JOURNAL OF LAW, ECONOMICS & POLICY

VOLUME 15 **WINTER 2018** **NUMBER 1**

JOURNAL OF LAW, ECONOMICS & POLICY

VOLUME 15 WINTER 2018 NUMBER 1

CONTENTS

ARTICLES

MEASURING COSTS AND BENEFITS OF PRIVACY CONTROLS: CONCEPTUAL ISSUES AND EMPIRICAL ESTIMATES[1]

Joseph J. Cordes[2] *& Daniel R. Pérez*[3]

INTRODUCTION

As increasing amounts of personal information become potentially available to internet providers, the government, and employers, a lively debate has emerged concerning the role of public policy in ensuring a proper balance between the various parties who may benefit from greater access to information and the protection of individual rights to privacy. A recent example is legislation passed in Congress repealing a regulation that "would have required internet service providers—like Comcast, Verizon and Charter—to get consumers' permission before selling their data."[4] As Robert Hahn, Anne Layne-Farrar,[5] and Adam Thierer[6] have noted, it is desirable that this debate be informed by a formal cost-benefit analysis based on empirical measures of costs and benefits.

Additionally, emerging technologies such as highly automated vehicles (HAVs or driverless cars) and unmanned aircraft systems (UAS or drones) bring privacy concerns to the forefront—particularly regarding the proper role of federal regulatory agencies. Accordingly, agencies such as the National Highway Traffic and Safety Administration (NHTSA) and the Federal Aviation Administration (FAA) currently face the difficult task of balancing their objectives of issuing sensible regulations that offer protec-

---

[1] This article reflects the views of the authors and does not represent an official position of the GW Regulatory Studies Center or the George Washington University. The Center's policy on research integrity is available at http://regulatorystudies.columbian.gwu.edu/policy-research-integrity.

[2] Professor of Economics, Public Policy and Public Administration, and International Affairs, Trachtenberg School of Public Policy and Public Administration, the George Washington University. Co-Director of the George Washington University Regulatory Studies Center. PhD University of Wisconsin-Madison Economics (1977).

[3] PhD Student, Public Policy and Public Administration, Trachtenberg School of Public Policy, the George Washington University. Policy Analyst at the George Washington University Regulatory Studies Center.

[4] Brian Naylor, *Congress Overturns Internet Privacy Regulation*, NPR (March 28, 2017, 6:10 PM), http://www.npr.org/2017/03/28/521831393/congress-overturns-internet-privacy-regulation.

[5] *See* Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 142-61 (2002).

[6] *See* Adam D. Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055, 1056-57 (2013).

tions to consumers and allowing continued innovation and use of these emerging technologies.

The regulatory process "incorporates significant requirements regarding the collection, use and accessibility of data that differ from other policymaking processes."[7] Statutes, such as the Administrative Procedure Act of 1946[8] (APA), require agencies to "justify most regulatory decisions based on the data, analyses, and other information collected and made part of a publically available record."[9] Data and other evidence used by agencies to justify rulemaking become part of the public record and are particularly relevant in the case of judicial review, where regulations can be vacated if reviewing courts determine agency actions to be "arbitrary and capricious."[10] The APA is only one of numerous mandates that constrain and guide the rulemaking process.[11]

Usable estimates of consumer privacy are a benefit to federal regulatory agencies because of the existing analytical requirements for collecting information under laws, such as the Paperwork Reduction Act (PRA).[12] The PRA requires agencies "to justify any collection of information from the public by establishing the need and intended use of . . . information . . . and showing that the collection is the least burdensome way to gather the information."[13] Agencies must receive approval from the Office of Information and Regulatory Affairs (OIRA) before initiating any information collection from ten or more people.[14]

In short, these mandates require agencies to base their rulemaking on a thorough analysis of regulatory costs and benefits, with added requirements to conduct retrospective *ex post* review of regulatory impacts. As the U.S. economy grows exponentially reliant on data generated by the collection of individuals' personally identifiable information (PII), regulatory agencies will need empirical measures of consumer valuations of privacy.

---

7 Marcus C. Peacock, Sofie E. Miller & Daniel R. Pérez, *A Proposed Framework for Evidence-Based Regulation* (2018), https://regulatorystudies.columbian.gwu.edu/proposed-framework-evidence-based-regulation (detailing a framework for producing evidence-based regulation structured around the three main phases of regulating: design, decision-making, and retrospective review).

8 PUB. L. NO. 79-404, 60 Stat. 237.

9 Peacock, Miller & Pérez, *supra* note 7, at 2.

10 5 U.S.C. § 706(2)(A).

11 *See, e.g.,* The Privacy Act of 1974, 5 U.S.C. § 552(a). *See generally* Susan E. Dudley & Jerry Brito, THE MERCATUS CTR. AND THE GEO. WASH. UNI. REG. STUDIES CTR., *Regulation: A Primer,* 45-47 (2d ed. 2012) (for a thorough list of laws and executive orders affecting regulatory policymaking). *See also* Susan E. Dudley, *Putting a Cap on Regulation*, 42 REG. LAW NEWS, AM. B. ASS'N 4-6 (2017) (providing a detailed explanation of executive orders affecting the rulemaking process signed by President Trump which include: Exec Order No. 13,771, 82 Fed. Reg. 9339 (February 3, 2017) and Exec Order No. 13777, 82 Fed. Reg. 12285 (March 1, 2017)).

12 44 U.S.C. §§ 3501-3520.

13 MAEVE P. CAREY, CONGRESSIONAL RESEARCH SERVICE, COST-BENEFIT AND OTHER ANALYSIS REQUIREMENTS IN THE RULEMAKING PROCESS, CRS REPORT R41974 15 (2014).

14 *Id.*

Our article strives to contribute to the development and greater use of such empirical measures. Drawing on the economics of privacy literature, we summarize why the costs and benefits of privacy controls should be measured *in principle*. We then discuss attempts that have been made to measure the costs and benefits of privacy control. Finally, we synthesize the various findings to advance promising practices for generating useful estimates of U.S. consumers' valuation of privacy.

I. THE BASIC FRAMEWORK FOR COST-BENEFIT ANALYSIS

As noted in a widely used textbook on cost-benefit analysis, the two foundational measures are: (1) willingness to pay (WTP) as measures of benefit to individuals who gain from a policy or as costs to individuals who are harmed; and (2) the social opportunity costs of inputs used to implement the policy.[15]

Willingness to pay can be measured in principle by the compensating variation (or in some cases equivalent variation) of a policy change, where the compensating variation equals the maximum amount of income a beneficiary of a policy would be willing to give up in order to have the policy implemented. Conversely, the compensating variation of someone harmed by the policy would equal the minimum amount of income that would need to be paid to someone harmed by the policy to leave them no worse than before the policy change. An alternative measure of willingness to pay, equivalent variation, equals the minimum amount of income that would need to be paid to a beneficiary of a policy in lieu of implementing the policy, or the maximum amount of income that someone harmed by a policy would be prepared to pay to prevent the implementation of the policy.

Defining the social opportunity cost of a policy is somewhat more straightforward. Namely, it is the value to society in its next best use of the resources that are used up in implementing a policy.

These measurement building blocks also apply to defining the benefits and costs of privacy controls, with appropriate adjustment for the somewhat distinctive nature of privacy markets, property rights, or both.

A. *A Simple Model of the Valuation of Online Privacy*

To help organize the discussion, we begin by summarizing the main features of an economic model of privacy formulated by Savage and

---

[15] *See* ANTHONY BOARDMAN, DAVID GREENBERG, AIDAN VINING, & DAVID WEIMER, COST-BENEFIT ANALYSIS 27 (Pearson Economic Series, 4th ed. 2010).

Waldman.[16] In the Savage and Waldman model, the individual is assumed to maximize a utility function which has as its arguments consumption (c), leisure (L), and privacy (P), which in turn is a declining function of the number of apps (a), so that P = P(a).[17]

Thus, the consumer's maximization problem can be stated as: $max_{h,a} U(c, L, P(a)) s.t.\ c = y + wh - p \cdot a; and\ L = T - h - T(a, e)$ In the problem, *y* represents unearned income, *w* is the wage rate, *h* is hours of work, and *p* is the per unit price of an app.[18] The function *T(a,e)* represents the impact of using apps on the amount of time the consumer uses for essential activities (essential time), which depends both on the number of apps used (*a*), and the individual's experience in using apps (e).[19] Holding *e* constant, increased use of apps is assumed to decrease the amount of essential time (e.g. result in essential time savings).

