Privacy Forum, et al., to Sen. Bliss (May 27, 2016), https://www.eff.org/files/2016/06/07/2016-05-27_letter_-_wpf_against_il_hb_6074_0.pdf.

97 Frank S. Hedin and David P. Milian, *BIPA Amendment Put on Hold After Backlash from Privacy Advocates,* Carey Rodriguez Attorneys (June 2, 2016), http://www.careyrodriguez.com/blog/bipa-amendment-put-on-hold-after-backlash-from-privacy-advocates/.

not included in the law. The amendment further includes a definition of "scan," which clarifies that a scan included in the law is "an in-person process whereby a part of the body is traversed by a detector or an electronic beam."[98] These changes would in effect confirm that the scanning of a digital photograph of a person's face is not covered by the law, and proponents argued that these changes are merely clarifications to the definitions in the existing law and are consistent with the intent of the law.[99]

The next day, Senator Link announced that the amendment was put on hold, but did not specify why.[100]

B. Other State Biometric Statutes Define Biometric Information Differently than BIPA

1. Texas' Biometric Statute Does Not Expressly Exclude Photographs from Its Definition of Biometric Information

The surging popularity of photograph-based facial recognition BIPA suits against Facebook, Google, and Snapchat begs the question: What about the biometric statutes of other states?

Texas enacted its biometric statute, the Capture or Use of Biometric Identifier ("CUBI"), in 2009.[101] BIPA and CUBI have many similarities. Like BIPA, CUBI prohibits the collection of biometric information without informed consent. Under CUBI, "[a] person may not capture a biometric identifier of an individual for a commercial purpose unless the person: (1) informs the individual before capturing the biometric identifier; and (2) receives the individual's consent to capture the biometric identifier."[102] And like BIPA, CUBI defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[103]

BIPA and CUBI, however, are not without differences. CUBI does ***not*** expressly exclude photographs from its definition of biometric identifier. And under CUBI, biometric identifiers include "record[s]" (as opposed to just "scans") of hand and face geometry. Arguably, CUBI has a broader reach than BIPA.

Certainly companies such as Google and Facebook have millions of users in Texas. Unquestionably, thousands of those users upload photographs upon which Google and Facebook scan and identify other users found in them. Unlike BIPA, however, CUBI is not subject to class action suits. That is because CUBI is enforceable only by the state attorney general. That CUBI does not allow for private rights of action seems to be the main reason why such suits are not prominent.

---

98 Linn Foster Freedman, *Proposed amendment to Illinois biometrics privacy law introduced then stalled,* Data Privacy & Security Insider (June 2, 2016), https://www.dataprivacyandsecurityinsider.com/2016/06/proposed-amendment-to-illinois-biometrics-privacy-law-introduced-then-stalled/.

99 *Id.*

100 *Id.*

101 Tex. Bus. & Com. Code Ann. § 503.001 (2009).

102 *Id.* § 503.001(b).

103 *Id.* § 503.001(a).

	BIPA	CUBI
Prohibit Collection of Biometric Identifiers without informed consent?	Yes	Yes
Definition of "biometric identifier"	A retina or iris scan, fingerprint, voiceprint, or ***scan*** of hand or face geometry	A retina or iris scan, fingerprint, voiceprint, ***or record*** of hand or face geometry
Definition of "biometric identifier" expressly exclude photographs?	Yes	No
Private Right of Action?	Yes	No

2. Unique Identifying Information Derived From Photographs Would Appear to Fall Under the Plain Text of Proposed Biometric Privacy Statutes in Other States

Proposed biometric privacy statutes in other states have varying definitions of "biometric information." For example, Alaska has a proposed biometric privacy statute that defines broadly **"biometric data"** as "fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual."[104] It defines further **"biometric information"** as "data used in a biometric system," and defines **"biometric system"** as an automated system that [1] captures biometric data from an individual's biometric information [2] extracts, processes, and stores that captured biometric data, and [3] compares the extracted biometric data from the individual with stored biometric data for recognition of the individual.[105] The proposed Alaska law does not apply to the collection, retention, analysis, disclosure, or distribution of "photographs," unless the photograph is collected for use in a biometric system.

Based on the text of the proposed statute, if the allegations in the existing BIPA photograph-based facial recognition BIPA suits are true, it would appear that uploading photographs to Facebook or Google Photos would be considered a photograph collected for use in a biometric system because:

[1] The defendants allegedly capture biometric data from an individual's biometric information;

[2] The defendants allegedly extract and processes that data; and

---

104 H.B. 96, 29th Leg. (Alaska 2015).

105 *Id.* § 18.14.090.

[3] The defendants allegedly compare the extracted data with an existing biometric data database to recognize the individual.

Before going dormant last September, California proposed a bill that would have extended the scope of California's data security law to biometric data. California's proposed amendment defined "biometric information" as "data generated by automatic measurements of an individual's fingerprint, voice print, eye retinas or irises, identifying DNA information, or unique facial characteristics, which are used by the owner or licensee to uniquely authenticate an individual's identity."[106]

New York's pending amendment defines biometric information as " . . . data generated by automatic measurements of an individual's physical characteristics, which are used by the owner or licensee to authenticate an individual's identity[.]"[107]

Under either definition, it would again appear that algorithms taking automatic measurements of a person's unique biological characteristics, even though through a photograph, would constitute biometric information. Neither of the proposed bills have an exclusions for photographs or information derived from photographs.

VI. PART FIVE: THE EFFECT THE UNCERTAIN BIOMETRIC LEGAL LANDSCAPE HAS ON PROTECTING GENUINE BIOMETRIC INFORMATION

The practical applications of facial recognition technology are seemingly limitless. Facial recognition technology offers convenience. For instance, Apple has a patent for using facial recognition to unlock an iPhone. Apple's patent application touts the convenience of this feature: "[it] would eliminate some of the time-consuming steps for unlocking a device. As it stands now, users need to drag a slide bar and enter a password, steps that some might find inconvenient."[108]

Facial recognition technology provides security benefits too. Companies such as FaceFirst rely on facial recognition technology to provide security services to other companies. Among the many security benefits FaceFirst provides include sending descriptive alerts when an unwanted individual walks into your building; flagging individuals who have caused problems previously; monitoring the movement of people in your facility to ensure that no one is in an unauthorized area; and eliminating the possibility of misidentification of criminals who are using false identification.[109]

But in a consumer driven world, arguably facial recognition technology's most valuable use will be targeted advertising; it can be used to track the likes and dislikes of specific individuals. For instance, companies like Affectiva use facial recognition

---

106 A.B. 83, 2015-2016 Leg., Reg. Sess. (Cal. 2015).

107 A.B. 06866, 2015-2016 Leg., Reg. Sess. (N.Y. 2015).

108 Abin Sam, *Now Unlock your Devices with a Selfie!,* Khurana & Khurana (July 20, 2015), http://www.khuranaandkhurana.com/2015/07/20/now-unlock-your-devices-with-a-selfie/; *see* U.S. Patent No. 8,994,499.

109 FaceFirst, http://www.facefirst.com/services/commercial-security; http://www.facefirst.com/services/law-enforcement (last visited October 6, 2016).

technology to measure and analyze the moment-to-moment facial expressions of people watching videos. To marketers, a person's visceral response to a video can be more accurate than their verbal description.[110] It should come as no surprise then that the facial recognition market is expected to grow to $6.19 billion by 2020.[111] The use of biometrics will only continue to grow.

The dearth of consumer privacy biometric statutes, however, and the corresponding disconnect between the judicial interpretation of BIPA and its plain text, greatly impacts biometrics. This uncertain landscape has allowed savvy class action attorneys to target social media giants such as Facebook and Google in seeking multi-million dollar judgments against them. Are these suits, which allege BIPA consent violations, and not that the purported biometric information has been compromised, intended to safeguard biometric information?

Ironically, BIPA and CUBI were enacted nearly one decade ago, which is an eternity when it comes to technology. Although at the forefront of the biometric information privacy and consumer interface, companies that do collect, store, and use biometric information are still uncertain of their legal obligations. Accordingly, these companies will likely focus on how to avoid suit as opposed to protecting genuine biometric information. Until the laws catch up with the technology, this discord will persist.

