PRIVACY COMMITMENTS

Rachel Wilka*

Abstract: What responsibilities do corporations have with regard to their consumers' information? Many articles have looked at ways to make personal information the "property" of the consumer. Property approaches attempt to overlay personal information on the legal frameworks of trade secret, trademark, and copyright law. While each approach has its merits, and contributes to the field, none of the proposals generate a concrete way for a consumer to enforce his or her rights against a company. The proposals all suffer from the same fatal flaw, a new system must not just create a consumer right but also balance the inequities in bargaining power between a consumer and a large corporation.

In patent law, there are similar conflicts of interest between a private property owner's (patent holder's) right to create a successful business and the ability of others (potential patent licensees) to negotiate a reasonable royalty rate. In response to this conflict, the patent field relies upon a self-regulatory system where patent holders agree to be "Reasonable and Non-Discriminatory" in their licensing practices. This system produces two concrete benefits. First, it helps correct the power imbalance between two negotiating parties. Second, it creates a third-party breach of contract right for a party who could not normally bring a case. As a process, a patent holder agrees to Reasonable and Non-Discriminatory practices ("RAND") with a standards-setting organization. Then, if the patent holder does not reasonably license their patent to a third party who wishes to negotiate for said license, the third party can sue the patent holder, even though the two parties never finalized an agreement.

This paper argues a similar system would lend much-needed structure to online data use. Creating a voluntary, quasi-self-regulatory regime would allow greater transparency as to corporate data practices, facilitate the creation of industry standards as to "reasonable" data use, balance the interests of corporation and consumer, and create a legal right for consumers who have had their personal data misused (in a way that could more easily support a class-action). The paper proceeds in four parts. The first part looks at current norms of data use and the issues a proposed system would need to address. The second part reviews and summarizes past intellectual property approaches to privacy, as well as each approach's respective drawbacks. The third part examines RAND commitments and their operation in the realm of patent law. The fourth part discusses a system for implementing RAND commitments in privacy law, and addresses potential benefits and drawbacks of the approach.

---

* Rachel Wilka holds degrees in law from University of Washington and Finance and Management Information Systems from University of Arizona. She is currently corporate counsel at Zillow Group, Inc. The author's views are her own and offered in her personal capacity; they do not reflect the views of Zillow Group or any other organization. The author would like to thank Professor Ryan Calo for his advice and encouragement throughout the writing process.

INTRODUCTION

Current privacy laws chase technological advances, and seem perennially unable to provide consumers effective ways to protect their privacy interests.[1] The insufficiencies in privacy law are not a simple outcome of a dearth of statute or regulation.[2] Specific laws may protect privacy in specific contexts, but lawmakers continually create legal requirements with similar flaws: (1) application to a limited demographic; (2) overly vague or easily avoided definitions of "violation of privacy"; (3) protection of limited types of "personally identifiable information" (PII); and/or (4) avoidance of meaningful requirements through overly generous safe harbors.[3]

A. Consumers Need to Know How Their Data Is Being Used

In any discussion of privacy practices, the biggest hurdle to achieving better, privacy-respecting, data use practices and regulation is getting the technology sector to care about, and invest in, privacy.[4] Without corporate buy-in, privacy practices will continue to rely on outdated privacy laws and enforcement by overworked government agencies. The best way to motivate "big-tech" is to empower and mobilize consumers to pressure the private sector into creating meaningful protections. To do

1. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1146 (2002).

2. *Id.* at 1090.

3. *Id.* at 1088–89 (discussing the problems with the definition of privacy described); Andrew Chin & Anne Klinefelter, *Differential Privacy as a Response to the Reidentification Threat: The Facebook Advertiser Case Study*, 90 N.C. L. REV. 1418, 1426 n.37 (2012) ("noting that the FTC's proposals are 'supported by a wide cross section of roundtable participants who stated that the traditional distinction between PII and non-PII continues to lose significance due to changes in technology and the ability to re-identify consumers from supposedly anonymous data'" (quoting FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 43 (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [https://perma.cc/HYZ4-EEND])).

4. Joseph Turow, *Google Still Doesn't Care About Your Privacy*, FORTUNE (June 28, 2017), http://fortune.com/2017/06/28/gmail-google-account-ads-privacy-concerns-home-settings-policy/ [https://perma.cc/U88P-NBUP].

so, consumers must first understand what they are fighting for—in other words, why privacy matters.

Until recently, consumers were apathetic to digital privacy practices.[5] They did not read companies' privacy policies[6] or see big data affecting their analog lives. As Donald Rumsfeld phrased it, "As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know."[7] Until recently, the average digital consumer only knew about the "known-knowns" of data use, like Facebook using his or her data to personalize shoe advertisements. The average consumer viewed corporate data use as innocuous and ignorable. As a result, companies saw no need to invest in privacy protections on the consumers' behalf.

The landscape has now changed. The "unknowns" have emerged. Data breaches expose credit card information,[8] medical histories and prescription lists,[9] financial holdings and home addresses,[10] and personal e-mails.[11] Over the course of 2014, 47% of U.S. adults, or 110 million

5. Greg Satell, *Let's Face It, We Don't Really Care About Privacy*, FORBES (Dec. 1, 2014, 12:38 AM), https://www.forbes.com/sites/gregsatell/2014/12/01/lets-face-it-we-dont-really-care-about-privacy/#53ea22825698 [https://perma.cc/P297-YXYZ]; Hayley Tsukayama, *People Care More About Convenience than Privacy Online*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/10/07/people-care-more-about-convenience-than-privacy-online/?utm_term=.a889c2c591a6 [https://perma.cc/AWB9-V5FV].

6. Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RESEARCH CTR.: FACT TANK (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ [https://perma.cc/2GBZ-4GPB].

7. David A. Graham, *Rumsfeld's Knowns and Unknowns: The Intellectual History of a Quip*, ATLANTIC (Mar. 27, 2014), http://www.theatlantic.com/politics/archive/2014/03/rumsfelds-knowns-and-unknowns-the-intellectual-history-of-a-quip/359719/ [https://perma.cc/WH9H-XBQ6].

8. Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY, (May 6, 2014 12:24 AM), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/ [https://perma.cc/C75X-BLFF].

9. Coral Garnick, *Premera Negligent in Data Breach, 5 Lawsuits Claim*, SEATTLE TIMES (Mar. 27, 2015), http://www.seattletimes.com/seattle-news/premera-negligent-in-data-breach-5-lawsuits-claim/ [https://perma.cc/B6HY-9TPW]; Shannon Pettypiece, *Sony Hack Reveals Health Details on Employees, Children*, BLOOMBERG BUSINESSWEEK (Dec. 11, 2014), http://www.bloomberg.com/news/articles/2014-12-11/sony-hack-reveals-health-details-on-employees-and-their-children (last visited June 11, 2018).

10. Jessica Silver-Greenberg, Matthew Goldstein, & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES: DEAL BOOK (Oct. 2, 2014, 12:50 PM), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/ [https://perma.cc/JE8Y-9SG9].

11. Elizabeth Weise, *Hijackers Get up Close and Personal with Hacked Accounts*, USA TODAY (Nov. 6, 2014, 10:08 AM), http://www.usatoday.com/story/tech/2014/11/06/email-hijacking-phishing-google/18564671/ [https://perma.cc/SN3Y-L6DF].

individuals, had their personal data stolen.[12] By 2017, approximately the same proportion of Americans were affected by the Equifax hack alone.[13] Outside of data breaches, companies argue that data distributed to partners is anonymized, but in the Human Genome Project, a respected medical study, between 84–97% of participants could be re-identified (i.e., their names could be connected to their individual "anonymized" data).[14]

Unless users gain insight into how their data is being used, and where it is going, they cannot make an informed choice as to which companies can access their data. Moreover, because companies may share data with other parties without the user's knowledge, the user's choice of which services to use may be moot. The data could be transmitted to companies the user consciously chose to avoid by the services he or she *is* choosing to use. As big data starts affecting our non-digital lives, respect for privacy, and responsible data use more broadly, becomes increasingly important. Consumer data analytics, based on collective user data, impacts every aspect of our lives including not only areas like marketing, but also our career,[15] credit score,[16] and exposure to targeted, deceptive information.[17] The era of privacy as a theoretical concern is over; big data is here to affect our lives. It is either control, or be controlled by, big data.

B. Big Data Negatively Affects the Offline World

Big data uses affect our non-digital lives in countless ways every day. Big data may affect the job-interview process to judge whether an applicant has the right "culture fit" with a company,[18] what college a high

12. Jose Pagliery, *Half of American Adults Hacked This Year*, CNNMONEY (May 28, 2014), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/ [https://perma.cc/NN6F-7FUF].

13. Ryan Grenoble, *2017 Was the Year of Hacks. 2018 Probably Won't Be Better*, HUFFPOST (Dec. 30, 2017, 7:00 AM), https://www.huffingtonpost.com/entry/data-breach-hacks_us_5a3a7f56e4b025f99e13cdbe [https://perma.cc/L9BG-LVM4].

14. LATANYA SWEENEY, AKUA ABU & JULIA WINN, HARVARD UNIV. DATA PRIVACY LAB, IDENTIFYING PARTICIPANTS IN THE PERSONAL GENOME PROJECT BY NAME 3 (2013).

15. Tim Adams, *Job Hunting Is a Matter of Big Data, Not How You Perform*, GUARDIAN: THE OBSERVER (May 10, 2014, 4:00 AM), https://www.theguardian.com/technology/2014/may/10/job-hunting-big-data-interview-algorithms-employees [https://perma.cc/JL3A-YWPZ].

16. Mikella Hurley & Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 YALE J.L. & TECH. 148, 150–51 (2016).

17. Claire Cain Miller, *When Algorithms Discriminate*, N.Y. TIMES: THE UPSHOT (July 9, 2015), https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html [https://perma.cc/8C8C-TAW7].

18. *About*, ARTISIAN FOR HIRE, INC., https://artisantalent.com/about-artisan/ [https://perma.cc/83ZF-EXRJ]; *cf.* Lydia Dishman, *How Big Data Might Change the Way You Find*

school student gets into,[19] and potentially even consumer credit scores.[20] Companies will argue that online services utilizing personal information have the ability to help consumers more than hurt them. Big data is touted as the solution to discrimination,[21] bad bosses,[22] and inaccurate or incomplete profiles with credit agencies.[23]

However, even if big data could deliver on those promises from a technical or theoretical standpoint, its benefit to consumers depends on the truthfulness of the data. In other words, an individual's ability to get a job or a mortgage can depend on the data stored by online companies and can conversely be negatively impacted by inaccurate information. In reality, data collected through normal avenues "only represents a thin slice of us" and 30–50% of collected online data is inaccurate.[24] The problem is so large that the tech industry is already investing millions to try to solve it themselves.[25] So far, industry attempts to control for quality have not demonstrated viability.