A key result of the model is that the rational consumer will acquire additional apps up to the point where $-wT_a = p + \left(\frac{U_P}{U_c}\right) \cdot P_a$.[20] The left-hand side of the aforementioned expression is the marginal value of essential savings of the marginal app purchased. The right-hand side of the equation represents the marginal cost of the marginal app, which is comprised of the per-unit app price (p) added to the marginal value of privacy lost by purchasing an additional app, $\left(\frac{U_P}{U_c}\right) \cdot P_a$.[21] The term $\left(\frac{U_P}{U_c}\right) \cdot P_a$ represents the marginal value to the consumer of giving up an additional unit of privacy at the margin, and hence represents the consumer's marginal valuation or willingness to pay for privacy.[22]

II. EMPIRICAL ESTIMATES OF THE WILLINGNESS TO PAY FOR PRIVACY

There are several ways of estimating the willingness to pay for privacy. One can attempt to estimate the marginal willingness to pay directly using data from choices that consumers are observed to make in the marketplace. Alternatively, one can use data from choices that consumers are observed to make in experimental settings or in surveys. Inferences can also be made from analogous markets, such as those that provide protections of consumer privacy. In this section, we summarize the results of such efforts.

---

16 *See* Scott Savage & Donald M. Waldman, *The Value of Online Privacy*, SSRN (2013), https://ssrn.com/abstract=2341311.

17 *Id.* at 9.

18 *Id.*

19 *See id.*

20 See id. at 10.

21 *See id.*

22 *See id.*

It is worth noting in advance that a review of literature on privacy provides considerable evidence that consumer privacy preferences vary substantially across different characteristics of interest. For example, studies generally find that females have higher valuations for privacy protection relative to males.[23] However, females also tend to value particular kinds of privacy protections over others (e.g. location data collected via a smartphone's GPS).[24] In contrast, males tend to value concealing their browsing history more highly than hiding their location data.[25]

Generating valid measures of consumer privacy is also made more difficult due to the so-called "privacy paradox" which notes that consumers' stated preferences for privacy protection are often completely uncorrelated with their behavior (i.e. what they actually pay to protect their PII).[26]

A. *Savage and Waldman, The Value of Online Privacy*[27]

Savage and Waldman estimated U.S. consumers' WTP to conceal various types of personal information from companies and third parties when downloading smartphone applications (apps).[28] The authors posed two primary research questions: (1) what is the value of online privacy for adults in the U.S., and (2) to what extent do these valuations vary with user experience?[29] They operationalized the concept of privacy by estimating U.S. consumers' WTP for smartphone apps in 2013.[30] Data on downloads of apps are generally useful for informing privacy valuations because consumers are required to relinquish various kinds of private information to app developers and third parties—in addition to the actual cost of the app—to benefit from using these apps on their smartphones.[31]

1. Methodology

The research design involved administering an in-person survey to consumers, with a pre-test and post-test, either in their homes or public

---

23 Dan Cvrcek, Vashek Matyas, Marek Kumpost & George Danezis, *A Study on the Value of Location Privacy*, PROCEEDINGS OF THE 5TH ACM WORKSHOP ON PRIVACY IN ELECTRONIC SOCIETY, 110, 116 (2006).

24 *See id.*

25 *See id.*

26 See generally Patricia A. Norberg, Daniel R. Horne & David A. Horne, The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors, 41 J. CONSUMER AFF. 100-126 (2007).

27 *See* Savage and Waldman, *supra* note 16.

28 *See id.* at 2.

29 *Id.* at 7-8.

30 *Id.* at 2.

31 *See id.* at 4.

places during the summer of 2013.[32] Interviewers used the pre-test partly to classify participants as either "experienced" or "inexperienced" users. Interviewers then showed participants an app on the interviewer's phone that was available to download in the marketplace.[33]

Participants were told that the app developer was considering several versions of the app that were identical with the exception of different privacy permissions, prices, and whether they included advertisements.[34] Participants were also told that they would have the opportunity to purchase the alternate version of their choice, which would soon be available in the market.[35] Interviewers asked respondents two questions: (1) which app do you prefer, and (2) do you intend to download the app once it is available?[36]

The post-test consisted of revealing to participants that the survey was conducted for research purposes only and that there were no alternative apps being developed, and asking questions to determine how likely participants were to follow through with their stated preference, in cases where they indicated they were going to download an alternate version of the app once it was available.

2. Primary Findings

The survey data indicated that the representative U.S. consumer is willing to pay $2.28 to conceal browser history, $4.05 to conceal list of contacts, $1.19 to conceal location, $1.75 to conceal a phone's ID number, $3.58 to conceal the contents of text messages, and $2.12 per app downloaded on a smartphone to eliminate advertising.[37] The Appendix contains a detailed list of findings, but it is worth noting here that the authors found the following characteristics to have significant effects on privacy valuations: gender, age, level of user experience, and education.[38]

B. *Acquisti, John & Loewenstein, What is Privacy Worth?*

Most of the studies summarized in this article attempt to generate specific estimates for consumers' WTP for privacy. However, Acquisti, John, and Loewenstein focused their efforts on investigating the extent to which

---

32 *Id.* at 16.
33 *Id.* at 12
34 *Id.* at 13
35 *Id.*
36 *Id.* at 13-14.
37 *See id.* at 22.
38 *Id.* at 25.

contextual, non-normative factors affect estimates for privacy preferences.[39] The authors note that findings from behavioral economics and decision research frame their assumption that consumer preferences for privacy are not as consistent or easy to measure as assumed by traditional economic theorists.[40] In short, they generally question the validity of estimates for consumers' WTP generated by research designs that tend to rely only on a single method of data collection.[41]

1. Methodology

The authors conducted a field experiment in which they offered two types of Visa gift cards to female shoppers at a mall in the U.S. in exchange for participating in a survey.[42] The subjects were offered, under various configurations, the options of: (1) a $10 "anonymous" gift card, for which purchases would not be linked to PII, and (2) a $12 "identified" gift card, for which purchases made would be tracked under their name and additional identifying information.[43] The authors provide a summary of the five conditions used to offer gift cards to subjects.[44] Conditions one and two test for endowment effects, conditions three and four check for order effects, and condition five is a rationality check control condition, offering a $12 anonymous card or a $10 identified card, to see if participants understood the trade-offs being presented.[45] The conditions are summarized below:

> 1. $10 endowed: Keep the anonymous $10 card or exchange it for an identified $12 card.
>
> 2. $12 endowed: Keep the identified $12 card or exchange it for an anonymous $10 card.
>
> 3. $10 choice: Choose between an anonymous $10 card and an identified $12 card.
>
> 4. $12 choice: Choose between an identified $12 card and an anonymous $10 card.
>
> 5. Rationality check control condition: choose between a $10 identified card or a $12 anonymous card. [46]

---

39 Alessandro Acquisti, Leslie K. John & George Loewenstein, *What is Privacy Worth?*, 42 J. LEGAL STUD. 249, 252 (2013).

40 *See id.* at 250.

41 *See id.*

42 *See id.* at 260-62.

43 *See id.* at 263.

44 *See generally id.* at 261.

45 Id.

46 *Id.*

2. Primary Findings

Over half of the participants endowed with the anonymous $10 card rejected an offer of $2 to reveal their future purchase data, while over 90% of the participants endowed with the identified $12 card refused to pay $2 to protect their privacy, e.g. not accepting the offer to switch to the $10 gift card.[47] These findings indicate that consumers' willingness to accept (WTA) is greater than or equal to $2 while consumers' WTP is less than $2.[48] The findings of this study raise substantial validity concerns for research that does not take into account insights from behavioral economics, including order and endowment effects into the design of the study.

C. *Beresford, Kübler & Preibusch, Unwillingness to Pay for Privacy: A Field Experiment*

Beresford, Kübler, and Preibusch conducted a field experiment in the form of a revealed preference test to estimate consumers' WTP for privacy protection, pertaining to the disclosure of their monthly income, during business transactions requiring the disclosure of PII.[49] The findings of this study are a substantial outlier relative to the other studies discussed in this article.

1. Methodology

The experiment involved 225 participants who were students at the Technical University of Berlin; 74 of the participants provided data via the option to purchase a DVD from one of two online stores.[50] The authors partnered with Amazon to create fictitious branches for two different retail stores that were ostensibly part of a known, multichannel retailer of DVDs in Germany.[51] Both stores were set up with different privacy disclosure requirements.[52] The treatments consisted of: (1) a scenario where both stores offered the same selection of DVDs for the same price, and (2) a scenario where one store offered the same selection of DVDs but at a dis-

---

47 *See id.* at 264-65.

48 *See id.* at 267.

49 Alastair R. Beresford, Dorothea Kübler & Sören Preibusch, *Unwillingness to pay for privacy: A field experiment*, 117 ECON. LETTERS (2012).

50 *Id.* at 26.

51 *Id.* at 25.

52 *See id.* at 25-26.

count of one Euro.[53] The store offering the one Euro discount required consumers to disclose their monthly income in exchange.[54]

2. Primary Findings

The authors indicated that consumers are generally unwilling to pay for privacy.[55] When faced with a trade-off between providing less sensitive, private information and a modest discount in price, approximately 92% of participants chose the discount.[56] Interestingly, the experiment also seemed to indicate that varying privacy disclosure requirements without varying price resulted in no significant effect on consumer decision-making. However, it is worth reiterating here that this study's findings are a substantial outlier in the privacy literature's estimates for consumer valuations of privacy. This is likely not only a result of sample selection bias, the sample having been college students, but also a result of the way that the authors chose to operationalize the concept of privacy, through disclosure of monthly income.