It may take many years for BIPA to become settled and many more for federal and state laws to catch up with biometric technology generally. In the interim, companies in the biometric industry should keep abreast of the following:

1. What other states are on the verge of passing biometric legislation?
2. Are any states proposing laws that would generate biometric privacy litigation?
3. Are there any proposed federal laws that would generate biometric privacy litigation?
4. Are there any proposed amendments to existing biometric privacy statutes, like BIPA and CUBI?
5. From what sources are the purported biometric information derived? Photographs?
6. Are the persons filing suit users or non-users of the company's services?
7. Does the state statute allow for a private right of action, or can only the State Attorney General file suit?
8. In what state is the private entity being sued? Is there personal jurisdiction?
9. In what court (state v. federal) is the private entity being sued? Can the suit be removed to federal court?

---

110 E.J. Schultz, *Facial-Recognition Lets Marketers Gauge Consumers' Real Responses to Ads,* AdvertisingAge (May 18, 2015), http://adage.com/article/digital/facial-recognition-lets-marketers-gauge-real-responses/298635/.

111 Press Release, Facial Recognition Market worth $6.19 Billion by 2020, Markets and Markets, http://www.marketsandmarkets.com/PressReleases/facial-recognition.asp.

10. What harm is the plaintiff alleging? Does this harm rise to the standard required under *Spokeo* to grant the federal court subject matter jurisdiction? Does this harm rise to establish the plaintiff is an "aggrieved party" as required under BIPA?

11. Is there an arbitration agreement that waives class actions?

12. What constitutes notice before a company can collect or use biometric information?

13. What are the existing requirements for a company to store or destroy biometric information after it has been collected?

These questions may help provide companies with direction as they navigate in an ever evolving and uncertain biometric legal world.

"CLEAR AND CONSPICUOUS" DISCLOSURES BETWEEN CELEBRITY ENDORSERS AND ADVERTISERS ON SOCIAL MEDIA WEBSITES

By Shafiel A. Karim[1]

I. INTRODUCTION

A. Recent Celebrity Endorsement Gaffes on Social Media

On August 17, 2016 the Kardashian women—America's "First" celebrity family—were served with a demand letter from Truth In Advertising ("TINA.org").[2] TINA.org alleged, "members of the Kardashian . . . women are engaged in deceptive marketing campaigns . . . by routinely creating and publishing sponsored social media posts . . . without clearly and conspicuously disclosing that they are paid representatives . . . ."[3] TINA.org published the letter and a database of 108 posts that allegedly violate federal disclosure rules.[4] The Kardashian women had one week to comply with TINA.org's demands.[5]

The Kardashian women apparently failed to satisfy the demands because on August 25, 2016, TINA.org notified the Federal Trade Commission ("the Commission") of the alleged violations.[6] TINA.org complained to the Commission that the Kardashian . . . women published a "plethora of posts that do not clearly or conspicuously disclose the [Kardashians'] material connections to the [advertising] companies featured or promoted in the posts or that the posts are advertisements as is required by law."[7]

---

1 Shafiel A. Karim is a solo practitioner in Southern California who represents small businesses and entrepreneurs in transactional and litigation matters as well as plaintiffs in consumer class actions.

2 Letter from Truth in Advertising to Kris Jenner, Kardashian family Manager (Aug. 17, 2016), https://www.truthinadvertising.org/wp-content/uploads/2016/08/8_17_16-ltr-from-TINA-to-K_Jenner-and-M_Kump_Redacted.pdf (last visited Oct. 10, 2016).

3 *Id.*

4 *Kardashian/Jenner Databas*e, TruthInAdvertising.org, https://www.truthinadvertising.org/kardashianjenner-database/ (last visited Sept. 27, 2016).

5 *Supra* note 2.

6 Letter from Truth in Advertising to FTC re: Kardashians (Aug. 25, 2016), https://www.truthinadvertising.org/wp-content/uploads/2016/08/8_25_16-ltr-from-TINA-to-FTC-re-Kardashian-Jenner-Instagram-posts.pdf (last visited Aug. 29, 2016).

7 *Id.*

In response, only 27 of the 108 posts identified by TINA.org's August 17 letter were revised to include the hashtag[8] "#ad" and only four were deleted.[9] But "the vast majority of the posts . . . remain[ed] unchanged."[10] TINA.org added, "The willingness of the Kardashians . . . to alter their Instagrams . . . suggests they would also fix other similarly deceptive posts if permitted to do so by the other companies they endorse."[11] As a result, TINA.org surmised, "it is apparent that the issue is with the [advertisers], who continue to flagrantly ignore the law."[12] The Kardashian womens' gaffe shows the need for greater clarity in federal disclosure rules and regulatory enforcement of social media endorsements.

Of course, the Kardashian women are not the only celebrities who promote and advertise products on social media without making appropriate disclosures. On September 6, 2016, Britney Spears posted a "selfie" applying EOS lip care products on Instagram exclaiming, "Yessss @eosproducts . . . Always saving my lips in the dry Vegas heat! #BritneyXeos."[13] Spears was identified as a paid EOS "brand ambassador" in a recent class action complaint against the lip care company.[14] On April 2, 2016, LeBron James posted a picture of a half-eaten pizza from Blaze Pizza on Instagram and wrote, "Had to stop by my favorite place to eat. Nothing like @blazepizza!!"[15] James failed to disclose his role as an investor in Blaze Pizza.[16] Justin Timberlake, a spokesperson for Sauza tequila, posted pictures of a tequila party that prominently showcased Sauza 901 tequila on a golf course on June 10, 2015. Timberlake failed to mention his financial relationship with the company.[17] The list of celebrity offenders is certainly long but their approach to sponsorship is usually

---

8 A hashtag is a pound symbol ("#") followed by a combination of alphanumeric characters and was not designed with federal disclosure rules in mind. Hashtags are also "bookmarks" or "symbol[s] of community membership." Lei Yang, et al., *We Know What @You #Tag: Does the Dual Role Affect Hashtag Adoption?* (2012), https://pdfs.semanticscholar.org/3050/ac83859cd059b28d63db1e93a00fffda8b29.pdf (last visited Sept. 30, 2016). Invented by Twitter to label and organize tweets, the hashtag has cross-pollinated to every major social media platform as well as popular culture and modern vernacular. *See, e.g.*, Miles Efron, *Hashtag Retrieval in Microblogging Environment*, SIGIR 2010 Geneva (2010), http://people.ischool.illinois.edu/~mefron/papers/efron-sigir2010.pdf (last visited Sept. 27, 2016); Allison Shapp, *Variation in the Use of Hashtags* (Spring 2014), http://www.nyu.edu/projects/shapp/Shapp_QP2_Hashtags_Final.pdf (last visited Sept. 27, 2016).

9 Letter from Truth in Advertising to FTC re: Kardashians (Aug. 25, 2016), https://www.truthinadvertising.org/wp-content/uploads/2016/08/8_25_16-ltr-from-TINA-to-FTC-re-Kardashian-Jenner-Instagram-posts.pdf (last visited Aug. 29, 2016).

10 *Id.*

11 *Id.*

12 *Id.*

13 Britney Spears (@britneyspears), Instagram (Sept. 6, 2016), https://www.instagram.com/p/BKBlBqABq_u/?hl=en (last visited Aug. 29, 2016); *see* Exhibit A.

14 *Nicole E. Caggiano v. EOS Products, LLC, et al.*, No. 1:16-cv-00408 (S.D.N.Y. Jan. 19, 2016).

15 LeBron James (@kingjames), Instagram (Apr. 2, 2016), https://www.instagram.com/p/BDtX6H9iTMX/ (last visited Sept. 27, 2016); *see* Exhibit B.

16 Charlotte Wilder, *Papa 'Brons? A LeBron-Approved Pizza Chain is Coming to Boston Soon*, The Boston Globe (Feb. 17, 2016), http://www.boston.com/culture/food/2016/02/17/papa-brons-a-lebron-approved-pizza-chain-is-coming-to-boston-soon (last visited Sept. 23, 2016).

17 Justin Timberlake (@justintimberlake), Instagram (June 10, 2015), https://www.instagram.com/p/3w5dz8ydvw/?hl=en (last visited Sept. 28, 2016); *see also* Sauza 901, https://www.sauza901.com/#/home (last visited Sept. 28, 2016); *see* Exhibit C.

relatively simplistic as indicated by the content of the aforementioned posts. However, some celebrities take an even more sophisticated approach.