The power of online companies compared to their consumers means users currently cannot control how data is used or how it will affect their lives. To begin taking control of data, users must first understand where data is going and who is using it.

C. It Is Not Clear Where Companies Are Sending Data

The difficulty of knowing how personal data is used goes beyond the lack of company transparency with its users—many companies currently

---

a Job, FAST COMPANY (Oct. 23, 2015), https://www.fastcompany.com/3052639/how-big-data-might-change-the-way-you-find-a-job [https://perma.cc/6GH2-XK6S] (discussing job seekers' use of big data to gain insight into the culture of potential employers).

19. Darian Somers, *Do Colleges Look at Your Social Media Accounts?*, U.S. NEWS (Feb. 10, 2017, 8:00 AM), https://www.usnews.com/education/best-colleges/articles/2017-02-10/colleges-really-are-looking-at-your-social-media-accounts (last visited June 3, 2018).

20. Colin Wilhelm, *Big Data vs. the Credit Gap*, POLITICO: THE AGENDA (Feb. 7, 2018, 5:02 AM), https://www.politico.com/agenda/story/2018/02/07/big-data-credit-gap-000630 [https://perma.cc/6KBC-NF9B].

21. MARTIN WATTENBERG, FERNANDA VIÉGAS & MORITZ HARDT, ATTACKING DISCRIMINATION WITH SMARTER MACHINE LEARNING,

https://research.google.com/bigpicture/attacking-discrimination-in-ml/ [https://perma.cc/6QWH-RPB5].

22. Dishman, *supra* note 18.

23. Wilhelm, *supra* note 20.

24. Julian Mitchell, *This Data Mining Startup Empowers Consumers to Own Their Digital Footprint*, FORBES (Jan. 25, 2017, 4:25 PM),

https://www.forbes.com/sites/julianmitchell/2017/01/25/this-data-mining-startup-gives-consumers-the-tools-to-own-their-digital-footprint/#554eb0f918db [https://perma.cc/QLS3-37KA].

25. *Id.*

do not track, or do not understand, the full scope of how their collected data is being used. As discussed in the previous section, one of the major issues with tracking data use is accounting for data breaches. Over the past several years, large-scale data breaches have become ubiquitous.[26] Equifax is the most recent and obvious example.[27] Equifax previously existed as a shining example of both individuals and government putting trust in keeping their most sensitive data secure through the private sector.[28] We now have no way of knowing where our full financial histories may be, and our only protection is monitoring after the fact to avoid direct financial repercussions. The underlying privacy is gone.[29]

In addition to the nefarious data breach scenario, there are new technology advancements changing how we must think about data use. New technologies, including machine learning and artificial intelligence, ingest large amounts of data, but may save only data useful to the underlying algorithm(s) or only store the knowledge learned from the data set (i.e., a derivative predictive value).[30] The data has a transformative effect on the technology, blurring the line between personal data and company innovation.

Therefore, understanding company data use is dependent on companies reliably tracking data use, which is far from universal. The illusion of comprehensive data tracking shattered recently with Facebook's admission that it allowed political targeting organizations to access millions of Facebook user profiles in violation of its own policies.[31] While Facebook clearly mishandled data, its practices are sophisticated compared to the average startup's blind use of data.[32] A real solution to current lackluster privacy practices will need to not only solve the privacy concerns of today; it will have to be scalable,

---

26. Press Release, Identity Theft Res. Ctr., At Mid-Year, U.S. Data Breaches Increase at Record Pace (July 18, 2017), https://www.idtheftcenter.org/Press-Releases/2017-mid-year-data-breach-report-press-release [https://perma.cc/9HPQ-PFAA].

27. Donna Borak & Kathryn Vasel, *The Equifax Hack Could Be Worse than We Thought*, CNNMONEY (Feb. 10, 2018, 10:43 AM), http://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html [https://perma.cc/LDB8-2GZ8].

28. *Id.*

29. *Id.*

30. David Rubinstein, *Where Does Big Data Go From Here?*, SD TIMES (Jan. 4, 2018), https://sdtimes.com/data/big-data-go/ [https://perma.cc/76CM-GQNP].

31. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018),

https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?action=click&module=Intentional&pgtype=Article (last visited June 3, 2018).

32. *See* Ronald A. Klain, *Proof Startups Can't Afford to Ignore the Law*, FORTUNE (Mar. 2, 2016), http://fortune.com/2016/03/02/startups-ignore-law/ [https://perma.cc/7Q7V-52DJ].

adaptable, and understandable in order to avoid being outpaced by technology or ignored by industry.

D. Scholars Have Proposed Protecting Private Data as Intellectual Property

Knowing the full risk of online data use, leading academics have proposed solving the privacy problem through intellectual property (IP) law frameworks, attempting to create a type of intangible property right in one's personal data.[33] The idea behind most of the approaches is if users have an ownership interest in their data, then use without compensation, or at least consent, would empower them by providing a cause of action. Previous published works considered potential systems based on trade secret, trademark, and copyright law.[34] Prior IP approaches generally have not met with a great deal of success.[35] Trademark, trade secret, and copyright law just do not provide a practical solution to protecting privacy rights.[36]

However, there is a very promising unexplored avenue of IP law: patent law. At first glance, the omission of a patent approach to privacy protection makes sense. Personal information is not an "invention" and even personal browsing data may not be "novel."[37] Despite the initial reaction that privacy law and patent law are completely incompatible fields, however, there is a common problem in both fields: how do you both respect the free market's ability to contract for use rights and prevent extremely lopsided contracts resulting from unequal bargaining power?

In patent law, this problem manifests as a Standard Essential Patent (SEP), where a piece of patented technology, generally a piece of software or hardware, is so integral to the industry that its use is required for anyone creating new technology in the space.[38] This presents a dilemma: the company holding an SEP has a legitimate right to receive license revenue from the use of the invention, but the potential licensee does not have a meaningful alternative technology to use.[39] The patent

33. *See infra* Part I.

34. *See infra* Part I.

35. *See infra* section I.A.2; section I.B.2; section I.C.2.

36. *See infra* section I.A.2; section I.B.4; section I.C.6.

37. 35 U.S.C. § 101 (2018).

38. Jeffrey C. Johnson, *Standard Essential Patents—The Transactional Side*, 86 BNA INSIGHTS 202, 202 (May 24, 2013).

39. *Id.*

holder is able to demand outrageous licensing fees, especially from current or potential competitors, which stifles the development of new inventions and competition for market share.[40] A similar problem exists in privacy protection for two reasons: (1) just a handful of companies completely dominate categories of online services[41]; and (2) choice of service provider is often outside of the consumer's control, as in the case of employers selecting a provider for employees. In the privacy context, however, market-dominant companies, instead of using their bargaining power to obtain exorbitant licensing fees, "obtain control" of users' data.[42] Users have to agree to a click-through, essentially waiving their right to challenge the company's use of their data, similar to a potential licensee who could be forced to pay outlandish royalties for a patent.[43]

For patents, the SEP conundrum led to a specific policy response: the creation of Reasonable and Non-Discriminatory (RAND) commitments.[44] In basic terms, RAND commitments are a voluntary obligation by a company to license its patented technology only under reasonable and non-discriminatory licensing terms.[45] The commitment creates a third-party cause of action against SEP holders who refuse to offer potential licensees a reasonable and non-discriminatory license.[46]

In the privacy context, a similar schema could speak to issues arising from a similar imbalance in negotiating power. However, to fully correct the problem, any IP approach would need to accomplish several goals. First, it would need to mandate accountability as to data use and sharing in order for the public to fully understand current practices. Second, it would have to address the inequities in bargaining power between an individual user and data-collecting companies. Third, it would need to represent a viable avenue for the companies themselves (i.e., not be seen as overly burdensome or incompatible with an industry's ability to monetize). Fourth, the model must include both government regulation and industry self-regulating aspects, in order to allow for flexibility of industry norms combined with the penalties of government regulation

40. *Id.*

41. *See, e.g.*, Jeff Desjardins, *This Chart Reveals Google's True Dominance over the Web*, VISUAL CAPITALIST (Apr. 20, 2018, 12:48 PM), http://www.visualcapitalist.com/this-chart-reveals-googles-true-dominance-over-the-web/ [https://perma.cc/RG5N-MWSY].

42. *Id.*

43. Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. CHI. LEGAL F. 69, 71.

44. *See infra* Section II discussion of RAND commitments.

45. *See infra* Section II discussion of RAND commitments.

46. *See infra* Section II discussion of RAND commitments.

for incentivizing compliance. Finally, it needs to provide a realistic and approachable remedy accessible to the public, either through the creation (or appointment) of a regulating body or by providing clear and real incentives for private rights of actions.

This paper argues a RAND system in the privacy law context could accomplish the above objectives. The paper proceeds by discussing: (1) previously proposed IP approaches and their shortcomings; (2) RAND commitments, both what they are and how they work in the patent law context; and (3) how RAND Commitments could apply in the privacy law field.

I. PREVIOUSLY PROPOSED IP APPROACHES TO PRIVACY

Scholars and policymakers have sought to address the problem of overbroad data use (i.e., lack of respect for privacy) in a number of ways. Some highly visible scholars suggest applying IP law concepts to the privacy context using different models. Generally, IP approaches to privacy have analogized privacy rights to three different categories of intellectual property: (A) copyright law; (B) trade secret law; and (C) trademark law.

A. Copyright

1. Copyright Approach to Privacy Law

The constitutional purpose of copyright law is "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[47] The Copyright Act of 1976 grants protection to a wide range of "creative or artistic works, including 'literary works, musical works (including lyrics), dramatic works (including accompanying music), pantomimes and choreographic works, pictorial, graphic and sculptural works, motion pictures and other audiovisual works, sound recordings, and architectural works.'"[48]

Jonathan Zittrain discusses copyright law in the privacy context in his article, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*.[49] In the discussion,

47. U.S. CONST., art. I, § 8, cl. 8.

48. Emily S. Day, *Double-Edged Scissor: Legal Protection for Fashion Design*, 86 N.C. L. REV. 237, 245 (2007).

49. Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privacation*, 52 STAN. L. REV. 1201 (2000).