D. *Hann, Hui, Lee & Png, Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach*

Hann et al. administered a survey to estimate consumers' WTP to protect their PII during online transactions.[57] The authors administered the survey to university students from both the U.S. and Singapore.[58] The survey questions asked as part of the pre-test were motivated by the authors' choice to conduct a conjoint analysis of the data based on the expectancy theory of motivation.[59] The pre-test involved asking participants to rate their reasons for valuing privacy across several dimensions.[60] Answers from the pre-test were later compared to results of stated valuations to determine if there were any significant drivers that motivate participants to prefer more or less privacy under different contexts.[61]

---

53 *Id.* at 26.

54 *Id.*

55 *Id.*

56 *Id.*

57 Il-Horn Hann, Kai-Lung Hui, Sang-Yong Tom Lee & Ivan P.L. Png, *Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach*, 24 J. MGMT. INFO. SYS. 13, 14 (2007).

58 *Id.* at 21.

59 *Id.* at 21.

60 *Id.* at 23

61 *Id.*

1. Methodology

The authors administered a survey to undergraduate students in both the U.S. and Singapore.[62] The students were first asked to rank their level of concern for privacy generally and then asked to rank specific reasons that motivated that belief.[63] The participants then made a series of choices concerning the use of websites that facilitated transactions for different industries: financial, health care, and travel.[64]

The websites presented to participants varied in two ways: (1) cost and (2) the ability given to users to manage the private information they would be required to disclose to websites in order to use them.[65] Privacy management was broken down into three areas: (1) users' ability to review and correct private information disclosed to websites; (2) the ability to restrict private information against improper, third party access; and (3) the ability to prevent private information from being used for secondary uses, e.g. by someone other than the website for marketing purposes.[66]

2. Primary Findings

The authors found U.S. participants' privacy to be worth between $30.49 and $44.62 (annually/person) while participants from Singapore valued their privacy at an average value of $57.11.[67] Additionally, based on their pre-test questions, the authors claimed to have identified three distinct segments of internet users: "privacy guardians," "information sellers," and "convenience seekers."[68] The authors' breakdown of their survey results is as follows:

Value of Privacy (in U.S. dollars)[69]		
Web site privacy policy	United States	Singapore
Review for error	$11.18-16.36	$10.45
Restriction against improper access	$11.33-16.58	$19.73
Secondary use not allowed	$7.98-11.68	$26.93

---

62 *Id.* at 21.
63 *Id.* at 23
64 *Id.*
65 *Id.* at 22.
66 *Id.*
67 *Id.* at 29.
68 *Id.* at 30.
69 *Id.* (modified from authors' Table 3).

E. *Schreiner & Hess, Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies*

In addition to estimating a WTP for privacy protection, this study applied the theory of planned behavior (TPB) to explain the necessary conditions under which consumers would be willing to pay for additional privacy protection when using online content platforms like Facebook.[70] Like the study by Acquisti, John, and Loewenstein, the authors here generated valuable evidence regarding the contexts that shape consumers' preferences for privacy protection.[71] Additionally, they provided a model, a framework based on TPB, that is useful for conceptualizing the various drivers and forces shaping consumer preferences to pay for privacy protection.[72]

1. Methodology

The authors administered an online survey to 553 Facebook users in Germany.[73] The survey involved deceiving participants into believing that they were being offered the opportunity to bid on a soon-to-be-released premium version of Facebook with additional privacy control features in return for paying a monthly fee.[74] The auction and deception components were valuable for estimating WTP via revealed, rather than stated, preferences.

A pre-test was administered to operationalize participants' motivations for privacy preferences across seven potential drivers: attitude, intention, perceived behavioral control, perceived internet privacy risk, perceived usefulness, subjective norms, and trust.[75] Measures for each driver were estimated by using respondents' answers to questions within each category on a seven-point Likert scale.[76] The authors used these results to describe the potential drivers of their consumer WTP estimate.[77] The following is an illustration of their research model:[78]

---

70 Michel Schreiner & Thomas Hess, *Why Are Consumers Willing to Pay for Privacy? An Application of the Privacy-freemium Model to Media Companies*, 164 ECIS COMPLETED RES. PAPERS 2 (2015).

71 *Id.*

72 *Id.*

73 *Id.* at 9.

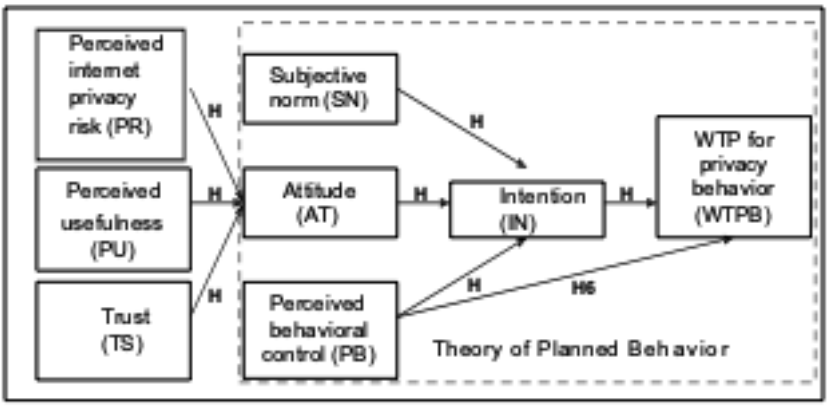
74 *See id.* at 8.

75 *Id.* at 7.

76 *Id.*

77 *Id.*

78 *Id.* at 6.



2. Primary Findings

The authors estimated a consumer WTP for additional privacy protection of 0.63 Euros per month when using online content platforms like Facebook.[79] The authors also performed an analysis on the various motivational coefficients, captured during the pre-test, to determine the relationship to revealed consumer WTP estimates. The authors found that participants' perceived usefulness (PU) and levels of trust (TS) in the fictitious premium version of Facebook significantly affected consumers' attitude (AT) about subscribing.[80] In this model, PU is a measure of the extent to which users believe that the privacy solutions offered by the premium version of Facebook are likely to address their privacy concerns.[81] Trust is a measure of the degree to which users believe Facebook is a trustworthy company.[82] Attitude is a more direct measure of participants' perception of actually subscribing to the premium version.[83]

Interestingly, the authors did not find a significant relationship between consumers' levels of perceived internet risk (PR) and consumers' attitudes towards the premium version of Facebook.[84] Overall, PR, PU, and TS explained 52% of the observed variance in AT under the causal assumptions of the model.[85] Finally, it is worth noting that subjective norms (SN) were estimated to also have a significant effect on intention (IN).[86]

---

79 See id. at 9.
80 *Id.* at 12.
81 *Id.* at 5.
82 *Id.* at 12.
83 *Id.*
84 *Id.* at 12.
85 *Id.* at 11.
86 *Id.*

F. *Cvrcek, Matyas, Kumpost, & Danezis, A Study on the Value of Location Privacy*

Cvrcek, Matyas, Kumpost, and Danezis conducted a survey to estimate the value of privacy, defined as participants' willingness to accept payment in exchange for use of their mobile phone data to track their location and movement on a daily basis for a month.[87] The auction involved the use of deception to convince participants that they were submitting bids to receive actual compensation in exchange for disclosure of their location data.[88] The experiment indicated that several consumer attributes might drive consumers' WTA payment for location data including: gender; nationality; the use of data, academic and commercial; and the duration of collection.[89]

1. Methodology

The study involved surveying 1,200 people from five different countries: Belgium, Czech Republic, Germany, Greece, and Slovenia.[90] The survey was structured using three separate auctions: (1) a one-month study with tracking data to be used for academic purposes only, (2) a one-month study where tracking data would be used for academic and commercial purposes, and (3) a year-long study that extended the conditions of the second auction.[91] It is worth noting that the authors re-calculated the values of bids submitted across different countries using a value of money coefficient, computed as a ratio of average salaries and price levels within a particular country.[92]

2. Primary Findings

The median bid, calculated using exchange rates in August 2006, was 43 Euros under the condition where participants chose to disclose their location data for academic purposes during a period of one month.[93] A breakdown of the data illustrates substantial variation among participants with certain characteristics. For instance, females' bids for the first condition were similar to males, but were 1.4 times higher for commercial use

---

87 Cvrcek, Matyas, Kumpost & Danezis, *supra* note 23.
88 *Id.*
89 *See id.* at 113.
90 *Id.* at 112.
91 *See id.* at 113.
92 *Id.*
93 *Id.* at 118.

and 1.8 times higher for extending the study from one month to one year.[94] Finally, participants' nationalities also accounted for variations in bids. For example, German and Slovak bids were five times the median bid.[95]

III. SYNTHESIS OF ARTICLE FINDINGS

A look across the findings within this article yields valuable information for future research to generate estimates for consumer valuations of their privacy. The Appendix contains a detailed list of findings for each study. The following are several key takeaways.