Exhibit A

britneyspears Follow

295k likes 5w

britneyspears Yessss @eosproducts... Always saving my lips in the dry Vegas heat! #BritneyXeos

view all 3,140 comments

emilly_vitoria_fontenele Tá a cara da Ivete

amy.lucio.7 Glory is great

ediside1 😍😍😍😍😍😍😍😍😍

sunzedd my goddess! !

bvolk2 I suppose @dillicious11

jcquatti Wow .. salvador dali ..!!

nunu2223 @britneyspears love you in this hat!

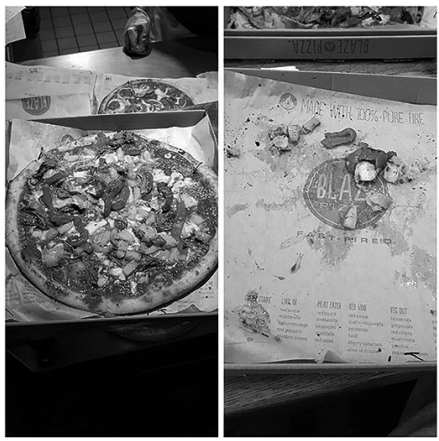
kissss4277 😘

ainamkoz_askhat Beautiful girl

alexxuber 🖤YOU'RE MY LIFE @britneyspears🖤BRAZIL🤍🖤

Log in to like or comment. ◦◦◦

Exhibit B



kingjames Follow

172k likes 27w

kingjames Had to stop by my favorite place to eat. Nothing like @blazepizza!! Before, less than 5 mins later After! Gone baby gone! If u in the Columbus area check it out on 1708 N. High St as well as many other locations across the US. #Yummy #BestPieYouCouldGet

view all 3,141 comments

tgags__92 @rileyccameron get a life u know Lebron stinks so why can't you admit it?

rccam10 @tgags__92 maybe because every nba finals he's won he got mvp?

rccam10 @tgags__92 stick to hockey obviously you know nothing about basketball

tgags__92 The reason why he always gets mvp is because he has skilled teammates who pass to him all the time such as Dwayne wade or kyrie Irving.

Log in to like or comment. ◦◦◦

Exhibit C

Selena Gomez recently posted a photograph of herself ostensibly watching *The Big Bang Theory* on a laptop. Gomez wrote, "The one thing that gets me going . . . Sheldon Cooper—Big Bang Theory."[18] The photograph depicts Gomez sitting on a chair in a dressing room with a cup in hand watching the popular sitcom. Gomez's head is turned away from the camera. But immediately adjacent to Gomez's laptop is an out-of-focus bottle of Coca-Cola. Further out-of-focus is a bottle of Smartwater on the dressing room table, another Coca-Cola product. Gomez of course, is a spokesperson for The Coca-Cola Company.

Exhibit D

This link between celebrities and product endorsements is nothing new. Marketers have a longstanding tradition of using celebrity spokespersons to advertise and promote goods and services.[19] However, this tendency has become nearly ubiquitous in recent

---

18 Selena Gomez (@selenagomez), INSTAGRAM, https://www.instagram.com/p/BG8tKDpujGH/?hl=en (last visited Sept. 27, 2016); *see Exhibit D.*

19 Leah W. Feinman, *Celebrity Endorsements in Non-Traditional Advertising: How the FTC Act Regulations Fail to Keep Up with the Kardashians, 22* FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 103-110 (2011).

years. Today, approximately fourteen to nineteen percent of all advertisements in the United States feature celebrity endorsements.[20] But it is not only the advertisers who favor these agreements. For example, Shaquille O'Neal is reportedly paid five million dollars per year to tweet positive endorsements for goods and services.[21] To put this into perspective, if O'Neal tweeted once daily and utilized the full 140-character limitation of Twitter, he would earn ninety-seven dollars per character. In fact, celebrities sometimes make more from their endorsement deals with advertisers than they do through their day jobs.[22]

Traditionally, the Commission's policy regarding such product placement favored advertiser self-regulation, but this method of regulation has recently become outdated.[23] Traditional media like newspapers, magazines, radio, and television created and distributed curated content that was only distributed to the public after passing editorial and regulatory scrutiny.[24] Self-regulation worked because the few large content creators and distributors almost exclusively controlled the flow of content. With so few points of origination, the Commission could better supervise advertising in spite of its laissez-faire approach.

All of that changed, however, with the advent of social media because it democratized the creation and distribution of content. Today, anyone can distribute content worldwide without any editorial or regulatory compliance filter. The absence of such restrictions has resulted in a lack of source identification in celebrity endorsements, a problem that has engendered distress for advertisers.

A 2012 survey reported that forty-five percent of responding advertising agencies were concerned about the lack of transparency in celebrity endorsed social media content.[25] But the lure of selling product is so great that only twenty-nine percent of responding advertising agencies discontinued their use of paid social media campaigns.[26]

This current state of affairs cannot endure. If advertisers continue creating product awareness on social media through celebrity endorsements, advertisers should brief endorsers regarding federal advertising laws including disclosure rules. Further, advertisers should contractually obligate endorsers to comply with those laws, and monitor endorsers to ensure compliance. To aid advertisers in their compliance, the Commission should clarify existing ambiguities in its regulations and guides with regard

---

20 Kevin Plank, *Under Armour's Founder on Learning to Leverage Celebrity Endorsements,* Harv. Bus. Rev., May 2012.

21 Kevin Gray, *Twitter Athletes: $5 Million in 140 Characters,* Men's Journal (Nov. 19, 2013), http://www.mensjournal.com/magazine/twitter-athletes-5-million-in-140-characters-20131119 (last visited Oct. 12, 2016).

22 Andre McNeil, *Athletes Who Make More From Endorsements Than Sports,* Investopedia, http://www.investopedia.com/financial-edge/1012/athletes-who-make-more-from-endorsements-than-playing-sports.aspx (last visited Sept. 27, 2016).

23 A.J. Casale, *Going Native: The Rise of Online Native Advertising and a Recommended Regulatory Approach,* 65 Cath. U.L. Rev. 129, 133 (2015).

24 Douglas Holt, *Branding in the Age of Social Media,* Harv. Bus. Rev. (Mar. 2016).

25 RSW/US, *Changes in Social Digital Media 2009-2012,* http ://www.rswus.com/images_and_uploads/Changes-in-Social-Digital-Media-2009-2012.pdf (last visited Sept. 10, 2016).

26 *Id.*

to advertising on social media. Finally, social media companies should exercise some editorial or regulatory compliance control over the content created and published on their platforms.

II. A BRIEF HISTORY OF ADVERTISING LAWS

A. Commercial Speech and the First Amendment

The First Amendment offers robust protection for political, literary, and artistic speech with few exceptions. Indeed, Justice Cardozo described the First Amendment as "the matrix, the indispensable condition of nearly every other form of freedom."[27] But commercial speech—"expression related solely to the economic interests of the speaker and its audience"—is the proverbial stepsibling of high value political, literary and artistic speech.[28] The Supreme Court said commercial speech is of "less constitutional moment" than non-commercial speech, and analyzes commercial speech protection with "less enthusiasm and with less exacting scrutiny" than it does non-commercial speech.[29]

Endorsements by celebrities are commercial speech because they are intended to sell goods and services. Until relatively recently, it was unclear whether commercial speech was entitled to full First Amendment protection. In *Valentine v. Chrestensen*, the Supreme Court concluded political speech could not be regulated but that "the Constitution imposes no such restraint on government as respects purely commercial advertising."[30] Since *Valentine*, the Court has expanded First Amendment protection of commercial speech and further developed the analysis to determine constitutionality.[31] Later, in an eight to one opinion, Justice Kennedy wrote:

> The commercial marketplace, like other spheres of our social and cultural life, provides a forum where ideas and information flourish. Some of the ideas and information are vital, some of slight worth. But the general rule is that the speaker and the audience, not the government, assess the value of the information presented.[32]

Nevertheless, while normal commercial speech may enjoy some First Amendment protection, the First Amendment does not protect false or misleading commercial

---

27 *Palko v. Connecticut,* 302 U.S. 319, 327 (1937) *overruled by Benton v. Maryland,* 395 U.S. 784 (1969) on other grounds.

28 *Cent. Hudson Gas & Elec. Corp. v. Public Serv. Comm'n,* 447 U.S. 557, 561 (1980); *see also* Elliot Zaret, *Commercial Speech and the Evolution of the First Amendment,* WASH. LAWYER (Sept. 2015).