Zittrain looks at some of the common problems faced by those who have had their copyrights violated and those who have had their privacy rights violated.[50] In both contexts, the internet enabled problematic behavior by creating increased accessibility and the ability to "copy" material created by the owner, whether an artist's song or a user's browsing history.[51] Additionally, in both contexts, "monetization" of the "owned" work benefits a third party without providing any benefit to the creator.[52] In the context of music copyright, a torrent site monetizes the work through advertisements.[53] In the privacy realm, a company monetizes users' data, either directly through targeted advertisements, or through an ad hoc approach of selling a customer "profile" to an outside organization.[54]

Zittrain's argument focuses on a "well-designed and trusted" system to protect privacy rights, and notably includes a discussion of "prevention versus punishment" mechanisms.[55] Zittrain points out that in both copyright and privacy contexts, punishment can be an incomplete remedy to the owner.[56] In the music industry, for example, it is has been difficult for copyright owners to track all the "pirates" of their copyrighted material.[57] Generally, a copyright holder is, practically, unable to obtain statutory damages from most copyright infringers, even when using Digital Millennium Copyright Act (DMCA) enforcement mechanisms.[58] In the privacy context, it is similarly difficult for individuals to track all uses of their private information by companies like Facebook, Google, and/or their associates.[59] Obtaining non-trivial

50. *See generally id.*

51. *Id.* at 1201("Both law and technology influence such balancing, making it more or less palatable to use data for particular purposes—whether one is an individual making a copy of a popular song for a friend, or a hospital selling a list of maternity ward patients to a day care service.").

52. Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN (Aug. 23, 2012, 3:52 PM), https://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html [https://perma.cc/XXJ3-ZEQW].

53. *How Do BitTorrent Sites like the Pirate Bay Make Money?*, INVESTOPEDIA, https://www.investopedia.com/ask/answers/052815/how-do-bittorrent-sites-pirate-bay-make-money.asp [https://perma.cc/6R97-ZDZN].

54. Zittrain, *supra* note 49, at 1229 (citing Stacy Collett, *Standard in Works for Sharing E-Customer Data: Ability to Easily Share Information Alarms Privacy Experts, Despite Planned Guidelines*, COMPUTERWORLD, Nov. 22, 1999, at 2).

55. *See id.* at 1222 (specifically Section C. "Prevention Rather than Punishment of Undesired Behavior").

56. *Id.*

57. *Id.*

58. *See id.*at 1248. The DMCA allows copyright holders to submit "takedown requests" to any platform or person reproducing their work without permission.

59. *Id.* at 1233.

remedies from companies violating user privacy has proven nearly impossible.[60]

To create a "trusted" system in the copyright arena, the industry used technological advancements, such as file encryption and tracking. There were also systematic legal changes, including the availability of DMCA take-down requests and negotiation of license rights with outside companies to stream music and movies (e.g., Pandora or Netflix). These two developments curbed the scope of unlicensed use of copyrighted material by end users.[61]

2. Potential Problems with a Copyright Approach

Zittrain's approach was met by several critiques. Zittrain's article focuses on implementing copyright frameworks in a limited sphere of privacy law—namely, medical patient privacy.[62] In that narrow context, the "well-designed and trusted" system approach might lead to meaningful improvements. The medical industry has unique statutory privacy requirements and well-established privacy rights which could enable it to implement Zittrain's proposed system.[63] However, in the wider realm of privacy law, the system is more difficult to envision because the characteristics of a "trusted" system, and the criteria used to measure a "well-designed" system, drastically vary across industries.[64]

The system also makes a basic assumption: personal information can be "owned" under copyright law. As one scholar noted,[65] this could lead to a plaintiff, seeking to control his or her personal data using copyright law, "feel[ing] initially incongruous: she was seeking to replace the personal harm she felt with a commercial one and thus was required to

---

60. *Id.*

61. *Id.* at 1214–16. Another discussion of the connection between privacy law and copyright is discussed in Pamela Samuelson's paper *Protecting Privacy through Copyright?*. Pamela Samuelson, *Protecting Privacy through Copyright?*, *in* PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS 192 (Marc Rotenberg et al. eds., 2015). However, the discussion in that paper focuses on privacy rights in photographic images, including the emergence of "revenge porn" and sharing of images that were not willingly provided by the subject, rather than on use of materials and data collected directly by companies for users of their service. The focus on images also is an area where individuals have traditionally had more control over privacy through both the DMCA and publicity rights, and so is only tangentially related to this paper's topic.

62. *See* Zittrain, *supra* note 49, at 1226–45 ("Medical Data: A Trajectory of Personal Privacy Worries—and Responses to Them—in a Digitally Networked Environment").

63. *Id.* at 1237.

64. Solove, *supra* note 1, at 1088–89.

65. In an example involving Dorthy Lewis and Malcolm Gladwell.

accept herself as a subject that could be owned."[66] In other words, the system reduces the personal details of a user's life to a quantifiable value, which a company can buy away from you. As long as a company can afford a fair price, consumers have no right to refuse.

Another criticism of a copyright approach considers the basic power dynamic differences between privacy law and copyright law. In *Code: Version 2.0*, Lawrence Lessig writes:

> The big difference between copyright and privacy law, however, is the political economy that seeks a solution to each problem. With copyright, the interests threatened are powerful and well organized; with privacy, the interests threatened are diffuse and disorganized. With copyright, the values on the other side of protection (the commons, or the public domain) are neither compelling nor well understood. With privacy, the values on the other side of protection (security, the war against terrorism) *are* compelling and well understood. The result of these differences, as any political theorist would then predict, is that over the past ten years, while we've seen a lot of legislative and technical changes to solve the problems facing copyright, we've seen very few that would solve the problems of privacy.[67]

Personal privacy interests are innately "diffuse and disorganized" because they belong solely to individuals without commercial interests in the information.[68] Expecting individuals to negotiate license agreements or require technical standards for organizations with access to their information, in the way a large corporation typically would, is unrealistic given the disparate negotiation positions of the two parties.[69]

B. Trade Secret

1. A Trade Secret Approach to Privacy Law

Trade secret law was originally a form of common law tort, later encoded as the principles of the Uniform Trade Secrets Act.[70] The

---

66. Laura A. Heymann, *How to Write a Life: Some Thoughts on Fixation and the Copyright/Privacy Divide*, 51 WM. & MARY L. REV. 825, 868–69 (2009).

67. LAWRENCE LESSIG, CODE VERSION 2.0 200–01 (2006).

68. *Id.* at 200.

69. *Id.* at 201 (stating that over the last 10 years, "we've seen very few [solutions] that would solve the problems of privacy.").

70. UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf [https://perma.cc/9AXF-XW99].

Uniform Trade Secrets Act has been adopted in forty-seven states.[71] The main objective of trade secret law is to protect commercial entities from outside use of their secret information. Also known as the law of "commercial morality,"[72] trade secret law generally protects formulas, patterns, compilations, programs, devices, methods, techniques, and processes.[73] Trade secret protection extends for as long as the information remains secret.[74] Generally, a trade secret does not require formal registration, and is only codified when a trade secret claim is made.[75] To successfully bring a trade secret claim, a plaintiff must satisfy three basic requirements: (1) the information must have value and be a secret (i.e., it was protectable subject matter under trade secret law); (2) reasonable efforts must have been made to protect the information; and (3) the information must have been obtained through wrongful conduct.[76]

Pamela Samuelson's article, *Privacy as Intellectual Property?*,[77] proposes a trade-secret-based privacy system.[78] Samuelson's approach looks at establishing a market right for individuals in their consumer data, where online users could force companies to pay for the right to use their data, subject to specific restrictions. In other words, individuals could "license" their data to companies with a requirement that the company keep said data private (i.e., not share it with third parties).[79]

---

71. Nat'l Conference of Comm'rs on Unif. State Laws, *Legislative Facts Sheet—Trade Secret Act*, UNIFORM LAW COMMISSION, http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act [https://perma.cc/4JVM-ESPH].

72. ROBERT P. MERGES, PETER S. MENELL & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 26 (6th ed. 2012).

73. *Id.*

74. *Id.*

75. James W. Hill, *Trade Secrets, Unjust Enrichment, and the Classification of Obligations*, 4 VA. J.L. & TECH. 2, 4 n.19 (1999) (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 475–76 (1974) ("The protection accorded the trade secret holder is against the disclosure or unauthorized use of the trade secret by those to whom the secret has been confided under the express or implied restriction of nondisclosure or nonuse. The law also protects the holder of a trade secret against disclosure or use when the knowledge is gained, not by the owner's volition, but by some 'improper means,' which may include theft, wiretapping, or even aerial reconnaissance.")).

76. UNIF. TRADE SECRETS ACT § 1 (UNIF. LAW COMM'N 1985).

77. Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125 (2000).

78. *Id.* at 1151. Sharon Sandeen has built on Samuelson's model system and discussed the evolution of privacy law and trade secret law from common law roots, and the different paths the two sets of laws have taken. Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 673 (2006).

79. Samuelson, *supra* note 77, at 1152.

One benefit of the proposal is it would provide doctrinal support to consumers without burdensome government regulation.[80]

As discussed above, trade secret law evolved from the Uniform Trade Secret Act, which was adopted state-by-state until it encompassed the vast majority of the country with a uniform standard.[81] Privacy law, on the other hand, evolved into mismatched and overlapping state statutes, niche federal statutes and regulations, and private tort causes of action.[82] Sandeen suggests that privacy law could learn from trade secret law by creating a uniform legal schema adopted across states and focusing on "reasonableness" to help clarify and develop the legal application.[83] Sandeen's suggestion has notable benefits, especially in contrast to the current hodge-podge of privacy law.[84] It would create a uniform standard across (hopefully) all fifty states, and by focusing on reasonableness, the definition of a violation of privacy could remain flexible and adaptable to different circumstances and industry norms.[85]

2. Potential Problems with a Trade Secret Approach

Despite Samuelson's unique, free-market-supportive proposal, many privacy law scholars have dismissed a trade secret approach. One article argued that a trade secret approach would not work because American law has not adopted the notion of automatic "confidentiality" in commercial relationships.[86] Without the default right to confidentiality in a commercial relationship, American law would not easily stretch the definition of confidentiality to cover the relationship between a business organization and its customer.[87] Another scholar noted, "[i]t is also clear that a trade secret must have some economic/commercial consequence; that is, the rationale for maintaining secrecy cannot be purely a personal matter that goes to feelings of dignity and privacy."[88]

The sharpest criticism of the trade secret approach is that trade secret law, in and of itself, has defects capable of bleeding into privacy law:

---

80. *Id.* at 1135.

81. *See supra* discussion Section II.B.1.

82. Sandeen, *supra* note 78, at 677–78, 687.

83. *Id.* at 694–95.

84. *Id.* at 681 n.84 (discussing the hodge-podge that was unfair competition law before deciding there was no common law trade secret doctrine).

85. *Id.* at 694, 704.

86. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 180–81 (2007).

87. *Id.*

88. Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 556 (2010).

> Unfortunately, the commercial morality approach doesn't cure the defects of tort-based theories of trade secrecy. "Commercial morality" has no more substantive content than "unfair competition" or "unjust enrichment"—it still requires some external source to determine what behavior is and is not moral. To be sure, the commercial morality approach does at least point us to an external source—the emergent consensus (if there is one) of what constitutes acceptable behavior. But relying on such a vague norm to set legal standards has a number of problems. It is context and time dependent; normal behavior in one industry may end up being illegal in another . . . . It is likely to lead to inefficient results, retarding rather than enhancing innovation.[89]

This critique does not preclude any reasonableness-based approach to privacy protection; it simply suggests that reasonableness, without some kind of concrete basis of measurement, will likely lead to an impractical and inconsistent application of law.[90]

C. Trademark Law

1. A Trademark Approach to Privacy Law

Under trademark law, "a trademark is any word, name, symbol, or design, or any combination thereof, used in commerce to identify and distinguish the goods of one manufacturer or seller from those of another and to indicate the source of the goods."[91] Under the Lanham Act, a trademark can be used to "'protect the elements of a design that indicate the source of the product,' such as a logo, 'but does not provide general protection for designs.'"[92]

Trademarks help brands maintain a prestige premium (i.e., consumer trust and goodwill in a brand and its products).[93]

---

89. THE LAW AND THEORY OF TRADE SECRECY: A HANDBOOK OF CONTEMPORARY RESEARCH 120 (Rochelle C. Dryfus & Kathrine J. Strandburg eds., 2011).

90. *Id.*

91. *Trademark*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/trademark [https://perma.cc/BB2J-38MW]; *see also* 15 U.S.C. § 1127 (2018).

92. Day, *supra* note 48, at 248 (quoting *A Bill to Provide Protection for Fashion Design: Hearing on H.R. 5055 Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 109th Cong. 2 (2006) (statement of Rep. Howard L. Berman, Ranking Member, Subcomm. on Courts, the Internet, and Intellectual Property)).

93. *See* Paul Campos, *How a Louis Vuitton Bag Can Explain the Higher Education Bubble*, WEEK (Feb. 26, 2014), http://theweek.com/articles/450341/how-louis-vuitton-bag-explain-higher-education-bubble [https://perma.cc/TCJ9-46A8].

Several scholars have suggested methods of incorporating trademark law principles into privacy law. One author, David Dante Troutt, suggests trademark law as a way to take control of, and create intellectual property rights in, one's own identity.[94] His discussion, however, was more of a social commentary than a true suggestion of a system.[95] Another author, Paul Ohm, discusses trademark law as a way of implementing a notice-and-choice model in his article, *Branding Privacy*.[96] Generally, notice-and-choice models of privacy regulation presume the best way to protect consumer privacy is to inform consumers of an entity's data use practices and provide a mechanism to "opt-out."[97] Ohm suggests implementing notice-and-choice by having an entity commit to standards of treatment for private information.[98] If the company later chooses to change its policy, it would have to change the trademark displayed for its product or service in order to notify consumers of the change.[99] For example, if Facebook were to change its privacy practices, it would be required to pick a new name, like "Facebook Prime." Ohm's suggestion goes beyond the traditional notice-and-choice model; it essentially guarantees consumers that the companies they provide their personal information will continue providing the same level of privacy protection or be forced to surrender their trademarks, an unappealing prospect for most profitable companies. In part, Ohm's argument rests on the assumption that because consumers are naturally inclined to choose services with strong privacy standards, an appropriate privacy-protecting system need only present a consistent standard and clear notice when a standard changes.[100]

2. Potential Problems with a Trademark Approach

There are several potential flaws in Ohm's trademark-based approach. The first is the feasibility of changing the entire American trademark system to support companies changing their names every time they update privacy policies. Currently, an average company will change its

94. David Dante Troutt, *A Portrait of the Trademark as a Black Man: Intellectual Property, Commodification, and Redescription*, 38 U.C. DAVIS L. REV. 1141 (2005).

95. *See generally id.* (discussing using trademark law as a way of providing compensation for the use of one's identity, especially for those of color).

96. Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013).

97. *Id.* at 929.

98. *Id.* at 945–46.

99. *Id.* at 958–59.

100. *Id.* at 984–85.

privacy policy at least one to two times per year.[101] These changes can lead to weakened privacy protections for consumers, and often do, but can also encompass non-threatening, or even beneficial, changes enhancing consumer privacy protections. Examples of useful changes include: clarifying language, adding new privacy protections, or adding provisions to ensure the company is complying with new laws. Alerting the consumer through a trademark, without further explanation, would be both heavily burdensome to the company and confusing to consumers.

Moreover, changes in privacy standards are difficult to demonstrate because they can be implemented without altering a company's official privacy policy; security and privacy standards are oftentimes proprietary, and therefore inaccessible to the public. A company fearing giving up a trademark is necessarily incentivized to not update its public-facing privacy standards, even when change is beneficial to privacy, in order to maintain absolute consistency. The threat of a brand identity loss may also incentivize companies to curtail privacy standards development altogether to avoid falling below the standard.

Another problem is Ohm assumes consumers need only be made aware of changes to privacy practices, i.e., a notice-and-choice model is sufficient.[102] In contrast, as one scholar, Frank Pasquale, notes:

> [C]onsumers are not flocking to companies like Facebook and Google out of a conscious preference for the privacy policies on offer. Rather, they are drawn to such firms because of their fine-tuning and personalization of search and social network services. Each firm's hostility to privacy may be an important reason why they have the data needed to provide such fine-tuning and personalization, or they may simply be taking advantage of near-monopoly status as the highest quality search and social network experience. Given the opacity of operations at such firms, we may never know how necessary invasions of privacy are to their business models.[103]

New approaches to privacy law should seek solutions to the imbalance in power between companies with near-monopoly market positions and disorganized consumers, rather than merely increasing the

---

101. *See, e.g.*, *Previous Privacy Policies*, TWITTER, https://twitter.com/en/privacy/previous [https://perma.cc/5BF2-5DSU]; *Updates: Privacy Policy*, GOOGLE, https://policies.google.com/privacy/archive [https://perma.cc/P6XW-SSB9].

102. Ohm, *supra* note 96, at 984–85.

103. Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON L. REV. 1009, 1014–15 (2013).

visibility of "take it or leave it" privacy policies. Notice-and-choice models have also been criticized for their inability to fully notify consumers of the company's policies and for the lack of real choice on the part of the consumer.[104] Consumers rarely, if ever, read the privacy policies of every site they visit (and would generally find them incomprehensible if they tried).[105] As Felix Wu states,

> [E]ven if consumers could know perfectly what will happen to their data in an immediate transaction, it is virtually impossible for them to assess the long-term effects of that transaction on their privacy. Online services may also exhibit network effects or otherwise have characteristics that make it more difficult for consumers unhappy with a company's privacy policies to move to a competitor.[106]

II. RAND COMMITMENTS

As discussed in the previous section, leading scholars have considered a variety of IP approaches for protecting privacy. Each attempts to create a property right to allow consumers to force companies to respect and protect their data. However, all of these approaches face a similar barrier to implementation—consumers do not have enough power, individually, to assert a property right against a large online company.

This paper asserts that RAND commitments could solve this fatal flaw. RAND commitments are a practical, self-regulating, intellectual property-based legal tool that would work well in the context of privacy law because the RAND system's core purpose is to address equivalent inequities in bargaining power. In the patent sector, beginning decades ago, associations within an industry would form and cross-license patents among members in order to encourage innovation.[107] However, those same associations would keep out new competitors without valuable patents of their own, and create barriers to entry.[108] For example, an individual with a patent on a car's gas tank could prevent other companies from manufacturing cars compatible with normal filling stations. RAND commitments were created to address the concern of

104. Wu, *supra* note 43, at 71.

105. *Id.*

106. *Id.*

107. Daniel S. Sternberg, *A Brief History of RAND*, 20 B.U. J. SCI. & TECH. L. 211, 215–17 (2014).

108. *Id.*

market suppression by companies, or industry groups, with market-dominant positions.[109] The concerns run parallel with those of online data use, where large companies have kept relatively similar, sub-optimal standards, for the treatment of consumer data. To understand how RAND commitments would work for privacy, we first examine how said commitments work in patent law.

Stated broadly, RAND is a commitment made by SEP holders (i.e. the market-dominating companies) to offer Fair, Reasonable, and Non-Discriminatory (FRAND or RAND) license terms to potential licensees.[110] The framework rests on several important underlying concepts: (A) the definition of an SEP and the types of standards an SEP can encompass; and (B) the definition of a RAND commitment and the types of behavior that can violate RAND commitments. The section also examines: (C) how RAND commitments have worked on the ground.

A. The Fundamentals of Standard Essential Patents

SEPs are "patents that cover technologies that are considered an established standard in a particular industry."[111] In other words, SEPs are patents owned by a particular company but necessary for an industry at large. There are three basic types of SEPs: de facto, de jure, and standard setting organization (SSO) governed. The type of SEP informs different levels of obligation by the patent holder (i.e., different standards for RAND commitments) and/or different levels of restriction on potential licensees (i.e., regulatory requirements).

A de facto SEP covers technology an industry has adopted as a standard over time, by choice, without any conscious coordination or formal agreements among industry members.[112] The adoption of the standard generally occurs after a patent is granted, though in some situations adoption may occur before the patent has been published, meaning the public does not yet know the technology is being patented. One example of a de facto SEP is the JPEG file format. Many entities have claimed to have invented the JPEG format, despite its long history as a standard in digital photography and electronic images.[113] In 2002,

---

109. *Id.* at 220–24.

110. Kai-Uwe Kühn et al., *Standard Setting Organizations Can Help Solve the Standard Essential Patents Licensing Problem*, CPI ANTITRUST CHRON., Mar. 2013, at 1–3.

111. Johnson, *supra* note 38, at 202.

112. SAADAT MALIK, NETWORK SECURITY PRINCIPLES AND PRACTICES 273 (2003).

113. Paul Caplan, *What Is a JPEG? The Invisible Object You See Every Day*, ATLANTIC (Sept. 24, 2013), https://www.theatlantic.com/technology/archive/2013/09/what-is-a-jpeg-the-invisible-object-you-see-every-day/279954/ [https://perma.cc/K8HC-47VQ].