A. *Operationalizing Privacy is Highly Context Dependent*

The studies demonstrate that, although privacy is a complex concept, thoughtful research designs can generate useful estimates of consumers' WTA or WTP for privacy. However, these estimates are most valid given a context-specific definition of the privacy issue in question. For example, it would be of questionable validity to say with any certainty that an individual's privacy, broadly speaking, is worth $X to them; it is substantially more plausible to state that male consumers in the U.S. using social media platforms online are willing to pay $X every month to prevent private companies from sharing their browsing information with third parties.

Interestingly, since the use of various technologies requires almost identical kinds of privacy disclosures, e.g. location tracking, estimates that are sufficiently well specified, i.e. location tracking provided to whom for what duration, are transferable across conditions. This is particularly valuable for regulatory agencies, all of which work under considerable time constraints, as it prevents them from having to reinvent the wheel to find estimates for the costs and benefits of consumer privacy that can be used as evidence to support their rulemaking.[96] This applies even to cases where agencies are considering regulation of emerging technology.

B. *Privacy Valuations are Not Necessarily Stable*

Acquisti, John, and Loewenstein point out that most studies within existing privacy literature operate under the assumption that a rational con-

---

94 *Id.* at 113.

95 *Id.* at 116.

96 *See* RAY PAWSON, THE SCIENCE OF EVALUATION: A REALIST MANIFESTO 159 (2013) (discussing the transferability of knowledge generated across fields and institutions).

sumer's WTP and WTA should be equal.[97] In fact, our literature review indicates that consumer valuations fluctuate substantially under different conditions and are highly dependent on certain decisions made in the research design. For example, researchers should pay close attention to the role that endowment effects could have in driving estimates of consumer privacy. This applies to both stated and revealed preference studies. Do participants begin with a default expectation of privacy? Are consumers paying for a benefit they don't currently have or are they being offered money in exchange for disclosure of their PII?[98]

Even estimates of well-specified privacy conditions can vary with minor differences, such as changes in the recipient of PII, even within the same industry. For instance, consumers might state or reveal certain WTP to protect their data from a company they consider trustworthy but may be willing to pay substantially more to protect their PII from a company they personally consider untrustworthy.[99]

C. *Improving the Validity of Privacy Estimates*

The most convincing research efforts seem to make use of auctions, deception, or both to more closely approximate actual consumer market behavior. Assuming the privacy paradox remains valid, research designs generating estimates using participants' stated preferences are not likely to yield valid results. Designs that either require participants to make purchases with their own money, or successfully deceive participants into believing that they are receiving payment, or studies that actually do pay participants, using an auction system are more likely to generate more useful estimates of consumer valuations of their PII.

D. *Consumer Characteristics Matter*

Finally, research that treats consumers as a homogenous group is unlikely to produce useful estimates. Almost all of the studies covered by this article indicate that consumer characteristics are highly correlated with their valuations of particular kinds of privacy. For example, gender may affect WTP for certain privacy areas, such as location, but not others, such as duration.[100] Country of origin, a proxy for admittedly difficult to conceptualize cultural differences, also affects privacy valuations. This is worth noting, in particular, because it presents substantial limits on the estimates that U.S.

---

97 *See* Acquisti, John & Loewenstein, *supra* note 39, at 251.

98 *See id.*

99 Cvrcek, Matyas, Kumpost & Danezis, *supra* note 23.

100 *Id.*

regulatory agencies can use to support their rulemaking, i.e. consumer valuations of privacy in Singapore or Germany are likely to vary considerably relative to consumer valuations of privacy in the U.S.[101]

CONCLUSION

Adam Thierer, who argues for the need for cost-benefit balancing in evaluating privacy regulations, also noted that the empirical data needed for such balancing might be difficult to come by.[102] Our survey offers a somewhat more optimistic view.

Although estimating the economic value of privacy is challenging, it is not impossible. Estimations of the social costs of implementing privacy regulations are comparable in difficulty to estimations of social costs in other policy areas. Not surprisingly, estimating individual willingness to pay to protect privacy is more difficult. However, both theoretical and empirical frameworks exist for doing so. Indeed, there appears to be enough empirical literature to provide plug-in values of both the social costs and social benefits of privacy regulations to be used in undertaking cost-benefit analysis. An important next step will be to adapt such estimates for the purposes of undertaking actual and proposed regulation of privacy.

APPENDIX: EMPIRICAL ESTIMATES OF CONSUMER PRIVACY VALUATIONS

Study	Country	Empirical Estimates	Additional Findings
Savage & Waldman (2013)	U.S.	U.S. consumer WTP for privacy (per app): • $2.28 to conceal browser history • $4.05 to conceal list of contacts • $1.19 to conceal location data • $1.75 to conceal unique phone ID • $3.58 to conceal text messages	• WTP varies substantially with level of user experience • Consumer preferences are heterogeneous and vary across race, gender, income, education, and level of technological experience.

101 *Id. See also* Hann, Hui, Lee & Png, *supra* note 57.

102 Thierer, *supra* note 6.

		• $2.12 to eliminate advertising Given typical app in U.S. marketplace: • Benefit of app must be at least $5.06 • Estimated $17.08 billion benefit of app marketplace	
Acquisti, John & Loewenstein (2013)	U.S.	U.S. consumer WTP ≠ WTA to conceal purchasing data: • WTA ≥ $2.00 • WTP < $2.00	Privacy estimates generated are sensitive to framing of research design (*e.g.* endowment and order effects) and other contextual, nonnormative factors.[103]
Beresford, Kübler & Preibusch (2012)	Germany	German consumer WTP to conceal monthly income during online purchases < 1 Euro.	
Hann, Hui, Lee & Png (2007)	U.S. and Singapore	Consumer WTP to protect PII across 3 different categories during online purchases (protection against errors, improper access, and secondary use of personal information): • Between $30.49 - $44.62 in the U.S. • $57.11 in Singapore	• Participants from Singapore valued privacy more highly relative to U.S. participants. • Study identifies three distinct groups of subjects based on behavior toward privacy: privacy guardians, information sellers, and convenience

[103] *See* Acquisti, John & Loewenstein, *supra* note 39 at 249.

			seekers
Schreiner & Hess (2015)	Germany	WTP for additional privacy protection when using online content platforms like Facebook of 0.63 Euros per month.	Consumer WTP for privacy protection highly contingent upon the *perceived trustworthiness* of the company making the offer and the *belief* that the product addresses the underlying privacy concern.
Cvrcek, Matyas, Kumpost, & Danezis (2006)	Belgium, the Czech Republic, Germany, Greece, and Slovenia	Participants' median WTA for disclosure of location tracking data (6 months, for academic purposes) = 43 Euros.	• Consumer valuations of PII highly contingent upon *recipient* of PII (*i.e.* academic vs. commercial) and *duration* of tracking. • WTA payment for location data varies substantially across characteristics including *gender* and *nationality*.

UNPACKING UNFAIRNESS: THE FTC'S EVOLVING MEASURES OF PRIVACY HARMS

Cobun Keegan[1] *& Calli Schroeder*[2]

INTRODUCTION

Since 1994, when Congress codified the Federal Trade Commission's (FTC or Commission) three-part test for unfair business practices, the FTC has been cautious in its use of charges of unfairness in consumer protection enforcement—instead relying primarily on charges of deception. This focus has led to "deception-creep," an expansion of the Commission's perception of what constitutes deception to include acts and practices that may more classically be described as unfair. Overall, the FTC's enforcement effectiveness is reduced by adhering to a process that avoids applying the cost-benefit analysis required by the substantial injury prong of unfairness analysis. This neglect of unfairness enforcement reduces certainty in the consistency of FTC enforcement for businesses and consumers alike.

The FTC should embrace unfairness as an equal enforcement mechanism to deception. To properly utilize unfairness in privacy enforcement, the FTC must redefine the perimeters of unfairness and clearly draw the distinction between unfairness and deception. Once there is a defined understanding of when a violation falls under unfairness charges, the FTC can more effectively determine how best to utilize the codified unfairness test, including the cost-benefit analysis portion of determining whether an injury is substantial and constitutes an unfair practice.

To that end, we first briefly review the history of unfairness as an FTC enforcement tool, including trends in the frequency of its use. Next, we examine the unfairness test itself, analyzing the broad types of informational injuries that the FTC has deemed substantial in those privacy cases alleg-

---

[1] Cobun Keegan, a former Westin Fellow at the International Association of Privacy Professionals, interned in the office of Commissioner Maureen Ohlhausen at the Federal Trade Commission. He currently serves as a Compliance Analyst at the Online Interest-Based Advertising Accountability Program in the Council of Better Business Bureaus, enforcing industry standards for privacy online and on mobile devices.

[2] Calli Schroeder is a former Westin Fellow at the International Association of Privacy Professionals. She served as an intern in the office of Commissioner Julie Brill at the Federal Trade Commission. Currently, she is an Associate Attorney in the Data Privacy and Security and Intellectual Property practices at Lewis, Bess, Williams & Weese P.C., specializing in international data laws, surveillance issues, and general paranoia.

ing unfairness.[3] Finally, we divide these previously recognized injuries into operational categories, showing that the FTC has engaged in an implicit balancing test that recognizes informational injury based on the value of personal data. We recommend that the FTC formalize and publish the factors it has used to determine informational injury to provide further certainty for future privacy enforcement.