29 *Id.* at 562 n. 5; *Cincinnati v. Discovery Network,* 507 U.S. 410, 435 (1993).

30 *Valentine v. Chrestensen,* 316 U.S. 52 (1942).

31 *See, e.g., Cent. Hudson Gas & Elec. Corp.,* 447 U.S. 557, 561 (1980) (Justice Powell articulated a four-part test that asks (1) whether expression protected by First Amendment; (2) whether commercial speech concerns lawful activity and is not misleading; (3) whether governmental interest is substantial; and (4) whether regulation directly advances government interest and is not more extensive than necessary to advance that interest).

32 *Edenfield v. Fane,* 507 U.S. 761, 767 (1993).

speech.[33] Prior to joining the Supreme Court, Justice Powell wrote, "advertising . . . must meet the most exacting standards of accuracy and professional excellence."[34] Commercial speech is misleading if the speaker furnishes insufficient material information to the audience that "restrict[s] the . . . flow [of information] to consumers" and potentially results in a purchase decision that may not otherwise have been made.[35]

Indeed, in *Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.,* the Supreme Court explained, "Untruthful speech, commercial or otherwise, has never been protected for its own sake . . . .The First Amendment as we construe it today, does not prohibit the State from insuring that the stream of commercial information flow cleanly as well as freely."[36] Similarly, in *Friedman v. Rogers,* the Supreme Court held a state requiring the "publication of additional information [that] could clarify or offset the effects of spurious communication" does not run afoul of the First Amendment's protection of commercial speech.[37] This principle undergirds the constitutionality of regulating advertisers that disseminate deceptive advertisements as demonstrated by several circuits that have expanded on the rule in *Friedman*.

For example, the Third Circuit held "[a]ny remedy formulated by [the Commission] that is reasonably necessary to prevent false or misleading practices does not impinge upon constitutionally protected commercial speech."[38] Further, the Fourth Circuit held that the Commission's regulations requiring the disclosure of funeral fees do not violate the First Amendment because not disclosing the fee "is misleading and poses no barrier to remedy formulated by [the Commission] reasonably necessary to prevent future deception."[39] To summarize, the First Amendment protects commercial speech but governmental regulation of commercial speech is not unconstitutional.

B. Federal Statutes

To prevent deceptive commercial speech, the legislature passed multiple bills mandating disclosure of material information. Congress passed the Newspaper Publicity Act in 1912 ("NPA") to clearly distinguish advertisements for journalism. In pertinent part,

---

33 *Cent. Hudson Gas,* 447 U.S. at 563 ("there can be no constitutional objection to the suppression of commercial messages that do not accurately inform the public about lawful activity"); *Gertz v. Robert Welch, Inc.,* 418 U.S. 323, 340 (1974) ("there is no constitutional value in false statements of fact"); Konigsberg v. State Bar, 366 U.S. 36, 49 n.10 (1961) (libel, slander, obscenity, perjury, and false advertising not protected by First Amendment).

34 Letter from Lewis F. Powell, Jr., to Eugene B. Sydnor, Jr., Chairman of the U.S. Chamber of Commerce Education Committee (Aug. 23, 1971) http://law2.wlu.edu/deptimages/Powell%20Archives/PowellMemorandumTypescript.pdf (last visited Oct. 7, 2016).

35 *Bates v. State Bar of Ariz.,* 433 U.S. 350, 374 (1977).

36 425 U.S. 748, 771-72 (1976).

37 *Friedman v. Rogers,* 440 U.S. 1, 12 n.11 (1979); *Goodman v. Ill. Dep't of Fin. & Prof'l Regulation,* 430 F.3d 432 (7th Cir. 2005).

38 *United States v. Reader's Digest Ass'n,* 662 F. 2d 955 (3d Cir. 1981); *United States v. Raymond,* 228 F.3d 804 (7th Cir. 2000)(no First Amendment protection for government prevention of false or misleading commercial speech); *United States v. Phillip Morris USA, Inc.* (566 F.3d 1095 (D.C. App. 2009) (no First Amendment protection for fraudulent and deliberate misrepresentations).

39 *Harry & Bryant Co. v. FTC Act,* 726 F.2d 993 (4th Cir. 1984).

the NPA stated: "all editorial or other reading matter published . . . [for] which money or other valuable consideration is paid . . . shall be plainly marked 'advertisement.'"[40] The NPA was designed to regulate native advertising or "advertorials," which were advertisements guised as news reporting.[41] Like the NPA, Congress passed the Radio Act of 1927 ("Radio Act"), which required broadcasters to distinguish paid advertisements from original programming.[42]

Two years after the NPA was passed, President Woodrow Wilson signed the Federal Trade Commission Act ("FTC Act") into law, creating the Commission. Originally, the Commission's mandate was similar to the impetus behind the Sherman Antitrust Act of 1890: regulate unfair methods of competition in the form of monopolies and trust.[43] But in 1938, the Wheeler-Lea Act expanded the Commission's authority to include regulation of "unfair or deceptive acts or practices," which is the source of the Commission's current authority to regulate advertising generally and endorsements specifically.[44]

C. Federal Regulations and Guides

As part of its enforcement mandate, the Commission has interpreted the FTC Act by promulgating regulations and publishing guides informing advertisers, endorsers, and the public at large of its endorsement policies and enforcement principles. The Commission defines an endorsement as "any advertising message . . . that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser."[45] Like all commercial speech, an endorsement must not be false or misleading and "must reflect the honest opinions, findings, beliefs, or experience of the endorser."[46] Although the Commission proscribes dishonesty in its guides and regulations, it does not describe how advertisers should ensure their advertisements are not unfair or deceptive. The FTC Act is also silent regarding celebrity endorsements on social media.

D. The FTC's Endorsement Guides: What People Are Asking

To supplement the promulgated regulations codified in the Code of Federal Regulations, the Commission has published several guides. In 2015, the Commission

---

40 62 Cong. Ch. 389.

41 The NPA was part of a larger bill that regulated the postal service and required newspapers and magazines to disclose circulation information, among other things. Shortly after the NPA was, a constitutional challenge followed. However, the Supreme Court held Congress has the authority to regulate the mails and for that reason the NPA's requirement that native advertising be marked "advertisement" was constitutional. *Lewis Pub. Co. v. Morgan*, 229 U.S. 288 (1913). The Court's analysis was limited to Congress' authority to regulate the mails, not the government's authority to regulate commercial speech.

42 69 Cong. Ch. 169.

43 15 U.S.C. § 45(a)(2); Marc Winerman, *The Origins of the FTC: Concentration, Cooperation, Control, and Competition*, 71 Antitrust L.J. 1, 96 (2003).

44 Winerman, *supra* note 43.

45 16 CFR 255.

46 16 CFR 255.1.

published "The FTC's Endorsement Guides: What People Are Asking." This Guide describes hypothetical factual scenarios followed by the Commission's application of the promulgated regulations. In a prescient factual hypothetical uncannily similar to the quagmire the Kardashian women currently face, the Commission considers the following:

> A famous celebrity has millions of followers on Twitter. Many people know that she regularly charges advertisers to mention their products in her tweets. Does she have to disclose when she's being paid to tweet about products?
>
> It depends on whether her followers understand that her tweets about products are paid endorsements. If a significant portion of her followers don't know that, disclosures are needed. Again, determining that could be tricky, so we recommend disclosure.[47]

Consistent with commercial speech jurisprudence, the analysis focuses on the impact that the undisclosed commercial speech has on the audience and the likelihood of resulting confusion. But this suggests that the standard may not be much of a standard at all; if the social media post is commercial in character, it should be disclosed irrespective of what a "significant portion" of the audience may know because successfully determining what a "significant portion" of a large audience knows is likely impossible.[48]

Further, the Guide does not clarify how celebrities can clearly and conspicuously disclose the material connection with the advertiser.[49] Some have proposed hashtags like "#ad" as clear and conspicuous disclosures. On the one hand, the Commission concluded a hashtag is not a clear and conspicuous disclosure because "it won't tell consumers of your relationship to the [advertiser]," which is a material fact since endorsements are considered more credible when they are not paid.[50] On the other hand, the Commission considers hashtags like "#ad" to "likely be effective":

---

47 *The FTC Act's Endorsement Guides: What People Are Asking*, Federal Trade Commission (May 2015) https://www.ftc.gov/system/files/documents/plain-language/pdf-0205-endorsement-guides-faqs_0.pdf (last visited Oct. 11, 2016).