Forgent Networks came forward with a patent granted in 1987 over the JPEG format.[114] Eventually, prior art was found to invalidate the patent, but only after the patent generated years of license fees from companies using the standard.[115] In the case of the JPEG, the industry not only informally adopted the standard, but the standard was so ubiquitous it became difficult to identify the original inventor.[116]

A de jure SEP is a standard patent imposed on an industry by a government organization.[117] One example would be encryption standards. Government organizations have mandated that particular industries, like the financial institution industry, must use certain encryption standards when sending financial information over the Internet.[118]

An SSO SEP is a patent chosen by a SSO to be the standard within an industry. An SSO is an institution that develops, coordinates, promulgates, and revises technical standards (whether or not patented or patentable). An example of an SSO is the Institute of Electrical and Electronic Engineers (IEEE), which uses working groups to choose uniform standards for cross-industry applicable technologies.[119] When an SSO adopts a standard owned under an SEP, it will often oversee the licensing and disclosure process with the SEP holder. Many different interested parties may weigh in on how an SSO decides to adopt a standard, including the Federal Trade Commission (FTC) and the Department of Justice (DOJ).[120] Although SSOs will converse with a company and set standards for an industry, they do not set the monetary FRAND/RAND royalty rates, avoiding the appearance of price manipulation. SSO SEPs are increasingly found at the core of high-stakes litigation among major players in SEP-reliant industries,[121] and are the focus of this paper.

---

114. Matt Hines, *Graphic Patent Suit Targets Dell, Others*, ZDNET (Apr. 23, 2004, 8:17 AM), https://www.zdnet.com/article/graphics-patent-suit-targets-dell-others/ [https://perma.cc/4AKN-8G3Q].

115. James Niccolai, *Parts of JPEG Patent Rejected; Forgent to Appeal*, COMPUTERWORLD (May 29, 2006, 1:00 AM), https://www.computerworld.com/article/2545756/security0/parts-of-jpeg-patent-rejected—forgent-to-appeal.html [https://perma.cc/H5AD-4AAL].

116. *Id*.

117. MALIK, *supra* note 112, at 273.

118. PCI SEC. STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE 16 (Oct. 2010) https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf [https://perma.cc/ZF58-VH5W].

119. Kühn et al., *supra* note 110, at 1–3.

120. *Id.*

121. Johnson, *supra* note 111, at 203.

B. The Fundamentals of RAND/FRAND Commitments

FRAND/RAND commitments, in the SSO SEP context, are voluntary obligations, undertaken by a SEP holder, to an SSO.[122] The terms FRAND and RAND are relatively interchangeable: the former stands for "Fair, Reasonable and Non-Discriminatory" and the latter stands for "Reasonable, and Non-Discriminatory." For purposes of this paper, the most important concept to understand about RAND commitments is they create third-party beneficiary rights. In other words, even though the contract establishing a RAND commitment is created between an individual SEP holder and an SSO, third parties who wish to license the SEP holder's invention/technology are allowed to challenge any license terms they believe are unreasonable or discriminatory.[123]

While there is no single definition of what constitutes a fair, reasonable, and non-discriminatory license, the following basic aspects tend to be fairly consistent.[124] "Reasonable" refers to the equitability of the set price per use or overall license price of the SEP, generally as measured against industry standards, averages, and other related factors.[125] "Non-discriminatory" refers to keeping both license terms and license rates consistent across potential licensees.[126] Combined, an SEP holder must, in order to comply with a RAND commitment, offer non-exclusive licenses with standard royalty, restriction, and permitted use provisions for all licensees without preferential treatment. Violating a RAND commitment creates a breach-of-contract claim for the licensee or potential licensee.

C. Legal Effects of RAND Commitments and Microsoft v. Motorola

One final important aspect to understand about RAND Commitments is how they can be used in a legal proceeding. First, if a defendant formally counters a patent infringement claim with a breach-of-contract claim, the RAND commitment can be a direct defense to the patent

---

122. Kühn et al., *supra* note 110, at 1–3.

123. *Id.*

124. No official body has formally defined what Fair, Reasonable, and Non-Discriminatory licensing schemas are. Anne Layne Farrar et al., *Pricing Patents for Licensing in Standard-Setting Organizations: Making Sense of FRAND Commitments*, 74 ANTITRUST L.J. 671, 671 (2007).

125. Jeffrey I. D. Lewis, *What Is "FRAND" All About? The Licensing of Patents Essential to an Accepted Standard* 9, CARDOZO L. (June 11, 2014), https://cardozo.yu.edu/sites/default/files/Lewis.WhatIsFrandAllAbout.pdf [https://perma.cc/3NCD-HLAF].

126. *Id.* at 7.

infringement claim.[127] Second, an infringement defendant can use RAND commitments to demonstrate the plaintiff has not suffered irreparable injury, and remedies available at law are sufficient compensation.[128] Specifically, a defendant can argue that back-royalties at a RAND royalty rate are the appropriate remedy. Even if the defendant is unable to use RAND commitments to directly counter the plaintiff's claims, the defendant can use RAND commitments as a partial shield. Any evidence a plaintiff tried to charge the defendant above RAND licensing rates or did anything contrary to the non-monetary terms set with the SSO can weigh against granting an injunction or limit monetary damages.[129]

Microsoft Corp. v. Motorola, Inc.,[130] a Ninth Circuit case from 2012, demonstrates how RAND commitments and equity factors weigh into the decision to grant an injunction.[131] Before its dispute with Microsoft began, Motorola submitted standard license terms to several SSOs—namely, the IEEE and the International Telecommunications Union (ITU).[132] The specific standards referred to Wi-Fi technology and .mpeg file formats.[133] On October 21, 2010 (after submitting its RAND license terms), Motorola offered Microsoft a license agreement for the implementation of the SEP technology into several Microsoft products, including the Xbox videogame console and Windows operating systems.[134] The proposed license included a 2.25% royalty rate on the final price of the goods.[135] Microsoft refused the license on those terms, and continued using the patented technology in their products.[136]

In 2012, Microsoft brought suit against Motorola, claiming Motorola was breaching its contractual RAND commitments.[137] Microsoft argued it was entitled to licensing under RAND terms with much lower prices than those offered by Motorola, and not based on a percentage of final

---

127. *See* Doris Johnson Hines & J. Preston (J.P.) Long, *Un-FRAND-ly Behavior*, 87 BNA PAT. TRADEMARK & COPYRIGHT J. 572 (2014).

128. RealTek Semiconductor Corp. v. LSI Corp., No. C-12-03451-RMW, slip op. at 15 (N.D. Cal. May 20, 2013).

129. Lewis, *supra* note 125, at 5.

130. 854 F. Supp. 2d 993 (W.D. Wash. 2012), *aff'd*, 696 F.3d 872 (9th Cir. 2012).

131. *Id.* at 999.

132. *Microsoft*, 696 F.3d at 875–76.

133. *Id.*

134. *Id.* at 877.

135. *Id.*

136. *See id.* at 878.

137. *Id.*

sales prices.[138] In response, Motorola claimed the terms were reasonable and non-discriminatory, as other licensees had previously agreed to the same terms, and also claimed that the right to obtain RAND rates requires a preexisting license agreement between the parties, which did not exist between Microsoft and Motorola.[139] While the case was pending in the United States, Motorola filed suit against Microsoft in Germany for patent infringement and obtained an injunction against Microsoft.[140]

The U.S. district court considered the case in two parts. First, it considered whether the German decision and its injunctive effect should be respected.[141] The court decided that by suing in Germany before the U.S. court had issued a judgment, Motorola was attempting to forum shop and therefore the German injunction had an oppressive effect on Microsoft.[142] The court of appeals also found that Motorola's actions had frustrated the lower court's "ability to adjudicate issues properly," and issued an anti-suit injunction on those grounds.[143] In the second part of the case, the court held that the rates offered by Motorola were unreasonable, and Microsoft was not required to have a pre-existing license agreement in order to benefit from Motorola's RAND commitments.[144] In the court's discussion of the injunction, the RAND finding informed other equity considerations as to the appropriateness of injunctive relief.[145] The court held that Motorola had not demonstrated irreparable injury, and so traditional remedies—namely, monetary damages—were sufficient; Motorola was therefore not entitled to an injunction.[146] The final jury judgment against Motorola, after licensing offsets, totaled $14.5 million.[147]

---

138. *Id.* at 879.

139. *Id.*

140. *Id.* at 875.

141. *Id.*

142. *Id.* at 880.

143. *Id.* The factors of consideration the court used were from *E. & J. Gallo Winery v. Andina Licores S.A.*, 446 F.3d 984, 990 (9th Cir. 2006), which are "whether the foreign litigation would (1) frustrate a policy of the forum issuing the injunction; (2) be vexatious or oppressive; (3) threaten the issuing court's *in rem* or *quasi in rem* jurisdiction; or (4) where the proceedings prejudice other equitable considerations." *Microsoft*, 696 F.3d at 882.

144. *Microsoft*, 696 F.3d at 879.

145. *Id.* at 885–86. Specifically, the court used the finding in the traditional injunction eBay test under factors one and two.

146. *Id.* at 880.

147. Rich Gervase et al., *Evolving SEP Jurisprudence and RAND Determinations in* Microsoft v. Motorola, GLOBAL IP MATTERS (Aug. 21, 2015), https://www.globalipmatters.com/2015/08/21/evolving-sep-jurisprudence-and-rand-determinations-

III. RAND FOR PRIVACY

This paper suggests RAND commitments are an aspect of intellectual property law that would work well in the privacy law context. A privacy RAND commitment would consist of the following: (1) companies using consumer data would make a commitment to an SSO (discussed in section (C)(1) below) to use consumer data only in reasonable and non-discriminatory ways; (2) consumers would be able to see which companies have made RAND commitments in order to inform their choice of service provider; (3) the company and SSO would arrange for some form of affirmative statement regarding the privacy practices of the company in order to demonstrate the reasonableness of the company's practices; and (4) if a consumer, the FTC, or a consumer protection agency felt a company had not honored its commitment (i.e., had unreasonable or discriminatory practices), the individual or group could sue the company for breach of contract as a beneficiary of the company's original commitment to the SSO. Using RAND commitments would allow courts to acknowledge consumers' lack of meaningful choice when deciding whether to let online companies use their personal information. It would also allow for the development of new industry standards for online data use, which could include flexibility and tailoring based on company needs and industry preferences, and allow consumers to bring claims as individuals or as a class action when a company's behavior becomes unreasonable.

A. Online Companies Impact Our Everyday Life

1. Online Companies Often Dominate Online Market Segments

What does it mean to have a market-dominant position, and why does it matter? In the United States, an SEP holder has a duty to potential licensees.[148] In several other countries, such as Germany, companies constitute SEP holders subject to SEP duties only if they have first abused a market-dominant position.[149] In other words, a company must

---

in-microsoft-v-motorola [https://perma.cc/24V3-G3Z3].