I. A BRIEF HISTORY OF UNFAIRNESS

"Unfair methods of competition in or affecting commerce, and *unfair or deceptive acts or practices in or affecting commerce*, are hereby declared unlawful."[4] In addition to the power to bring antitrust cases, Section 5 of the FTC Act provides the Commission with two mechanisms by which to bring consumer protection cases. Though the language is sparse, it is clear enough on one point, the fact that two distinct types of illegal trade practices fall within the FTC's enforcement power: unfair acts and deceptive acts. Unfair trade practices have for a variety of reasons been much less frequently enforced than the other half of the FTC's consumer protection mandate. In this section, we review the reasons for this relative dearth in enforcement, laying the groundwork to understand the current context of unfairness enforcement. Throughout this review of unfairness enforcement, we will show that when the Commission has alleged unfair trade practices in its consumer enforcement cases, it has engaged in an implicit balancing test, even before it was statutorily required to do so.

A. *1914–1938: From Unfair Competition to Unfair Practices*

Since its founding in 1914, the FTC has operated under a continuous mandate to protect U.S. consumers from unfair business practices.[5] But in the century since the passage of the FTC Act, the set of practices that the Commission considers unfair has shifted dramatically—due both to changes in the law and shifting FTC practices.[6] Section 5, the operative provision of

---

[3] We focus specifically on privacy cases rather than including data breach cases, or still broader types of consumer protection enforcement. It is worth noting that there is an ongoing internal FTC debate about the harms that may be used for establishing substantial injury in data breach cases. Acting Chairman Ohlhausen has indicated that health and safety risks and the exposure risks caused by collection of real-time, highly accurate location data (which, if breached could leave consumers vulnerable to stalking or other crimes) are likely to be considered sufficient. *But see* LabMD v. FTC, 894 F.3d 1221 (11th Cir. 2018) (finding that purely speculative harm is not enough to make a practice unfair).

[4] Federal Trade Commission Act, Section 5, codified at 15 U.S.C. § 45 (emphasis added).

[5] George Rublee, *The Original Plan and Early History of the Federal Trade Commission*, PROC. ACAD. POL. SCI. CITY NEW YORK, Jan. 1926, at 114, 117.

[6] Stephen Calkins, *FTC Unfairness: An Essay*, 46 WAYNE L. REV. 1935 (2000).

the FTC Act, at first banned only "unfair methods of competition in commerce."[7]

In 1931, the Supreme Court determined that Section 5, rooted as it was in the trust-busting goals of the progressive era, did not include within its definition of unfairness acts that injured consumers but left competitors unharmed.[8] In *Raladam*, despite the serious risk of harm to consumers and public health from grossly deceptive marketing of a dangerous "obesity cure," the Court concluded that the FTC had shown no harm to competitors or competition, and therefore had failed to prove its unfairness claim.[9] In fact, the Court showed that Congress had meant "unfair methods" to include only "those resorted to for the purpose of destroying competition or of eliminating a competitor or of introducing monopoly-such as tend unfairly to destroy or injure the business of a competitor."[10] Thus, though policing the fairness of business practices was part of the FTC's original mandate, this was limited to the antitrust context and the only recognized injuries were those to the market or to competition between businesses.

In response to the perceived inequity in enforcement that this interpretation created, Congress passed the Wheeler-Lea amendment of 1938, curing this shortcoming by adding "unfair or deceptive acts or practices" to the FTC's mandate.[11] The inclusion of injuries suffered by consumers, rather than solely injuries to businesses, enabled the FTC to bring enforcement actions against practices that were neither deceptive nor anticompetitive.

B. *1938–1972: Shaping a Standard for Unfairness*

Thus empowered, the FTC spent the subsequent decades finding unfairness in a wide variety of contexts, though it often charged companies simultaneously with engaging in both "unfair competition" and "unfair or deceptive trade practices."[12] The FTC's interpretation of unfairness therefore remained heavily influenced by the history of this term in antitrust law. Even when the FTC began to bring pure consumer protection cases, it generally alleged "unfair and deceptive" practices—as one complete phrase—rather than differentiating between "unfair" and "deceptive" acts.[13] As one

---

7 H.R. 15613, 63rd Congress (1914). *See* Rublee, *supra* note 5, recalling that "there was no intention to cover merely deceptive or dishonest practices by the prohibition of unfair methods of competition."

8 FTC v. Raladam Co., 283 U.S. 643, 652 (1931).

9 *Id.* at 653.

10 *Id.* at 650. The Court continued, "Although protection to the public interest was recognized as the ultimate aim, comparatively little was said about it." *Id*

11 Calkins, *supra* note 6, at 1949-1950.

12 *Id.*

13 *See, e.g.*, Holland Furnace Co., 55 F.T.C. 55 (1958), *aff'd* 295 F. 2d 302 (7th Cir. 1961); Dorfman v. FTC, 144 F.2d 737 (8th Cir. 1944).

contemporary FTC scholar noted, though a charge of unfairness "has been utilized in several cases involving sales practices, unfairness as a concept distinct from deception has been primarily restricted to cases of negative option selling and regulation of the holder in due course doctrine."[14]

It was not until 1964, fifty years after the FTC Act was first passed, that the Commission's understanding of unfair trade practices coalesced into its first published version of a three-factor test for determining that an unfair trade practice had taken place. This test was included as part of its Statement of Basis and Purpose on a regulation of cigarette advertising.[15] The Commission explained that it considered the following factors when determining whether a practice should be forbidden as unfair:

> (1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers (or competitors or other businessmen).[16]

Though this test bears significant similarity to the FTC's current three-part unfairness test, it is worth noting that the FTC had not yet—at least explicitly—interpreted unfairness to require a balancing of costs and benefits.[17]

During this time, the FTC viewed its own authority and discretion quite broadly, as seen in this language from a 1969 case:

> [The Commission] . . . is charged not only with preventing well-understood, clearly defined, unlawful conduct but with utilizing its broad powers of investigation and its accumulated knowledge and experience in the field of trade regulation to investigate, identify, and define

---

14 Larry Saret, *Unfairness without Deception: Recent Positions of the Federal Trade Commission*, 5 LOY. U. CHI. L.J. 537, 555 (1974).

15 Calkins, *supra* note 6, at 1951.

16 Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking ("Cigarette Rule"), 29 Fed. Reg. 8325, 8355 (July 2, 1964), http://cdn.loc.gov/service/ll/fedreg/fr029/fr029129/fr029129.pdf. The Cigarette Rule was reticent about whether all three factors were necessary for a finding of unfairness, saying only that they were sufficient: "If all three factors are present, the challenged conduct will surely violate Section 5 even if there is no specific precedent for proscribing it." *Id.*

17 *See* Calkins, *supra* note 6, at 1979 (arguing that the FTC's frequent enforcement against practices that have no conceivable benefit (such as theft or extortion) did not present the Commission with the opportunity to explicitly consider the balance between costs and benefits since "[a]ny harm outweighs zero benefit").

> those practices which should be forbidden as unfair because contrary to the public policy declared in the Act. The Commission, in short, is expected to proceed not only against practices forbidden by statute or common law, but also against practices not previously considered unlawful, and thus to create a new body of law—a law of unfair trade practices adapted to the diverse and changing needs of a complex and evolving competitive system.[18]

However, perhaps due to loud Congressional pushback over the Cigarette Rule, the Commission continued to avoid alleging unfairness in consumer protection cases during the 1960s.[19] When it did allege unfairness, the FTC still did so almost exclusively alongside charges of deception.[20] For example, in its directive against All-State Industries, the FTC alleged that failure to disclose the assignability of debt instruments was both unfair and deceptive.[21] On appeal, the Fourth Circuit affirmed the FTC opinion, without needing to explicitly determine whether both charges were warranted.[22]

C. *1972–1980: Unfairness Reaches its Peak*

The Commission was emboldened in its enforcement efforts by the Supreme Court's 1972 ruling in *FTC v. Sperry and Hutchinson Co.* (*S&H*).[23] In *S&H*, though ruling against the Commission, the Court expressed approval of the FTC's authority to bring charges of unfairness in consumer protection cases in a manner that "considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."[24] In a footnote, the Court cited the FTC's three-part unfairness test from the 1964 Cigarette Rule as an example of a clear and useful test.[25] The FTC chose to read this nod of approval as an implicit sanction, if not an outright endorsement, of its unfairness test.[26] Following the ruling, the FTC

---

18 All-State Indus. of N.C., Inc., 75 F.T.C. 465, 491 (1967).

19 J. Howard Beales, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection*, The Marketing and Public Policy Conference (May 30, 2003).

20 Michael L. Denger, *The Unfairness Standard and FTC Rulemaking: The Controversy Over the Scope of the Commission's Authority*, ANTITRUST L.J., Summer 1980, at 53, 57.

21 *All-State Indus. of N.C., Inc.*, 75 F.T.C. at 490.