48 For example, the Guide ignores the fact that many users on social media are infants. In fact, the minimum age to create a user account on Facebook, Instagram, and Twitter is thirteen. Some estimates suggest Facebook alone has thirteen million teenage users. *See* Ryan W. Neal, *Facebook Gets Older: Demographic Report Shows 3 Million Teens Left Social Network In 3 Years*, International Business Times (Jan. 16, 2014), http://www.ibtimes.com/facebook-gets-older-demographic-report-shows-3-million-teens-left-social-network-3-years-1543092 (last visited Sept. 27, 2016).

49 A material financial connection includes "either the payment or promise of compensation prior to and in exchange for the endorsement." 16 CFR 255.5. A connection is material and subject to the disclosure rules if "it would likely affect the consumer's conduct or decisions with regard to a product or service." FTC Statement on Deception, 103 F.T.C. 174, 175 (1984) (*appended to Cliffdale Assocs., Inc.*, 103 F.T.C. 110 (1984)); *see also* 81 FR 22596. The Supreme Court agreed with the Commission's position that "the misrepresentation of any fact" is material if it affects a consumer's purchase decision. *See FTC v. Colgate Palmolive*, 380 U.S. 374, 386-387 (1965). It is also well settled that "[a]ctual injury is not required." *In re Cliffdale Associates, Inc., et al.*, 103 F.T.C. 110, 107 n.11 (1981). The materiality requirement is satisfied if "an act or practice . . . [is] likely to cause injury to be considered deceptive." *Id.*

50 *Supra* note 47; *see also* 16 CFR 255.5.

What about a platform like Twitter? How can I make a disclosure when my message is limited to 140 characters?

The FTC isn't mandating the specific wording of disclosures. However, the same general principle—that get the information they need to evaluate sponsored statements—applies across the board, regardless of the advertising medium. The words "Sponsored" and "Promotion" use only 9 characters. "Paid ad" only uses 7 characters. Starting a tweet with "Ad:" or "#ad"—which takes only 3 characters—would likely be effective.

III. ANALYSIS

A. The Problem

The Commission's current regulations are ambiguous because (1) the "clearly and conspicuously disclose" standard is not "synonymous" with the "clearly and prominently disclose" standard and it is unclear what factual circumstances warrant the application of one standard instead of the other; (2) the Commission's definition of "significant minority" is too expansive and should be redefined using class action jurisprudence; (3) the Commission's enforcement activity in social media is sporadic or non-existent; (4) the Commission provides conflicting guidance on the use of hashtags in social media endorsements; and (5) the Commission does not affirmatively and unambiguously describe what word or combination of words constitutes a proper disclosure.

1. "Clearly and Conspicuously Disclose" Is Not Synonymous with "Clearly and Prominently Disclose"

The Commission requires endorsers to "clearly and conspicuously disclose" a material financial connection with advertisers.[51] A material financial connection includes "either the payment or promise of compensation prior to and in exchange for the endorsement."[52] A connection is material and subject to the disclosure rules if "it would likely affect the consumer's conduct or decisions with regard to a product or service."[53] The Supreme Court agreed with the Commission's position that "the misrepresentation of any fact" is material if it affects a consumer's purchase decision.[54] It is also well settled that "[a]ctual injury is not required."[55] The materiality requirement is satisfied if "an act or practice . . . [is] likely to cause injury to be considered deceptive."[56]

---

51 16 CFR 255.5.

52 *Id.*

53 FTC Statement on Deception, 103 F.T.C. 174, 175 (1984) (*appended to In re Cliffdale Associates, Inc.*, 103 F.T.C. 110 (1984)); *see also* 81 FR 22596.

54 *See FTC v. Colgate Palmolive,* 380 U.S. 374, 386-387 (1965).

55 *Cliffdale Associates,* 103 F.T.C. 107 n.11 (1981).

56 *Id.*

But in some rules, guides, and enforcement actions, the Commission has also articulated a "clearly and prominently disclose" standard.[57] In one guide, the Commission claims "clearly and prominently" and "clearly and conspicuously" are "synonymous" but that "[t]hey may have different meanings under other statutes."[58] In practice, however, the "clearly and prominently disclose" standard appears to be less comprehensive than the "clearly and conspicuously disclose" standard. For example, compare the Commission's orders in *In re Machinima, Inc.* and *In re Warner Bros. Home Videos.*

a. *In re Machinima, Inc.*[59]

In 2013, Microsoft Corporation hired Starcom MediaVest Group, an advertising agency, to help advertise and promote its Xbox One video game console.[60] In turn, Starcom hired Machinima, Inc., a network of channels on YouTube with nearly three billion monthly views and 400 million active subscribers, to create and publish game reviews showcasing Microsoft's game console.[61] Machinima paid $15,000 to $30,000 to YouTube influencers to create and publish the actual videos.[62] These influencers were later paid an additional one dollar per thousand views up to $25,000. The influencers were contractually obligated to keep their compensation confidential.[63] In March 2016, the Commission issued an order using the "clearly and prominently disclose" standard.

b. *In re Warner Brothers Home Entertainment, Inc.*[64]

In 2014, a Warner Brothers division hired several YouTube influencers to create video play-by-play reviews of its new video game *Middle Earth: Shadow of Mordor.*[65] The hyperlinks to these videos were subsequently posted on other social media websites like Twitter and Facebook.[66] Warner Brothers required the endorsers to post an "FTC disclaimer" in the description section beneath the video on YouTube but "did not require that the YouTube influencers be instructed to place sponsorship disclosures clearly and conspicuously in the video itself."[67] "[C]onsumers ha[d] to click on a 'Show More' button

---

57 *See, e.g., In re Machinima, Inc.,* FTC Docket No. C-4569 (Mar. 16, 2016),https://www.ftc.gov/system/files/documents/cases/160317machinimado.pdf (last visited Sept. 28, 2016); *In re AmeriFreight, Inc.,* FTC Docket No. C-4518 (Apr.13, 2015),https://www.ftc.gov/system/files/documents/cases/150420amerifreightdo.pdf (last visited Sept. 28, 2016).

58 *.com Disclosures: How to Make Effective Disclosures in Digital Advertising,* 6 n.18, Federal Trade Commission (Mar. 2013) https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf (last visited Oct. 9, 2016).

59 Complaint, *In re Machinima, Inc.,* FTC Docket No. C-4569 (Sept. 2, 2015), https://www.ftc.gov/system/files/documents/cases/150902machinima-cmpt.pdf (last visited Sept. 28, 2016).

60 *Id.* at 1.

61 *Id.*

62 *Id.* at 3.

63 *Id.* at 4.

64 Complaint, *In re Warner Bros. Home Entertainment, Inc.,* FTC File No. 152-3034 (Jul. 11, 2016) https://www.ftc.gov/system/files/documents/cases/160711warnerbroscmpt.pdf (last visited Sept. 28, 2016).

65 *Id.* at 1-2.

66 *Id.* at 3.

67 *Id.*

in the description box and potentially scroll down before they c[ould] see the sponsorship disclosure."[68] In July 2016, the Commission issued an order using the "clearly and conspicuously disclose" standard.

c. *In re Lord & Taylor, LLC*[69]

In 2014, clothing company Lord & Taylor hired fifty influencers on social media.[70] The influencers were paid to post photographs of themselves wearing Lord & Taylor's clothes and post the photographs on social media websites like Instagram.[71] Lord & Taylor required the influencers to include "@lordandtaylor" and "#DesignLab" in the photograph posts but did not require the influencers to disclose the fact that they were paid to take and post the photographs.[72] Approximately 11.4 million users viewed the photographs taken and posted by the influencers.[73] Some of the influencer's photographs were subsequently featured in a fashion magazine.[74] The Commission's Order repeated the "clearly and conspicuously" definition in *Warner Brothers*.[75] In May 2016, the Commission issued an order using the "clearly and conspicuously disclose" standard and defined the phrase using the verbatim language from *Warner Brothers*.

d. *In re AmeriFreight, Inc., et al.*[76]

In 2015, AmeriFreight, Inc. offered its customers discounts if they wrote and posted positive reviews on various social media websites.[77] AmeriFreight offered its customers additional remuneration if their review was deemed most "creative" and "informative."[78] The terms of the discount did not require any disclosure of the fact that the endorser would receive a discount in exchange for a positive review.[79] In April 2015, the Commission issued an order using the "clearly and prominently" standard and defined the phrase using the verbatim language from *Machinima*.[80]

---

68 *Id.* at 3.