148. AIPPI SPECIAL COMM. PATENTS AND STANDARDS, AVAILABILITY OF INJUNCTIVE RELIEF FOR FRAND-COMMITTED STANDARD ESSENTIAL PATENTS 8 (2014), https://aippi.org/wp-content/uploads/committees/222/Report222AIPPI+report+on+the+availability+of+injunctive+relief+for+FRAND-committed+standard+essential+patentsEnglish.pdf [https://perma.cc/UM2R-GMCY].

149. Consolidated Version of the Treaty on the Functioning of the European Union art. 102, Mar. 25, 1957, 2012 O.J. (C326) reads: "Any abuse by one or more undertakings of a dominant position within the internal market or in a substantial part of it shall be prohibited as incompatible with the

hold a market-dominant position in order to become subject to SEP licensing obligations. Under both definitions, having a "standard" or abusing a market-dominant position is an acknowledgment that the SEP-holder is in a position to make outrageous demands on any potential licensee, which the licensee is forced to accept based on the ubiquity of the patented technology within the industry.

In the realm of privacy, companies with market-dominant positions are able to impose whatever terms they want on an individual, offering their services on a "take it or leave it" basis, so consumers do not have a legitimate choice in how their data is used. While online companies may not be true "monopolies," and still face competition within the market, it is undeniable that many companies hold market-dominant positions.[150] The top two search companies, Google and Microsoft, together take up 85.5% of the online search market.[151] Facebook "owns" social networking with 30% more market share than its nearest competitors, Twitter and Reddit.[152] While some market segments include more than one company, those markets still tend to be "oligopolies," containing only a handful of major players, all with similar privacy practices.[153] For example, 50% of all Americans subscribe to Netflix, and 29% subscribe to Amazon Prime.[154] It is also important to note that many "competitors" are not actually market substitutes, i.e., a user cannot simply exchange their use of one company with another because the competitors are not actually providing the same product or service. For example, only 58% of Americans subscribe to any online streaming service, so the Netflix subscription population necessarily includes at least 72% of the users subscribing to Amazon Prime, making them complementary, rather than

---

internal market in so far as it may affect trade between Member States."

150. Given when market dominance is a measure of the strength of a brand, product, service, or firm, relative to competitive offerings. Susan Athey & Armin Schmutzler, *Investment and Market Dominance*, 32 RAND J. ECON. 1, 1–26 (2001).

151. Todd Bishop, *Google's Market Share Climbs in Latest U.S. Search Stats*, GEEKWIRE (Jan. 15, 2014, 2:14 PM), http://www.geekwire.com/2014/googles-market-share-climbs-latest-u-s-search-stats/ [https://perma.cc/QRV3-SJ67].

152. Priit Kallas, *Top 10 Social Networking Sites by Market Share Statistics [November 2017]*, DREAMGROW (Dec. 4, 2017), https://www.dreamgrow.com/top-10-social-networking-sites-market-share-of-visits/ [https://perma.cc/QRV3-SJ67].

153. Daniel Altman, *The New Monopolies*, FOREIGN POL'Y (Jan. 7, 2013, 3:45 PM), http://www.foreignpolicy.com/articles/2013/01/07/the_new_monopolies [https://perma.cc/6Y5T-QVKU].

154. *Share of Consumers Who Have a Subscription to an On-Demand Video Service in the United States in 2017*, STATISTA, https://www.statista.com/statistics/318778/subscription-based-video-streaming-services-usage-usa/ [https://perma.cc/S8Z8-SUGL].

interchangeable, products.[155] Therefore, a consumer looking to avoid using one product may not have a reasonable alternative, meaning that, from a practical standpoint, the company has a monopoly.

Even statistics underestimate the dominant positions of online companies. Facebook's market share is measured against companies like YouTube, Twitter, Pinterest, and LinkedIn—companies with very different functionality and value to the user.[156] It is unlikely that people tired of using Facebook would consider YouTube a meaningful alternative to stay in touch with friends and family. Even the arguably closest substitute to Facebook, LinkedIn, maintains a very different role in the market—professional networking versus Facebook's personal networking.[157] In the words of one writer, "no one expects . . . Skype to take over from Twitter. Though the border incursions do keep dominant firms on their toes, they have largely foundered as business ventures."[158] Just like Microsoft needed Motorola's exact file format to create the X-box, consumers "need" (or at least have few alternatives) to use Facebook to communicate with friends and loved ones, and unlike patented technology, possession of the "winning formula" doesn't expire after twenty years.[159] Facebook will never have to release its code for other companies to replicate.[160] As mentioned earlier in this paper, scholars have already taken note of the fact that "consumers . . . are drawn to such firms because of their fine-tuning and personalization of search and social network services."[161] Due to these industry dynamics, there is no Target versus Wal-Mart or McDonalds versus Burger King rivalry. Additionally, in these dominated online-market segments, the choice to use a service is dependent on community choices and technical compatibility. It does not reside solely with a consumer.

---

155. *Id.*

156. *Updated Social Media Market Share—March 2013*, VISUALLY, http://visual.ly/social-media-market-share-2013 [https://perma.cc/E2G5-VEAE].

157. Founded in 2004, Facebook's mission is to "give people the power to build community and bring the world closer together." *About*, FACEBOOK, https://www.facebook.com/facebook/info [https://perma.cc/SVH9-WXQF]. LinkedIn is "the world's largest professional network with more than 562 million users in more than 200 countries and territories worldwide." *About LinkedIn*, LINKEDIN, http://press.linkedin.com/about [https://perma.cc/S4ZM-QFUT].

158. Tim Wu, *In the Grip of the New Monopolists*, WALL STREET J. (Nov. 13, 2010, 12:01 AM), http://online.wsj.com/news/articles/SB10001424052748704635704575604993311538482 [https://perma.cc/7ASK-6V5V].

159. *See supra* section III.C.

160. Under the Uniform Trade Secret Act, trade secrets are protectable for as long as the information is kept secret. *See, e.g.*, UNIF. TRADE SECRETS ACT, supra note 70; WASH. REV. CODE ANN. § 19.108.010 (West 2018).

161. Pasquale, *supra* note 103, at 1014–15.

2. *Consumers Have Little Control over What Online Services They Use*

Online companies also resemble "standards" in that users often have little control over choosing a service. Just as a company who creates a part for a phone manufacturer will need to adapt the electricity standard the phone uses to ensure compatibility, consumers must use multiple online services to participate in modern culture. For example, a student's school e-mail account is frequently provided through Gmail. His or her work e-mail is frequently provided through Outlook.[162] Facebook and LinkedIn both use personal information for direct advertising: all his or her family is on Facebook, and LinkedIn is how he or she communicates with fellow alumni.[163] While a user can try avoiding using geolocation to get directions, sign-off of all social media, and use alternative internet browsers—to do so essentially eliminates the usefulness of technology developed over the past decade. All of the consumer's daily life is affected by technology, and there is no escape.

3. *Online Companies Have a Vastly Superior Bargaining Position in Relation to Consumers*

Because online services are so entangled with daily life, and given corporate market dominance, consumers have no ability to negotiate the terms of their relationship with service providers. In contrast to how businesses are often able to negotiate data-protection terms with each other,[164] individual consumers are left in the "take it or leave it" situation.[165] As discussed earlier, in privacy law, consumer interests are small and diffuse, so, in comparison with most forms of intellectual property law, imbalance of power between negotiating parties is much

---

162. Outlook's privacy standards and information gathered is governed by the Microsoft Online Privacy statement. *Microsoft Privacy Statement*, MICROSOFT, http://privacy.microsoft.com/en-us/fullnotice.mspx [https://perma.cc/2FCL-SYPN].

163. *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ [https://perma.cc/82JP-Z6PX]; *Privacy Policy*, LINKEDIN, https://www.linkedin.com/legal/privacy-policy [https://perma.cc/M4QS-S67F].

164. While specific negotiations are generally confidential and hard to cite directly, the practice of negotiating data security clauses in a business-to-business context is so common that IAPP releases "standard" contract clauses for integration into contracts. Dana B. Rosenfeld & Alysa Zeltzer Hutnik, *Data Security Contract Clauses for Service Provider Arrangements (Pro-customer)*, PRACTICAL LAW COMPANY (2011), https://iapp.org/media/pdf/resource_center/Rosenfeld_Hutnik_Contract-clauses_Service-provider.pdf [https://perma.cc/Y8J5-K2CJ].

165. Pasquale, *supra* note 103, at 1014–15.

greater.[166] SEPs create similar problems; the only difference is the source of the power. SEP holders benefit from a government-granted market-dominant position while online companies benefit from propriety technology.[167] In the data-use context, it is unclear whether a company's use of personal data is actually necessary to its business models, because consumers do not have the ability to negotiate as a group and gain insight into why a business wishes to gather said data.[168]

B. RAND Commitments Could Accomplish Real Privacy Objectives

1. RAND Commitments Would Facilitate Accountability

As discussed in previous sections, visibility into company data practices is a necessary prerequisite to setting standards for data use. However, companies often will not provide full transparency into their data cycle, due to both commercial and security concerns. A RAND system would necessarily require insight into data use and sharing in order to understand whether a company's practices were reasonable, but could do so in a more practical way than pure public disclosure. RAND commitments would require companies to explain and justify their information use as reasonable, both from a business perspective and from the perspective of the consumer. Even this simple requirement would drastically change the landscape of privacy law by giving consumers a better view into how companies are actually using their data, and helping them understand the true trade-off between utility and privacy.[169] In addition, a RAND system would present better practical methods for companies to disclose the details of their data use than the present "privacy policy" disclosure because it would provide avenues for disclosure without also disclosing proprietary information to the public at large. The disclosure could be made both proactively and

166. LESSIG, *supra* note 67, at 200.

167. Patents are generally defined as government granted monopolies. *A Patent Is a Government Granted Monopoly on an Invention*, LAWTEACHER (May 25, 2018), http://www.lawteacher.net/commercial-law/essays/a-patent-is-a-government-granted-monopoly-on-an-invention-commercial-law-essay.php [https://perma.cc/9WZT-TL5E].

168. Pasquale, *supra* note 103, at 1014–15.

169. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 60 (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/Y2J6-WQ5Y]. ("Commission staff called on industry to make privacy statements clearer, shorter, and more standardized; give consumers reasonable access to their data; and undertake consumer education efforts to improve consumers' understanding of how companies collect, use, and share their data.").

retroactively. Proactively, companies could disclose via a periodic audit by, or periodic reporting to, the SSO, similar to current FTC enforcement action requirements and/or business-to-business (B2B) contractually-mandated security audits, the results of which could be then relayed to consumers without the specific proprietary formulas or names of business partners. Retroactively, companies would have to respond to discovery requests in connection with the created causes of action, in which case trade secrets could be redacted from the information provided to the plaintiff. Both avenues for disclosure could make use of processes, like third-party audits and periodic reporting, that online companies already have in place for non-privacy related business processes.