22 All-State Indus. of N.C., Inc. v. FTC, 423 F.2d 423, 425 (1970). The closest thing to approval of the unfairness charge in this case was the court's assertion that, "Despite its severity the Commission thought the directive was a needed public precaution," a determination that, "was peculiarly justifiable here because of the nature and prevalence of All-State's deceptions."

23 405 U.S. 233 (1972). Note, however, that *S&H* did not find in favor of the FTC because the Commission had failed to rigorously apply its own standards in its enforcement action.

24 *Id.* at 244.

25 *Id.* at n.5.

26 *See, e.g.*, Letter from Federal Trade Commission to Senators Ford and Danforth (Dec. 17, 1980), *appended to* International Harvester 104 F.T.C. 949, 1070 (1984) [hereinafter Unfairness Policy Statement], https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

expanded its unfairness reach with a series of cases and rulemakings that established the working boundaries of unfairness.

During this period, the FTC expanded the application of unfairness to a variety of practices, often rooted in a finding of economic harms suffered by consumers. Such practices included transferring credit balances without informing consumers,[27] suing consumers in inconvenient forums,[28] and failing to possess a reasonable basis for making affirmative claims about product features—a harm that is economic in that it impedes "a consumer's ability to make an economically rational product choice."[29] Other alleged unfair practices centered around claims that the practices were morally objectionable and that this was sufficient to establish unfairness even though the economic effects of the practices may have been insubstantial. Key examples of these unfair practices include packaging razor blades in home-delivered newspapers[30] and advertising vitamins to children.[31]

The case against Beneficial Corp. is an early example of an unfairness argument regarding data privacy during this period.[32] In this case, the FTC alleged that Beneficial's failure to disclose that the company would use financial information it collected from customers for tax purposes to offer customers loans without their consent constituted unfairness.[33] More than twenty years later, FTC Chairman Pitofsky cited this case as precedent for the idea that "the misuse of certain types of private financial information can be 'legally unfair.'"[34] There are also cases during this period through which the FTC made clear that unfairness charges were not appropriate, further establishing the limit to the applicability of unfairness in enforcement actions.[35]

The 1970s also marked the beginning of the FTC's attempts to assert its authority over advertising practices.[36] This expansion of FTC authority into a new realm is relevant to the FTC's privacy enforcement because it

---

27 Genesco, Inc., 89 F.T.C. 451 (1977).

28 Spiegel, Inc. v. FTC, 540 F.2d 287 (7th Cir. 1976).

29 Pfizer, Inc., 81 F.T.C. 23, 60–62 (1972).

30 Phillip Morris, Inc., 82 F.T.C. 16 (1973).

31 Hudson Pharm. Corp., 89 F.T.C. 82 (1977).

32 Beneficial Corp., 86 F.T.C. 119 (1975), *aff'd in part, remanded on other grounds*, Beneficial Corp. v. FTC, 542 F.2d 611 (3d Cir. 1976).

33 *Id.* at 140. "Existing, established public policy, manifested in federal and state statutes as well as in the ethical codes of professional associations regards individual income tax information as confidential. Respondents' failure to respect the confidentiality of individual income tax information by allowing such information to be used to solicit tax customers for loans without their consent offends public policy and constitutes an unfair practice under [*S&H*]." *Id.*

34 Statement of Chairman Pitofsky and Commissioners Anthony and Thompson, In the Matter of *Touch Tone Information, Inc.*, File No. 982-3619 (1999), https://www.ftc.gov/sites/default/files/documents/cases/1999/04/ftc.gov-majoritystatement.htm.

35 Peter Turk & Michael Bernacchi, *Critique: The Expanding Jurisdiction of Deceptive, Misleading and False Advertising by the FTC*, J. ADVERT., Vol. 7, No. 2 (Spring, 1978), 58–59.

36 Both *Pfizer* and *Hudson Pharmaceuticals* are advertising cases.

laid the groundwork for FTC enforcement authority over later technological developments, such as algorithmic marketing practices that utilize big data in advertising to consumers. These later practices forge the connection between unauthorized use of consumer data (privacy) and big-data analytics in marketing (advertisements), still relevant today.

Pfizer served as a turning point in the understanding of FTC unfairness enforcement. Prior to the ruling, there was little need to define "unfairness" as a concept because most cases dealing with unfairness charges also included a deception charge. Because courts had rarely required the FTC to draw the charges apart, unfairness had functioned as more of an intensifier of deception charges than as an independent cause of action.

But in *Pfizer*, the FTC made clear its intention to pursue unfairness in this way, noting: "unfairness is potentially a dynamic analytical tool capable of a progressive, evolving application which can keep pace with a rapidly changing economy."[37] The *Pfizer* enforcement drew a clear line—the advertisements at issue did not deceive consumers regarding scientific testing of the advertised products, but made claims without any prior reasonable basis, affecting consumers' reasonable understanding of the products and possibly affecting their purchasing choices as a result.[38]

During the same period, shortly after the Supreme Court lent support to the FTC's unfairness criteria, Congress also expressed approval of the FTC's enforcement direction by supplementing the agency's jurisdiction, granting it broad rulemaking authority.[39] The FTC immediately moved to exercise its new rulemaking authority and "promulgate into Trade Regulation Rules the principles of consumer protection law which it has developed in the course of deciding individual cases."[40] Thus, the FTC tested the extent of its rulemaking powers—and quickly discovered their upper limit.

In attempting to apply theories it had used in case-by-case unfairness enforcement to the creation of broad new industry regulations, the FTC overstretched its mandate. In 1978, the FTC proposed a complete ban on all advertising directed at children, based on the unfairness principle of "public policy"—specifically, that any advertising to children was "immoral, unscrupulous, and unethical."[41] The breadth of this ban and perceived overreach of unfairness enforcement caused an outcry from the advertising

---

37 FTC v. Pfizer, 81 F.T.C. 23, 61 (1972) (citing FTC v. Standard Educ. Soc'y, 302 U.S. 112 (1937)).

38 Saret, *supra* note 14, at 550–53; Note, *The Pfizer Reasonable Basis Test—Fast Relief for Consumers but a Headache for Advertisers*, 1973 DUKE L.J. 563, n.26 (1973).

39 Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975). *See* Caswell O. Hobbs, *Unfairness at the FTC—The Legacy of* S&H, 47 ANTITRUST L.J. 1023, 1023–24 (1978) (explaining that this grant of rulemaking power "created a new procedural framework for the development of many of the FTC's emerging unfairness concepts.").

40 41 Fed. Reg. 3322 (1976).

41 *See* FTC Staff Report on Television Advertising to Children (Feb. 1978); Notice of Proposed Rulemaking on Television Advertising to Children, 43 Fed. Reg. 17, 967 (1978).

industry.[42] Congress responded in 1980 with a law temporarily cutting back the FTC's powers, including a ban from using funds to promulgate any unfairness-based regulation of commercial advertising.[43] As it turned out, this Congressional prohibition lasted for fourteen years.[44]

D. *1980–1994: Unfairness Lite*

In December 1980, in anticipation of oversight hearings before the Senate Consumer Subcommittee, the FTC issued its unanimous Policy Statement on Unfairness (Unfairness Policy Statement), which is still cited today as the most definitive analysis of the Commission's approach to unfairness enforcement.[45] Referencing the previous iteration of its unfairness test, the FTC revised the order of its steps: "(1) whether the practice injures consumers; (2) whether it violates established public policy; (3) whether it is unethical or unscrupulous."[46] The Unfairness Policy Statement also provided analysis to explain how each of these steps had been and would be applied in consumer protection enforcement. The Commission declared that "[un]justified consumer injury is the primary focus of the FTC Act, and the most important of the three *S&H* criteria."[47] Most importantly, the Unfairness Policy Statement laid out the three criteria the FTC would apply in determining whether the "injury" prong of its unfairness test was satisfied: the injury "must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided."[48]

Chastened by Congress's removal of its unfairness rulemaking authority, the FTC again became cautious in its unfairness enforcement, focusing its attention in most cases on direct financial harms, a clear and easily-measured form of injury. For example, it brought several actions during this time against companies that ran child-directed 900 numbers lacking safeguards to prevent children from racking up large fees without parental

---

42 Ernest Gellhorn, *Trading Stamps,* S&H*, and the FTC's Unfairness Doctrine*, 1983 DUKE L.J. 903, 941 (1983). *See* Hobbs *supra* note 39, at 1027 (illustrating the "lack of focus" of the FTC's unfairness theories with examples from the Commission's staff report on advertising).

43 *See* Federal Trade Commission Improvements Act of 1980, Pub. L. 96-252, 94 Stat. 374 (1980).

44 Roscoe B. Starek III, Speech: The ABC's at the FTC: Marketing and Advertising to Children (July 25, 1997), https://www.ftc.gov/public-statements/1997/07/abcs-ftc-marketing-and-advertising-children.

45 Unfairness Policy Statement, *supra* note 26, at 1070-71.

46 *Id.* at 1072.

47 *Id.* at 1073.