69 Complaint, *In re Lord & Taylor, LLC,* FTC Docket No. C-4576 (May 23, 2016),https://www.ftc.gov/system/files/documents/cases/160523lordtaylorcmpt.pdf (last visited Oct. 9, 2016).

70 Complaint, *In re Warner Bros. Home Entertainment, Inc.,* FTC File No. 152-3034 (July 11, 2016), https://www.ftc.gov/system/files/documents/cases/160711warnerbroscmpt.pdf (last visited Sept. 28, 2016).

71 *Id.*

72 *Id.*

73 *Id.*

74 *Id.*

75 *Id.* at 3-4.

76 *See In re AmeriFreight, Inc.,* FTC Docket No. C-4518 (Apr. 20, 2015), https://www.ftc.gov/system/files/documents/cases/150420amerifreightcmpt.pdf (last visited Sept. 28, 2016).

77 Complaint, *In re Warner Bros. Home Entertainment, Inc.,* FTC File No. 152-3034 (July 11, 2016), https://www.ftc.gov/system/files/documents/cases/160711warnerbroscmpt.pdf (last visited Sept. 28, 2016).

78 *Id.* at 2-3.

79 *Id.*

80 Order, *In re AmeriFreight, Inc.,* FTC Docket No. C-4518 (Apr. 20, 2015), https://www.ftc.gov/system/files/documents/cases/150420amerifreightdo.pdf (last visited Sept. 28, 2016).

e. *Machinima*, *Warner Brothers*, *Lord & Taylor*, and *AmeriFreight* Compared

Both Machinima and Warner Brothers used YouTube influencers to advertise and promote video game products through endorsements and both companies failed to require the influencers to disclose the fact that they were paid to endorse the video game products. Lord & Taylor paid Instagram influencers to post photographs of them wearing the company's clothes without requiring disclosure of the fact that the endorsers were paid. And AmeriFreight offered its customers money for positive endorsements on the Internet without requiring disclosure of that fact. Despite the factual similarity between *Machinima* and *Warner Brothers* as well as the general issue similarity among *Machinima, Warner Brothers, Lord & Taylor,* and *AmeriFreight,* the Commission used the "clearly and prominently" standard in *Machinima* and *AmeriFreight* and "clearly and conspicuously" in *Warner Brothers* and *Lord & Taylor.* Moreover, the Commission's definitions of the two standards shows "clearly and prominently" is not synonymous with "clearly and conspicuously."

Specifically, the Commission's order required Warner Brothers and Lord & Taylor in "clearly and conspicuously" cases to make disclosures "through the same means through which the communication is presented . . . simultaneously."[81] Warner Brothers and Lord & Taylor were also required to consider the impact of its "representation[s] or sales practice[s]" on "children, the elderly, or terminally ill."[82] The Commission's order added, "disclosure[s] must comply with these requirements in each medium through which it is received, including but not limited to all electronic devices and face-to-face communications."[83] Similar to the volume and cadence disclosure requirements of the "clearly and prominently disclose" standard for audible communications, the "clearly and conspicuously disclose" standard also requires audible disclosures to be in the same speed as an audible advertisement.[84] And disclosures for text communications must be of "sufficient" duration and "sufficiently noticeable" under the "clearly and prominently disclose" standard but must also be the same "length of time" and "easily noticed" under the "clearly and conspicuously disclose" standard.[85]

A comparison of *Machinima* and *AmeriFreight* with *Warner Brothers* and *Lord & Taylor* shows how the "clearly and prominently disclose" standard is not synonymous with the "clearly and conspicuously disclose" standard. The two standards are different. The "clearly and prominently disclose" standard is slightly less restrictive because disclosures need not be made simultaneously with the endorsement nor do advertisers need to consider the impact on children, elderly, or the terminally ill. Additionally, the Commission's failure to articulate what would trigger each standard further complicates the matter. When might the Commission accept disclosure under the less restrictive "clearly and prominently"

---

81 *See* Order, *In re Warner Bros. Home Entertainment, Inc.,* FTC File No. 152-3034 (July 11, 2016), https://www.ftc.gov/system/files/documents/cases/160711warnerbrosdo.pdf (last visited Oct. 12, 2016); *See* Order, *In re Lord & Taylor, LLC,* FTC Docket No. C-4576 (May 23, 2016), https://www.ftc.gov/system/files/documents/cases/160523lordtaylordo.pdf (last visited Oct. 12, 2016).

82 *Id.*

83 *Id.*

84 *Id.*

85 *Id.*

standard? And when is the heightened "clearly and conspicuously" standard required? To eliminate this ambiguity, the Commission should publicly abandon the "clearly and prominently disclose" standard and apply only the "clearly and conspicuously disclose" standard because it is more comprehensive. Also, unlike the "clearly and prominently disclose" standard, the "clearly and conspicuously disclose" was also the product of the public comment process before a regulation is promulgated by an administrative agency.

2. Significant Minority

A paid endorsement is deceptive if it does not disclose a material connection and misleads a "significant minority" of the target audience.[86] The Commission considers ten to twenty-two percent of an audience to constitute a "significant minority" for purposes of determining whether an endorsement is deceptive or misleading.[87]As an illustration, a paid endorsement on Instagram by Kim Kardashian-West would need to deceive approximately 8.4 million users for it to satisfy the "significant minority" standard.[88] But a class comprising of 8.4 million deceived individuals is large by any consumer protection statute standard because courts have held 40 injured individuals as sufficient to certify a putative class action.[89]

3. The Commission's Enforcement of Endorsements on Social Media Is Inconsistent or Sporadic

The Commission is authorized to pursue an administrative proceeding or a judicial action under Sections 5(b) or 13(b) of the FTC Act, respectively. A Section 5(b) proceeding is heard before an administrative law judge who issues an "initial decision" that may be appealed before the full Commission, then a federal circuit court, and ultimately before the Supreme Court.[90] Unlike a Section 13(b) judicial opinion, a Section 5(b) order becomes effective 60 days after service. Conversely, the Commission may pursue a civil action directly in federal court under Section 13(b) where the order becomes effective immediately upon issuance.[91]

---

86 *Telebrands,* 140 F.T.C. 278, 291 (2005), *aff'd,* 457 F.3d 354 (4th Cir. 2006)("An ad is misleading if at least a significant minority of reasonable consumers are likely to take way the misleading claim."); *Heinz W. Kirchner,* 63 F.T.C. 1282 (1963)("An interpretation [of an advertisement] may be reasonable even though it is not shared by a majority of consumers in the relevant class, or by particularly sophisticated consumers. A material practice that misleads a significant minority of reasonable consumers is deceptive.").

87 *See, e.g., Firestone Tire & Rubber Co. v. F.T.C.,* 481 F.2d 246, 249 (6th Cir. 1973); *Telebrands,* 140 F.T.C. 278, 325 (2005), *aff'd* 457 F.3d 354 (4th Cir. 2006).

88 Kardashian-West has 83.6 million followers on Instagram. *See* Kim Kardashian-West (@kimkardashian), Instagram, http://instagram.com/kimkardashian (Sept. 27, 2016).

89 The federal numerosity requirement for certification of a class under Rule 23 of the Federal Rules of Civil Procedure is satisfied with as few as 40 persons injured by the defendant's conduct. *Wolkenstein v. Reville,* 539 F. Supp. 87 (2d Cir. N.Y. 1982); *Kreiger v. Gast,* 197 F.R.D. 310 (W.D. Mich. 2000); *Animal Sci. Prods., Inc. v. Hebei Welcome Pharm. Co. (In re Vitamin C Antitrust Litig.),* 279 F.R.D. 90 (E.D. N.Y. 2012).

90 15 U.S.C. § 45(c).

91 *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority,* Federal Trade Commission (Jul. 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Oct. 9, 2016).

The Commission notes, however, "administrative adjudication offers certain advantages over direct judicial enforcement [because] in an adjudicatory proceeding, the Commission has the first opportunity to make factual findings and articulate the relevant legal standard . . . .Thus, where a case involves novel legal issues or fact patterns, the Commission has tended to prefer administrative adjudication."[92] Not surprisingly, the Commission's limited social media endorsement enforcement actions have been through administrative adjudication under Section 5(b).