2. RAND Commitments Are Workable for the Industry and Provide Flexibility While Still Allowing for Regulation

One of the biggest complaints from the tech industry, particularly in regard to enacting new, broader, privacy law, is that regulation is stifling and cannot move quickly enough to address changes in technology. Each year, technology evolves at a faster rate. While privacy laws in the United States have been adapted to effectively regulate specific concerns—for example, with children's privacy through the Children's Online Privacy Protection Act (COPPA)—the United States has failed to enact broader federal protections that would curb online companies' use of data. In fact, the United States has mainly focused on notice to consumers, rather than focusing on the data use itself. RAND commitments would change industry norms by allowing standards to adapt year over year, soliciting input from the industry as well as regulators and the public, and reflecting ongoing developments in technology.

Similar systems are already in place in the tech industry to address other concerns. Founded in 1996, the Interactive Advertising Bureau (IAB) in the last two decades has established itself as the creator of the default advertising terms for online ad placement through insertion order, based on the input of its members.[170] Hundreds of leading media organizations are now IAB members and rely on the IAB terms, either in their original form or with company specific addendums. This model demonstrates that even in the presence of competitive forces, technology companies can collaborate on "guidelines" for addressing shared concerns. Additionally, as discussed in the previous section, most of the

170. *About IAB*, IAB, https://www.iab.com/our-story/ [https://perma.cc/Q33U-VT7T].

transparency requirements needed to make a RAND system work are already utilized by data collectors to address concerns in other business segments. Thus, while the use of audits, proactive reporting, and responses to discovery requests may add a marginal administrative burden, they would not require businesses to make enormous outlays for new systems.

Companies also have incentives to make this system work. At a base level, given the recent public relations exposure from privacy violations, companies are looking for methods of "signaling" their respect for consumer privacy. RAND commitments would include tangible actions the market has the ability to reward, enabling both consumer participation in privacy law and reputational benefits enhancing company value. Signaling has a "virtuous-circle quality: as more people signal . . . as a positive reputation signal, the positive reputation signal grows in strength."[171] There are also very practical incentives to enacting effective self-regulatory systems. Following the introduction of the EU General Data Protection Regulation (GDPR), approved in 2016, and enforceable starting May 25, 2018, technology companies with an international presence will have to overhaul their current privacy practices.[172] In light of the changes, the industry needs to demonstrate that an industry-run regulatory system can work, and ideally work better, than new federal and state statutory schemes. This way, they could steer the federal government, or progressive individual states, away from implementing legislation with burdensome requirements similar to GDPR, like the newly-enacted statute in California[173] which technology companies are already trying to change due to its stringent requirements.[174] Government systems may also find that a RAND system addresses their concerns better than additional legislation would. By allowing for private rights of action, FTC follow-on enforcement,

171. Susan C. Morse, *Tax Compliance and Norm Formation Under High-Penalty Regimes*, 44 CONN. L. REV. 675, 683 (2012).

172. Megan Leonhardt & Alix Langone, *You've Probably Received a Ton of Privacy Policy Emails This Week. Here's What's Changing*, TIME: MONEY (May 24, 2018), http://time.com/money/5254754/gdpr-privacy-policy-rules/ [https://perma.cc/QE4C-YP7D].

173. Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/Q4VU-FEKX].

174. Derek Hawkins, *The Cybersecurity 202: Big Tech Is Going After California's New Privacy Law*, WASH. POST: POWERPOST (July 3, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/07/03/the-cybersecurity-202-big-tech-is-going-after-california-s-new-privacy-law/5b3a4e081b326b3348addc76/?noredirect=on&utm_term=.1a4c27be5736 [https://perma.cc/9UG9-C7WR].

and industry reporting, RAND commitments include avenues for governmental enforcement and governmental oversight, but also provide more efficient regulation by including the self-regulatory component.

3. RAND Commitments Support Concrete Enforcement and Remedies

RAND commitments would create several mechanisms for ensuring companies are incentivized to comply with the RAND requirements. First, as discussed in previous sections, breaking a RAND commitment (in the patent setting) is considered a breach of contract. Similarly, in the privacy world, RAND commitments would provide better mechanisms for class actions than current statutory rights of action because a breach-of-contract claim based on a company's commitments to privacy would be uniform across the entire class of consumers in most cases, and not subject to mandatory arbitration or damage limitations present in most "click-throughs."[175] Judges would also have more leeway to decide whether a company was being unreasonable based on its conduct.[176] This structure would incentivize class-action attorneys to take on contingency-fee cases, lessening the monetary burden on plaintiffs.

Second, RAND commitments introduce a self-regulatory component within the industry, because a violation of RAND commitments could be considered an "unfair business practice," which would allow other businesses (likely competitors) to bring a suit against a RAND-violating company based on the legal theory that the violation negatively affected their ability to compete in the market. This type of remedy already exists in other legal spaces. For example, in California, including a non-compete or no-hire clause in a contract can be challenged by a competitor as an unfair business practice.[177]

Third, RAND commitments would allow for enforcement by the SSO itself, which could investigate based on consumer complaints and

---

175. Class actions, in recent years, have generally had problems meeting uniformity requirements due to certain Supreme Court rulings, and this problem has also applied in the privacy context. *See* Wal-Mart Stores, Inc. v. Dukes, 564 U.S. 338 (2011). For an example of where a privacy violation was uniform across a class and therefore met the requirements of *Wal-Mart v. Dukes*, see *In re* Google Referrer Header Privacy Litig., No. 5:10-CV-04809 EJD, 2014 WL 1266091, at *3 (N.D. Cal. Mar. 26, 2014) ("Here, Plaintiffs contend the commonality requirement is met because the claims of all class members arise from one critical allegation: that Defendant's system-wide practice and policy of storage and disclosure of their search query information was unlawful.").

176. *See supra* section III.C. for an example of how judges can consider reasonableness in RAND commitments.

177. Spencer Hamer, *Non-Compete Clauses in California*, LAW JOURNAL NEWSLETTERS (Jan. 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/01/01/non-compete-clauses-in-california/?slreturn=20180513185256 [https://perma.cc/Q7FJ-UCNP].

detection of wrongdoing from reviewing periodic reports. Relatedly, RAND commitments would benefit current regulatory bodies like the FTC. The FTC can already investigate based on deceptive business practices and has issued guidance on "reasonable" privacy in its report, "Protecting Consumer Privacy in an Era of Rapid Change," which emphasizes three guiding principles: (1) privacy by design; (2) simplified consumer choice; and (3) greater transparency.[178] All three principles are furthered by a RAND approach. Additionally, the RAND system would address another problem in the current privacy regulatory space—the FTC's finite resources. By creating new private causes of action and B2B reporting, a RAND system would lower the pressure on the FTC to investigate every large technology company, while simultaneously leveraging their investigatory resources through the added reporting incentives and transparency requirements.

4. RAND Commitments Would Address Bargaining Power Imbalances

By creating the enforcement mechanisms and enhanced transparency discussed in previous sections, RAND commitments strengthen consumer bargaining power by amalgamating diffuse interests into a collective public good. The result is a relationship that more closely resembles two organizations with comparable size, rather than one large organization against a mass of individuals.

Some research has already been done to demonstrate that private companies respond to market pressures in the realm of privacy law.[179] Currently, those pressures appear to come from competitors and statutory sources, not from consumers.[180] By enabling competitor reporting and supporting regulatory enforcement, RAND commitments would use the pressure of competitors and government bodies to back consumer rights. In conjunction with the current change in public sentiment regarding privacy rights, RAND commitments should enable consumers to exert real influence on industry practices for personal data use.

---

178. FED. TRADE COMM'N, *supra* note 169, at 22–71.

179. Kusum L. Ailawadi, Donald R. Lehmann & Scott A. Neslin, *Market Response to a Major Policy Change in the Marketing Mix: Learning from Procter and Gamble's Value Pricing Strategy*, 65 J. MARKETING 44 (2001).

180. *See* Turow, *supra* note 4.

C. How Could a RAND System Work in Practice?

1. Finding an SSO

Organizations, for-profit and non-profit, big and small, have already started trying to establish privacy standards for online companies, and to hold those companies accountable for their actions. For-profit organizations like TRUSTe have tried to create self-regulatory systems to signal respect for privacy, but have run into obstacles both in adoption and maintaining reputational integrity.[181] Non-profit organizations, such as the Electronic Frontier Foundation (EFF), the American Civil Liberties Union (ACLU), and the Electronic Privacy Information Center (EPIC) have made it their mission to try to protect online consumer privacy.[182] The non-profit organizations have helped plaintiffs bring consumer privacy lawsuits, provide input for proposed legislation, and issue advisory reports.[183] Many companies considering a large change in their privacy policies may, at some point, consult the ACLU.[184] However, their relationships with technology companies are generally more adversarial than collaborative. That is not to say that such

---

181. *TRUSTe Settles FTC Charges It Deceived Consumers Through Its Privacy Seal Program*, FED. TRADE COMM'N (Nov. 17, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its [https://perma.cc/5EME-WAB6].

182. *See About*, ELEC. FRONTIER FOUND., https://www.eff.org/about [https://perma.cc/9CC9-LJ24]. ("Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development."); *Privacy & Technology*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/technology-and-liberty [https://perma.cc/2U8U-5BY7] ("The ACLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation."); *About EPIC*, ELEC. PRIVACY INFO. CTR., http://epic.org/epic/about.html [https://perma.cc/G2K2-K8VH] ("EPIC . . . was established . . . to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.").

183. *See, e.g.*, *ACLU Letter to the Data Privacy and Integrity Advisory Committee Regarding Its Report "The Use of RFID for Human Identification"*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/letter/aclu-letter-data-privacy-and-integrity-advisory-committee-regarding-its-report-use-rfid-human [https://perma.cc/46BD-92FW]; AM. CIVIL LIBERTIES UNION, ENFORCING PRIVACY: BUILDING AMERICAN INSTITUTIONS TO PROTECT PRIVACY IN THE FACE OF NEW TECHNOLOGY AND GOVERNMENT POWERS (2009), https://www.aclu.org/files/assets/ACLU_Report_-_Enforcing_Privacy_2009.pdf [https://perma.cc/89Y2-JLMV]; Apple v. Does, ELEC. FRONTIER FOUND., https://www.eff.org/cases/apple-v-does [https://perma.cc/5PAK-Y4V5].