48 *Id.*

consent.[49] This relative vacuum of unfairness enforcement led to a modern FTC much more comfortable with pursuing charges of deception than unfairness. This gap became even more significant as technological developments led to new types of consumer harm and, in turn, new enforcement concerns at the agency.

E. *1994–Present: Codified and Underused*

In 1994, Congress amended the Federal Trade Commission Act.[50] The amendment effectively codified the promises of prosecutorial rigor in the Unfairness Policy Statement, including the explicit balancing test for meeting the substantial injury requirement for finding a practice to be unfair:

> The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers, which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[51]

Over the subsequent decades of FTC unfair trade practices enforcement, the Commission has kept within the outlines of this requirement, alleging unfairness only when it claims that consumer injuries pass the balancing test. The FTC's arguments have remained broadly consistent with the outlines provided in the Unfairness Policy Statement: in general, the FTC uses its unfairness authority to protect what it has termed the "free exercise of consumer decision-making."[52] Acts and practices that restrain this freedom in a manner that causes substantial injury can be deemed unfair, whether that injury involves direct financial loss, coercion into the purchase of unwanted goods or services, or serious risks to health or safety.

To count as causing "substantial injury," a practice may cause serious harm to a small number of people, or relatively small harms to many people.[53] The Unfairness Policy Statement does set some limit on the types of injuries that will count, explaining that "emotional impact and other more subjective types of harm . . . will not ordinarily make a practice unfair."[54]

---

49 *See* Fone Telecomm., Inc., 116 F.T.C. 426, 426 (1993), Phone Programs, Inc., 115 F.T.C. 977, 977 (1992); Teleline, Inc., 114 F.T.C. 99, 399 (1991); Audio Commc'ns, Inc., 114 F.T.C. 414, 414 (1991).

50 H.R. 2243, 103rd Congress (1994).

51 15 U.S.C. § 45(n) (2012). The statute continues with a nod to the FTC's broad mandate: "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination." *Id.*

52 Unfairness Policy Statement, *supra* note 26, at 1074.

53 *Id.* at 1073 n.12.

54 *Id.* at 1073.

For example, the FTC will not "ban an advertisement merely because it offends the tastes or social beliefs of some viewers."[55] However, the Unfairness Policy Statement leaves open the possibility that certain emotional effects may be considered "in an extreme case" so long as "tangible injury could be clearly demonstrated."[56] A harm may not be "merely speculative," but an injury may be substantial if it "raises a significant risk of concrete harm."[57]

The following sections provide a close analysis of substantial injury, the lynchpin of FTC unfairness enforcement. We examine the ways in which the FTC has previously described consumer harms when alleging unfairness in data privacy enforcement cases. Looking closely at the facts of these unfair privacy cases, we summarize the arguments the Commission has already used to find informational injury. Finally, we recommend that the FTC formalize these methods into a clear and robust balancing test to both broaden and clarify the scope of unfairness enforcement.

II. DECEPTION VS. UNFAIRNESS IN DATA PRIVACY CASES

By the turn of the twenty-first century, the FTC was well on its way to establishing its position as the primary U.S. privacy enforcement agency.[58] As with other unfairness cases, the substantial majority of the FTC's data privacy cases have also alleged deception—and even more cases have alleged deception without bringing an unfairness charge.[59] When it is alleged, unfairness often seems to be included as an intensifier and more often than not, the FTC's analysis of its enforcement authority focuses on deceptive practices, providing only peripheral insights into its application of the cost-benefit unfairness analysis.

This habit of avoiding unfairness analysis by expanding the reach of deception charges is actually weakening the effectiveness of FTC enforce-

---

55 *Id.*

56 *Id.* at n.16 (citing as a public policy example the Fair Debt Collection Practices Act's ban on harassing late-night telephone calls).

57 *Id.* at n.12. *But see* Order Re Motion to Dismiss, FTC v. D-Link Systems, Inc., No. 3:17-cv-00039-JD, at *1, 6-10 (N.D. Cal. Sept. 19, 2017) (dismissing the FTC's unfairness claim against a router manufacturer because it only alleged a future likelihood of substantial injury brought about by an identified security vulnerability), https://www.hldataprotection.com/files/2017/09/Opinion___12b6____19-Sept.-2017.pdf.

58 *See generally* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).

59 Appendix I, *infra*, provides a selected list of FTC cases that have alleged unfair privacy practices (excluding data breach cases). See the International Association of Privacy Professional's FTC Casebook for a complete database of data privacy cases, including those alleging only deception: https://iapp.org/resources/ftc-casebook/.

ment.[60] Though preventing deceptive acts and practices is one of the FTC's most vital roles, an enforcement regime focused primarily on deception and neglecting use of its other enforcement abilities reduces the efficacy and longevity of FTC enforcement for a variety of reasons: (1) deception in privacy cases is largely premised on the legal fiction that consumer expectations originate with a close understanding of lengthy terms of service agreements;[61] (2) deception is reactive and limited in reach to companies that violate their own privacy promises;[62] and (3) when expanded to include mere inadequate disclosures, deception eclipses the central question of unfairness cases: whether informational injuries caused by an unexpected collection or use of consumer data are outweighed by benefits.[63]

The FTC's 2015 case against Nomi Technologies illustrates the first two concerns.[64] Nomi Technologies developed and sold technology that enabled in-store retail location tracking of individual customers.[65] By enforcing against Nomi, the Commission sought to curb the potentially unfair practice of surreptitious in-store retail location tracking of individuals without proper consent.[66] Yet the FTC shoehorned Nomi's practices into a charge of deception, alleging that the third-party tracking company omitted material facts from a privacy policy few, if any, consumers had read.[67] Indeed, consumers were likely just as unaware of the startup's existence as they were of its tracking technology. Harms to consumers flowed more directly from retail stores' installation of technology that contravened consumer expectations, tracking shopping behavior without notice, consent, or an opportunity to opt out. Thus, in *Nomi*, the split Commission debated the materiality of an online privacy disclosure—an argument over the reach of a deception claim—rather than debating the merits of in-store tracking

---

60 For an analysis of how internal divisions in the FTC's prioritization of privacy enforcement have contributed to its relatively cautious enforcement record, see Chris Jay Hoofnagle, *The Federal Trade Commission's Inner Privacy Struggle*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Evan Selinger, Jules Polonetsky, & Omer Tene, eds.) (Cambridge University Press 2018, forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2901526.

61 *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 105 (2009).

62 *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 334 (2016) (explaining that "deception is increasingly difficult to use against online privacy problems because companies can write longer, more comprehensive, and more ambiguous privacy policies.").

63 See the VIZIO discussion, *infra*, for an example of a practice that was disclosed in the company's privacy policy but remained surprising to consumers. Such a practice could fall within the FTC's purview either through the deceptive nature of an inadequate disclosure (such as the lack of a just-in-time notice), though this is not truly deceptive in the legal sense, or by being deemed unfair, which requires that the FTC apply its balancing test.

64 Complaint, Nomi Techns., Inc., F.T.C. No. 132 3251 (Sept. 3, 2015), https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf.

65 *Id.*

66 *Id.*

67 *Id.*

technologies, including their costs and benefits.[68] A shift to unfairness in such a case would cause the Commission to analyze whether consumer perceptions of the harm of surreptitious retail tracking practices outweigh any benefits of these practices. This analysis, in turn, would lead to more robust guidance for businesses and consumers alike, highlighting the need for real notice of unfairly surreptitious data collection practices, no matter how well such practices are disclosed in a privacy policy.

The FTC's recent case against the television manufacturer VIZIO demonstrates the third risk of the Commission underplaying its unfairness hand.[69] In VIZIO, the FTC argued that a single data collection practice—the granular and longitudinal monitoring of household TV viewing data—was both unfair and deceptive when engaged in by a television manufacturer without proper notice and consent.[70] The FTC applied its expanded *Sears*-type definition of deception, wherein a company's full privacy disclosures are deemed deceptive if not presented to consumers with enough prominence and clarity.[71] And, while the FTC did also allege that VIZIO's collection of TV viewing data was unfair, it did not engage in the steps of an unfairness analysis, instead merely stating in its complaint that VIZIO's collection of "sensitive" TV viewing data had caused substantial injury. This prompted Commissioner Ohlhausen to call for the FTC to "examine more rigorously what constitutes 'substantial injury' in the context of information about consumers."[72] The workshop, held in December, 2017, resulted in a rich new set of scholarship in this developing research area.[73]

---

[68] *Compare id., and* Statement of Commissioner Julie Brill (Aug. 28, 2015), https://www.ftc.gov/system/files/documents/public_statements/799561/150828nomitechbrillstatement.pdf, *with* Dissenting Statement of Commissioner Maureen K. Ohlhausen (Aug. 28, 2015), https://www.ftc.gov/public-statements/2015/08/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-nomi, *and* Dissenting Statement of Commissioner Joshua D. Wright (Apr. 3, 2015), https://www.ftc.gov/system/files/documents/public_statements/638371/150423nomiwrightstatement.pdf .

[69] Complaint for Permanent Injunction and Other Equitable and Monetary Relief, FTC v. VIZIO, Inc., No. 2:17-cv-00758 (D. N.J. Feb. 6, 2017), https://www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf.