On August 13, 2015, the Commission published its "Statement of Enforcement Principles Regarding 'Unfair Methods of Competition' Under Section 5 of the FTC Act."[93] In its statement, the Commission enumerated three enforcement principles. First, the Commission will initiate an administrative proceeding if the enforcement action promotes consumer welfare.[94] Second, the endorser's or advertiser's alleged "act or practice . . . must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications."[95] Third, the Commission will avoid Section 5(b) enforcement if enforcement under the Sherman or Clayton Act is sufficient to protect consumer welfare.[96]

In practice, however, the Commission has adopted a laissez-faire attitude toward endorsements on social media. This approach has led to inconsistent and sporadic enforcement actions despite high profile violations. For example, in 2011, Hyundai Motor America launched a pre-Super Bowl promotional campaign in anticipation of the automaker's television advertisements scheduled to air during halftime. Specifically, Hyundai furnished gift certificates to bloggers who included a hyperlink to the promotional videos in their blog posts.[97] Hyundai's terms and conditions for the campaign did not require the bloggers to "clearly and conspicuously" disclose the fact that the bloggers received gift certificates in exchange for including a hyperlink to the promotional videos.[98]

---

92 *Id.*

93 Donald S. Clark, *Statement of Enforcement Principles Regarding 'Unfair Methods of Competition' Under Section 5 of the FTC Act,* Federal Trade Commission (Aug. 13, 2015), https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf (last visited Sept. 25, 2016).

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.*

98 *Id.*

Instead of filing an administrative complaint or commencing a civil action in federal court, the Commission merely sent a letter to Hyundai. The Commission explained, "Hyundai did not know in advance about use of these incentives, that a relatively small number of bloggers received the gift certificates, and that some of them did in fact, disclose this information."[99] The Commission added, "the actions with which we are most concerned here were taken not by Hyundai employees, but by an individual who was working for a third-party media firm hired to conduct the blogging campaign."[100] But this fact is not different from *Machinima, Warner Brothers,* or *Lord & Taylor.* Microsoft hired Machinima and Warner Brothers and Lord & Taylor hired third-party social media influencers. This inconsistency is further muddled by the fact that the Commission's decision was based on non-public information.

Similarly, although TINA.org put a spotlight on the Kardashian women, 13.3 million people viewed Spears' endorsement of EOS, 25.1 million people viewed James' endorsement of Blaze Pizza, Timberlake's tequila photo was viewed by almost 36 million people, and approximately 100 million Instagram users viewed Gomez's dressing room photograph.[101] Neither Spears, James, Timberlake, nor Gomez has been the subject of a private or public inquiry or enforcement action. Ultimately, the lack of enforcement actions—whether administrative or judicial—by the Commission demonstrating the application of existing regulations to real-world facts results in greater opacity not clarity.

4. Hashtags Are Not Clear and Conspicuous Disclosures Because They Are Not Always in Sufficiently Close Proximity to the Commercial Endorsement and Can Be Co-opted for Non-advertisement Purposes

On some social media websites like YouTube, the hashtag is not in sufficiently close proximity to the endorser's video content. A hashtag disclosure on YouTube can only be made in the description section below the video unless the content creator or YouTube superimposes the hashtag—in which case any disclaimer, not just a hashtag could be made—to the video. Similarly, a text hashtag on Instagram would not satisfy the proximity requirement for a "clear and conspicuous" disclosure because the disclosure should be made in the same medium as the endorsement; photographic endorsements should include disclosures in the photographs themselves (*e.g.,* superimposed text on the photographic endorsement). Text endorsements on Facebook and Twitter face the problem of hashtag cooption.

Hashtags are limited to labeling and organizing information on a social media website. More important, hashtags can be used by anyone for both commercial and non-commercial speech. As a result, hashtags can be intentionally coopted for political or satirical purposes or unintentionally coopted by social media users who use it outside of the United States where "#ad" has a different connotation than advertisement. Similarly, a hashtag disclosure could be used to categorize posts that are commenting on a particular social media endorsement.

---

99 *Id.*

100 *Id.*

101 These numbers are accurate as of September 27, 2016.

For instance, a search for the hashtag "#ad" on Twitter reveals both commercial and non-commercial posts. Search results include both actual advertisement tweets as well as non-advertisement tweets that refer or relate to advertising generally. For example, *Ad Age* magazine's official Twitter feed ranks high on the results for the hashtag "#ad."[102] It also includes the verified Twitter feed of popular blogger Anaggh Desai.[103] Similarly, the Twitter account for United Parcel Services ("UPS") logo and "#ups" and "#ad" hashtags could be subversively parodied to "United Pot Smokers" and "#ups" and "#ad", satirically advertising and promoting marijuana instead of the freight delivery services of UPS.

5. The Commission Does Not Recommend Specific Words or Combination of Words That Are Sufficiently "Clear and Conspicuous"

Unlike the NPA and the Radio Act of 1927, the FTC Act nor the regulations, guidance documents, or enforcement orders from the Commission recommend a specific word or set of words to satisfy the "clearly and conspicuously" or "clearly and prominently" disclosure standards. Indeed, the Commission has expressly avoided fixing the words or combination of words that would sufficiently disclose a material connection between an endorser and advertiser. The Commission explained:

> The FTC isn't mandating the specific wording of disclosures. However, the same general principle—that people get the information they need to evaluate sponsored statements—applies across the board, regardless of the advertising medium. The words "Sponsored" and "Promotion" use only 9 characters. "Paid ad" only uses 7 characters. Starting a tweet with "Ad:" or "#ad"—which takes only 3 characters—would likely be effective.[104]

But the Commission's reluctance to prescribe a set of descriptive words leaves advertisers guessing as to what will constitute a "clear and conspicuous" or "clear and prominent" disclosure. Social media companies like Facebook and Twitter are also left in the dark as to what specifically they could do—from a terms of use and technology perspective—to ensure compliance with the FTC Act's disclosure requirements.

B. Proposed Solutions

1. Best Practices for Celebrity Endorsements on Social Media

Based on *Machinima, Warner Brothers, Lord & Taylor,* and *AmeriFreight,* an advertiser should follow the three "M's" referring to (1) mandating endorsers to comply with the disclosure requirements of Section 5; (2) make sure endorsers are aware of the Section 5 disclosure rules; and (3) monitor all endorsements. Any endorser that fails to strictly comply with disclosure rules should be terminated.

---

102 Ad Age Magazine (@adage), Twitter, https://twitter.com/adage (last visited Oct. 9, 2016).

103 Anaggh Desai (@anaggh), Twitter, https://twitter.com/anaggh (last visited Oct. 9, 2016).

104 *See supra* note 47.

2. The Commission Should Eliminate the "Clearly and Prominently" Standard in Favor of "Clearly and Conspicuously"

The Commission should discontinue the use of the "clearly and prominently" disclosure standard used in *Machinima* and *AmeriFreight*. The "clearly and conspicuously disclose" standard is more comprehensive than the "clearly and prominently disclose" standard and has been promulgated in the Code of Federal Register after comment from industry. The Commission should publicly state that the "clearly and prominently disclose" standard is being abandoned and that "clearly and conspicuously disclose" will only be used in its enforcement actions for purposes of uniformity of compliance and enforcement. Adopting a single standard will result in greater clarity for industry and the Commission. In particular, celebrity endorsers and advertisers will know, with greater certainty, the standard that the Commission will apply to a given factual circumstance instead of wondering whether the more relaxed "clearly and prominently disclose" standard will be applied.

3. The Commission Should Replace "Significant Minority" with "Sufficient Minority" by Requiring Fewer People to Be Affected by Unlawful Conduct

Celebrity social media accounts disseminate non-commercial and commercial content to millions of viewers at the click of a button. Selena Gomez recently broke records by acquiring more than 100 million followers.[105] Since the Commission previously defined "significant minority" as anywhere from ten to twenty-two percent of an audience, potentially 10 million to 22 million of Gomez's followers need to be deceived to satisfy the standard.[106] In the world of celebrity social media, ten to twenty-two percent of an audience is too broad. Thus, the Commission should use the minimum number of plaintiffs required to certify a class action as the basis for whether a "*sufficient* minority"—not *"significant* minority"—has been deceived. Courts have widely held that forty injured individuals are sufficient to certify a class.[107] Accordingly, an objective standard of forty individuals should constitute a "sufficient minority." By doing so, the Commission will effectively grant millions of social media users a potential administrative remedy that they otherwise would not have had because too few people were deceived or misled.