184. *See, e.g.*, Theo Francis, *Strange Bedfellows on Health Privacy: ACLU & Microsoft*, WALL STREET J.: HEALTH BLOG (Oct. 19, 2007, 3:12 PM), http://blogs.wsj.com/health/2007/10/19/strange-bedfellows-on-health-privacy-aclu-microsoft/ (last visited June 11, 2018).

organizations do not play an important, indeed necessary, role in holding technology companies accountable for their actions, but their mission often necessitates fighting for idealism rather than pursuing compromised practicality.

To maximize buy-in while still protecting organizational integrity and concrete changes to privacy practices, a RAND SSO must be seen as independent from, but responsive to, industry members. In the realm of patent law, that role is filled by no single organization that holds all RAND commitments. Instead, multiple SSOs like the American Society of Mechanical Engineering (ASME) or the IEEE, became the recipient of said commitments.[185] In the privacy field, there are already organizations that could be viewed as functional equivalents. For example, the International Association of Privacy Professionals (IAPP), a non-profit formed in 2000, has become an industry leader in certifying individuals with the requisite knowledge to be considered "Privacy Professionals."[186] The IAPP also partners with corporate sponsors to host industry collaboration on important privacy topics and could be an appropriate recipient for initial privacy RAND commitments.[187] SOC and SOC 2, and related auditing, are self-regulatory standards created to support and verify responsible information security practices.[188] Alternatively, the industry could elect to create a new SSO dedicated to forming and enforcing RAND commitments.

One of the best recommenders for a RAND system, and self-regulatory models generally, is that they are adaptable. If one organization proves to be unable to effectively regulate and balance industry and public interests, a new organization can take its place without having to repeal any existing systems. In fact, allowing for multiple standards organizations allows for faster adoption by: (a) providing options for companies with specific preferences; and (b) allowing competition to clarify an optimal approach.

2. Expanding on Existing Legislation, in Word and in Deed

Once a privacy RAND SSO is selected or created, the question remains as to what privacy RAND standards would look like in practice.

---

185. *See, e.g.*, Am. Soc'y of Mech. Eng'rs v. Hydrolevel Corp., 456 US 556, 572 (1982).

186. *IAPP Mission and Background*, IAPP, https://iapp.org/about/mission-and-background/ [https://perma.cc/7PK4-BBLC].

187. *Id.*

188. *SOC for Service Organizations: Information for Service Organizations*, AICPA, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html [https://perma.cc/XXP5-T7KT].

As discussed above, the FTC has already issued "guiding principles" for privacy: (a) privacy by design; (b) simplified consumer choice; and (c) greater transparency. Additionally, the FTC has already issued some guidance on "unreasonable" practices by prosecuting and entering into enforcement actions in particularly egregious cases.

To create RAND privacy commitments, the SSO, and its industry members, could build upon the FTC's foundation, and the foundation of other legislation,[189] to go through a drafting and comment process to build policies addressing the privacy concerns at every stage of the data life cycle. After said policies are finalized and implemented, consumers can view the commitments put forth by a company and bring a breach-of-contract claim (if they believe the policies are unreasonable) at any point before, during, or after they commence using the service. The commitment, and the right to bring a RAND related claim, is not sacrificed if the consumer uses the service. From the company's perspective, the requirements and industry norms become clearer over time. If a customer brings a claim against the businesses' policies or actions that seemingly violate its commitments, a judge can issue a concrete ruling that will apply not just to that company, but to all other RAND-committed companies as well. As a result, the company would only have to litigate once, and consumers would all essentially be held to the ruling. If the judge ruled against it, the company would have clarity in terms of what aspects of its policies were unreasonable, analysis often lacking in the current legal environment. Therefore, the company would have legal certainty about its position for as long as it chooses to stay within its current personal data practices and policies and continue its non-discriminatory use of data. The judicial mechanism would provide an incentive to the company to continue using a simplified consumer choice model.

The system would also enable implementation of some of the more novel approaches to privacy rights. What if a machine learning algorithm could be used to anonymize data to the point that it could not be re-identified, categorizing users into effective segment profiles, rather than using individualized targeting? What if an algorithm could be created to effectively weed out falsified articles, or advertisers with inappropriate content? Technical advancements with the mission of

189. Other legislation includes current state laws in privacy-progressive states like Massachusetts, Illinois, and California, and industry-specific legislation like COPPA and HIPAA. LEUAN JOLLY, DATA PROTECTION IN THE UNITED STATES: OVERVIEW, WESTLAW: PRACTICAL LAW https://1.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true (last visited June 24, 2018).

protecting user privacy are already theorized. One set of academics analyzed a new machine-learning system called Chiron which attempts to anonymize training data for machine learning.[190] If an algorithm works better than a policy, SSOs could require or recommend the technology as a best practice.

To summarize, a RAND system will allow regulation to exist in a space between a mere principle and a stiff exacting requirement, allowing for the development of an applicable body of case law while still preserving the ability to adapt over time. Additionally, it does not have to hold to a pre-conceived idea of what a secure private system looks like, and can therefore examine new behavioral and technical solutions, perhaps managing to better predict and manage new privacy issues before they affect the public.

D. Concerns with a RAND Approach

1. Making Assertions Concrete

The first potential critique of a RAND system is that companies will not be forced to create clearer standards through RAND commitments than they already have under their opaque privacy policies. This paper argues that RAND commitments will help companies move towards clearer, more concrete commitments in two ways. First, if a company has clear standards, those standards will provide a litigation advantage and, as discussed above, will drastically decrease the company's overall litigation volume. For example, it would be much easier for a company to demonstrate the reasonableness of a data retention period of six months compared to a commitment that it was keeping data as long as reasonably necessary, because one is inherently easier to measure than the other, and does not require proof that retention was reasonably necessary. Second, even if only a small number of companies initially steer towards clearer commitments as a way to avoid litigation, their commitments will help create industry standards. In response to the development of standards, other companies will begin making their policies clearer as a way of ensuring they are not seen as a target for litigation or press that could hurt their public image. Essentially, the implementation of a RAND regime will result in a self-improving system; early adapters build the base standards, and in doing so, demonstrate the positive benefits of enacting said standards. Eventually,

190. *See generally* Tyler Hunt et al., *Chiron: Privacy-Preserving Machine Learning as a Service*, ARXIV (Mar. 15, 2018), https://arxiv.org/pdf/1803.05961.pdf [https://perma.cc/9BR3-GAHF].

those who refrain from making RAND commitments will face clear operational, legal, and reputational disadvantages compared to others within the industry.

2. Legally Demonstrating that a Company Violated Its Commitments

The next concern critics may raise is the difficulty of proving that a company violated its privacy commitments. The solution to this problem lies in shifting the burden to a company to show that its policies were reasonable, once the consumer has pled basic facts demonstrating that the average consumer *could* find the practices unreasonable. Proving that a company violated its commitments will also be easier to prove because, as discussed above, RAND commitments inherently define standards over time in measurable ways in contrast to the muddied waters of the present legal schema. The clearer the assertion, the less difficult it is for a plaintiff to support said assertions through discovery. Additionally, as privacy commitments would be consistent across all consumers, a named plaintiff could represent the reasonable consumer, allowing for a unified class more capable of bringing a successful class action.

3. Incentivizing Companies to Begin Making RAND Commitments

The final critique of this approach is that companies might not make RAND privacy commitments because they want privacy standards to remain unclear, preventing the system from gaining traction. This argument was brought up when RAND commitments were first presented in patent law. The argument was refuted fairly quickly when Samsung, Apple, Microsoft, Motorola, and many other companies chose voluntarily to make RAND patent commitments.[191] In fact, RAND policy (although initially present only within the United States) has already been accepted throughout much of Europe and Asia.[192] The benefits to adopters—given the intraoperative nature of the market and incentivized commitments—created an industry norm of SEP holders

---

191. *See generally* Microsoft Corp. v. Motorola, Inc., 696 F.3d 872 (9th Cir. 2012); Apple, Inc. v. Samsung Electronics Co., 678 F.3d 1314 (Fed. Cir. 2012).

192. Michael Frohlich, *FRAND and Injunctive Relief*, AIPPI (July 2012), https://www.aippi.org/enews/2012/edition25/Michael_Frohlich.html [https://perma.cc/9WEM-6ZDN]; Florian Mueller, *UK Judge Does Not Consider EU Court Case a Reason to Stay FRAND Rate-Setting and Damages Cases*, FOSS PATENTS (May 8, 2013), http://www.fosspatents.com/2013/05/uk-judge-does-not-consider-eu-court.html [https://perma.cc/BVG4-QSTW].

using RAND licensing.[193] Those who adopt RAND privacy commitments obtain multitudinous benefits: clearer legal expectations and standards, lower litigation volume, and a level playing field within the industry. While there is no way of knowing with absolute certainty that privacy RAND commitments would be used by companies until the option is presented, the investment needed to set up the framework is minimal given the self-regulatory nature of a RAND system. Additionally, as discussed in previous sections, the digital services industry is currently incentivized to create its own concrete obligations to avoid rigid and inconsistent regulation being enacted by applicable governing authorities. RAND commitments would allow technology companies to do what they do best, find innovative business and technical solutions to solve consumer concerns.

CONCLUSION

Many scholars have attempted to place privacy protections into the framework of intellectual property, but thus far their proposals have been hard to operationalize. One explanation for this difficulty is the common feature of the proposals—providing a property right to the consumer, who as an individual is unable to exercise the right in a meaningful way. In contrast to other intellectual property approaches, RAND commitments inherently consider inequity in bargaining positions and compensate for the imbalance. RAND commitments are also self-regulatory, allowing rapid and flexible adoption. The principle inducement for using RAND commitments is that the framework benefits both companies and consumers. The consumer is given a clear and demonstrable cause of action based on reasonable expectation; the company is given a flexible but consistent standard. Additionally, outside stakeholders have the opportunity to provide input and suggest standards for the industry. While there is no guarantee that RAND commitments would create meaningful legal reform, the low cost of implementation and self-regulatory nature means that adoption has a very low chance of causing any detrimental effects to either the law or the industry. For these reasons, the implementation of RAND commitments should be considered in the context of privacy law.

193. Jennifer Vanderhart, *F/RAND – The Economic Incentives and a Discussion of* Microsoft v. Motorola, MONDAQ (Sept. 12, 2013), http://www.mondaq.com/unitedstates/x/260112/Patent/FRand+The+Economic+Incentives+And+A+Discussion+Of+Microsoft+V+Motorola [https://perma.cc/Z8FB-BNFX].