---

105 Gil Kaufman, *Selena Gomez First To Reach 100 Million Instagram Followers,* Billboard Magazine (Sept. 27, 2016), http://www.billboard.com/articles/columns/pop/7525497/selena-gomez-first-to-reach-100-million-instagram-followers (last visited Sept. 28, 2016).

106 *See, e.g., Firestone Tire,* 481 F.2d 249*; Telebrands,* 140 F.T.C. 278, 325 (2005), *aff'd* 457 F.3d 354 (4th Cir. 2006).

107 *See Wolkenstein v. Reville,* 539 F. Supp. 87 (2d Cir. N.Y. 1982); *Kreiger v. Gast*, 197 F.R.D. 310 (W.D. Mich. 2000); *Animal Sci. Prods., Inc. v. Hebei Welcome Pharm. Co. (In re Vitamin C Antitrust Litig.*), 279 F.R.D. 90 (E.D. N.Y. 2012).

4. The Commission Should Enforce the FTC Act Disclosure Requirements Against Celebrity Endorsers, Advertisers, and Social Media Companies Uniformly

The Commission should adopt a policy requiring disclosure of all material facts in an administrative enforcement action—even in cases where no enforcement action was actually taken—so that industry understands what the Commission considers violative and not violative.

5. The Commission Should Prohibit the Use of Hashtag Disclosures and Require Social Media Companies to Identify and Publish Advertisements Differently Than Non-advertisement Posts

The Commission should eliminate any doubt as to the sufficiency of hashtag disclosures and publicly state that hashtags are not "clear and conspicuous" disclosures. Instead, the Commission should publicly state that social media companies should explore technology solutions to identify advertisement content from non-advertisement content and publish advertisement content differently than non-advertisement content. For example, Facebook, Instagram, and Twitter all use "verified" accounts for public personalities as identity theft safeguards.[108] Google's software scans Gmail users' e-mails to display salient advertisements.[109] YouTube scans the user-uploaded videos to prevent copyright infringement. Reddit publishes promoted commercial posts using a different background color from non-commercial posts.[110] And Facebook charges advertisers to insert posts into a user's feed.[111] These examples illustrate social media companies' ability and willingness to deploy technology solutions to legal and regulatory problems.

Similar to these established methods of monitoring their content, social media companies should scan the content of verified celebrity posts for keyword or image triggers suggestive of an endorsement. If commercial speech is identified, the social media company should affirmatively require the verified celebrity poster to disclose the material connection by identifying the advertiser. The commercial post should be displayed differently than non-commercial posts; the font and background color should be different by default so that viewers are on notice of the commercial character of the post.

Further, like the way traditional media charges for print display advertising and radio and television charge for airtime, social media companies should charge celebrity endorsers to post commercial content on their platforms. By aligning the financial incentives of social media companies with the FTC Act's clear and conspicuous disclosure

---

108 *See Verified Page or Profile,* Facebook (Sept. 28, 2016), https://www.facebook.com/help/196050490547892; *Verified Badges,* Instagram (Sept. 28, 2016), https://help.instagram.com/854227311295302; *About Verified Accounts,* Twitter (Sept. 28, 2016), https://support.twitter.com/articles/119135.

109 *How Gmail Ads Work,* Google (Sept. 28, 2016), https://support.google.com/mail/answer/6603?hl=en.

110 *Sponsored Headline Tests: Placement and Design,* Reddit (June 23, 2016), https://www.reddit.com/r/announcements/comments/4phzsi/sponsored_headline_tests_placement_and_design/ (last visited Sept. 30, 2016).

111 *Facebook Ad Basics,* Facebook (Sept. 30, 2016) https://www.facebook.com/business/learn/facebook-ads-basics.

requirements, the Commission will have an editorial/compliance filter for the social media world just as it does in traditional media. The result would be a greater likelihood of self-regulation and compliance with the FTC Act.

6. The Commission Should Propose a Specific Word or Combination of Words to Connote an Advertisement

Finally, the Commission should require all advertisement content on social media to not only be published differently than non-advertisement content, but also be clearly disclaimed as "ADVERTISEMENT" like the NPA and Radio Act of 1927.

IV. CONCLUSION

The Commission's modus operandi of permitting advertisers to self-regulate is inappropriate with the fast changing social media landscape. The Commission's preference for administrative enforcement in social media cases illustrates the fact that social media is a changing landscape that requires some regulatory intervention. But the Commission's intervention has been insufficient. The need for "clear and conspicuous" disclosures between celebrity endorsers and advertisers is greater than ever. The Commission should abandon the "clearly and prominently disclose" standard for the "clear and conspicuous standard", replace the "significant minority" threshold with "sufficient minority," and publicly state that hashtags are not clear nor conspicuous disclosures in social media posts. Each of these recommendations will result in greater clarity for industry and should ultimately lead to greater compliance with the FTC Act.

THE ANTITRUST, UCL AND PRIVACY SECTION

The Antitrust, UCL and Privacy Section was established by the State Bar of California in 1981 for the purpose of furthering the knowledge of its members in federal and state antitrust, unfair competition, and privacy law. The focus of the Section is on litigation, counseling and government contracts.

The Section is governed by an Executive Committee appointed by the Board of Governors of the State Bar of California.

SECTION MEMBERSHIP

There are no prerequisites to membership. All interested attorneys, judges, non-attorneys, paralegals, law students and out-of-state attorneys are invited to enroll in the Section. New Bar admittees can be enrolled free for the first year upon written request to the Section.

STANDING COMMITTEES

The Section has the following standing committees in which the Section members are urged to participate:

- Education/Programs
- Publications/Journal
- Outreach/Diversity

JOURNAL

The Section publishes Competition, a periodic journal. Members who wish to author articles or assist with publications are encouraged to contact the Editor.

PROGRAMS

The Section presents an annual MCLE-accredited institute, and Antitrust Lawyer of the Year Award, as well as programs at the Section Education Institute and the State Bar of California Annual Meeting.

MEMBERSHIP BENEFITS

- Free annual subscription to the Section's journal, Competition to keep members current on issues and developments.
- Discount on all Antitrust, UCL and Privacy Section programs.
- Discount on the California Antitrust and Unfair Competition Law treatise.
- Discounts on any Section publications.
- Opportunity to participate in Section and Committee activities.
- Opportunity to meet other members of the Antitrust, UCL and Privacy Section.

ENROLL NOW AND START RECEIVING YOUR MEMBERSHIP BENEFITS!

ANTITRUST, UCL AND PRIVACY SECTION ENROLLMENT FORM

You can join the Antitrust, UCL and Privacy Section ONLINE by visiting:
www.calbar.org/join-a-section

Or, if paying by check or joining as a Judge, a Non-Attorney, or a Non-Attorney Law Student, please use the form below.

Please enroll me as a member or associate member of the
Antitrust, UCL and Privacy Section of the State Bar of California

Name: _____ State Bar Number:_____

Firm: _____

Address: _____

City, State, Zip: _____

Telephone: _____ Fax: _____

E-mail: _____

SECTION ENROLLMENT FAX/MAIL FORM:

☐ Attorney (Members) and Non-Attorneys (Associate Members)	$75
☐ Judges (Associate Membership)	FREE (Join Form ONLY)
☐ Non-Attorney Law Student	FREE (Join Form ONLY)

(Up to 3 Complimentary Sections for Non-Attorney Law Students)

Enclose your check, payable to The State Bar of California and mail to:
Section Enrollments; State Bar of California; 180 Howard Street; San Francisco, CA 94105-1639

If paying by credit card, you may mail this form to the above address or fax to:
Section Enrollments at 415.538.2368

CREDIT CARD INFORMATION (mandatory if faxing registration)
I authorize The State Bar of California to charge my program registration and/or fees as noted above to my VISA or Mastercard account. **(No other cards will be accepted)**

Account number:_____ Expiration Date: _____

Cardholder's Name: _____ Cardholder's Signature: _____

For further information, please contact the Antitrust, UCL and Privacy Section at 415.538.2554, or visit our website at www.calbar.org/antitrust

The State Bar of California
Antitrust, UCL and Privacy Section
180 Howard Street
San Francisco, CA 94105-1639