[70] *Id.*

[71] *See* Complaint, Sears Holdings Mgmt. Corp., F.T.C. No. C-4264 (Sept. 9, 2009), https://www.ftc.gov/sites/default/files/documents/cases/2009/09/090604searscmpt.pdf.

[72] Concurring Statement of Acting Chairman Maureen K. Ohlhausen In the Matter of Vizio, Inc. (Feb. 6, 2017), https://www.ftc.gov/system/files/documents/public_statements/1070773/vizio_concurring_statement_of_chairman_ohlhausen_2-6-17.pdf.

[73] *Informational Injury Workshop*, FTC (Dec. 12, 2017), https://www.ftc.gov/news-events/events-calendar/2017/12/informational-injury-workshop. Public comments filed in advance of the workshop are available at https://www.ftc.gov/policy/public-comments/2017/10/initiative-721.

Through its case history, the FTC reveals that it engages in a balancing test—sometimes implicitly—when it alleges that a practice is unfair, weighing consumer injuries (and potential injuries) against any benefits to consumers and competition. Since the balancing test was added to the FTC Act, the Commission has consistently referenced the three-part test in its complaints, but has only rarely engaged in an explicit justification of its step-by-step analysis. However, by analyzing the facts and context in which the FTC has previously alleged unfairness, we are able to identify aspects of the balancing test at work in the FTC's unfair privacy complaints. Thus, our recommendations to the FTC about future engagement in unfairness analysis do not represent a substantial change from existing practice but merely a call to open this implicit test to public scrutiny. The Commission should provide a robust and transparent cost-benefit analysis in its complaints describing the criteria it has considered in arriving at an allegation of unfairness.

Others have claimed that, "the extent to which practices like online tracking or sharing data with third party advertisers would constitute 'substantial consumer injury' for the purposes of unfairness remains unclear."[74] However, as various tracking and data-sharing practices become more prevalent in day-to-day business practices, enforcement precedent provides helpful signposts for the boundaries of fairness in the use of such technologies. Additionally, the prior history of FTC enforcement can provide a significant amount of clarity as to the direction enforcement will likely take regarding these advancements.

There are a limited—but not insubstantial—number of prior FTC cases from which to draw conclusions about what constitutes substantial injury in the data privacy context. In fact, in the past two decades the FTC has brought a total of at least twenty-eight data privacy cases in which it has brought an allegation of unfairness. Of those cases, only twelve have alleged an unfairness claim without an accompanying deception claim.[75] Below we provide a deep-dive analysis of these twelve "pure" unfairness cases, organized by type of harm alleged. In all these cases, the three elements considered in establishing substantial injury for purposes of unfairness have, as one would expect, remained consistent. The injury to consumers must be: "(1) substantial, (2) without offsetting benefits, and (3) one that consumers are unable to reasonably avoid."[76] Those cases that charge unfairness alone are more representative of the FTC's understanding of its

---

74 James C. Cooper & Joshua D. Wright, *The Missing Role of Economics in FTC Privacy Policy*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 465, 467 (Evan Selinger, Jules Polonetsky, & Omer Tene, eds., 2018).

75 *See* Appendix I, *infra*.

76 Beales, *supra* note 19.

unfairness authority and, when contrasted with cases charging both deception and unfairness, provide a complete picture of what constitutes an unfair data privacy practice.

In general, our analysis reveals that the FTC has been reluctant to acknowledge privacy injuries beyond direct and indirect financial harm. Most privacy unfairness cases involve consumer data that was actually sold for value or sensitive data that was shared with third parties. In the latter case, though direct financial harm may not be calculable, the proxy of financial injury appears to be assumed based on (1) the sensitivity of the data, (2) the lack of a direct relationship with consumers, (3) consumers' lack of knowledge of and agency over the sharing. We also note a couple of outlier cases in which the FTC describes emotional or reputational harms in its complaints.

A. *Financial Injury—Unauthorized Sale of Data*

Many FTC unfairness cases assert direct financial harms, that is, losses suffered by consumers, as a basis for substantial injury. While other forms of injury require a more in-depth analysis about the value associated with consumer loss of information, the depth or seriousness of injury, or proper methods of enforcement for a given injury, direct financial harm is readily measurable—the dollar amount lost to consumers and sometimes the monetary amount gained by the violator in unfair profit. There are two (often implicit) arguments that have resulted in almost all data privacy unfairness allegations being brought in cases in which data was shared without consumer permission. First, data has value, and consumers only give up this value if they give permission to share.[77] In many cases, economic loss that consumers suffered can be considered equivalent to the amount of money that the company earned from the sale of that same data. This is the only scenario in which the FTC has been able to extract financial penalties through a 13(b) suit that alleges this type of harm.[78] Second, consumers only share sensitive data with entities that they expect to have a confidential relationship with (banks, etc.). This reliance leads to strong consumer expectations about the privacy of certain types of their personal data.

---

[77] Cassandra Liem and Georgios Petropolous, *The Economic Value of Personal Data for Online Platforms, Firms and Consumers*, BRUEGEL (Jan. 14, 2016), http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/.

[78] *See* Michael Scully & Cobun Keegan, *IAPP Guide to FTC Privacy Enforcement*, IAPP, https://iapp.org/media/pdf/resource_center/Scully-FTC-Remedies2017.pdf (last visited Nov. 13, 2017) (describing the process and requirements of the FTC's 13(b) judicial enforcement mechanism).

The recent enforcement actions against Sequoia One[79] and LeapLab[80] show this type of consumer injury in its most dramatic form. In these actions, the entities sold payday loan applications (containing consumer Social Security numbers, financial account information, and other sensitive information) to third parties without consumer consent or knowledge, continuing to do so even after receiving complaints from customers that the third parties were making unauthorized debits from consumer accounts. The lack of relationship between the entities and consumers meant that the FTC did not pursue deception charges.

In its complaints, the FTC concluded that selling the applications containing consumers' sensitive information to non-lenders caused a financial injury to consumers measurable by the amount of ill-gotten gains that Sequoia made from the unauthorized sales. In this case, the FTC implies the lack of any countervailing benefit to consumers or competition, stating that there was no legitimate need to sell the sensitive information to non-lenders.[81] Balancing injuries and benefits is straightforward in cases like this. Because the sale of sensitive information to unsafe parties only provides monetary benefit derived directly from the fraudulent injury, which can have no benefit to competition, there is nothing to place in the benefit column. And because the ill-gotten gains from the unauthorized sale of consumers' sensitive information totaled over $7 million, the sum of the balancing test is clear.[82] In fact, the 13(b) case filed against LeapLab resulted in a rare monetary penalty being imposed based on these ill-gotten gains and totaling more than $4 million.[83]

Another example of unauthorized sharing is the case against Vision I Properties, a supplier of shopping cart software for websites.[84] Vision I began renting consumer information, collected from its third-party website clients, contrary to the posted privacy policies on some of their sites, even though it was aware of the privacy policies presented on the merchant

---

[79] Complaint for Permanent Injunction and Other Equitable Relief at 3-4, FTC v. Sequoia One, LLC, No. 2:15-cv-01512 (D. Nev. Aug. 7, 2015), https://www.ftc.gov/system/files/documents/cases/150812sequoiaonecmpt.pdf.

[80] Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Sitesearch Corp., (D. Ariz. Dec. 11, 2014), https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf.

[81] Complaint for Permanent Injunction and Other Equitable Relief at 11, FTC v. Sequoia One, LLC, No. 2:15-cv-01512 (D. Nev. Aug. 7, 2015).

[82] Default Judgment and Order for Permanent Injunctions as to Defendants Sequoia One, LLC and Gen X Marketing Group, LLC at 4, FTC v. Sequoia One, LLC No. 2:15-cv-01512-JCM-CWH (D. Nev. Nov. 14, 2016), https://www.ftc.gov/system/files/documents/cases/161129_sequioa_-_default_jdgmnt_ord_.pdf.

[83] Final Judgment and Order for Injunctive and Other Relief at 6, FTC v. Sitesearch Corp., No. CV-14-02750-PHX-NVW (D. Ariz. Dec. 11, 2015), https://www.ftc.gov/system/files/documents/cases/160218leaplabsitesearch.pdf.

[84] Complaint, Vision I Properties, LLC, F.T.C. No. 042 3068 (Mar. 10, 2005), https://www.ftc.gov/sites/default/files/documents/cases/2005/03/050310comp0423068.pdf.

sites.[85] It also failed to inform any of the merchant sites that it intended to share consumer information with third parties, denying them the opportunity to contract around such use or to adjust their privacy policies to reflect the data use.[86]

Notably, unlike LeapLab and Sequoia One, Vision I Properties was not making use of highly sensitive financial data, but simple transactional data. This highlights another trend distinguishing unfairness charges from deception: the consumer injury in all three of these cases related to sharing already-collected data in a manner to which consumers could not consent and of which they had had absolutely no knowledge. Note that, like many unfairness cases, it is not the collection itself, but the improper use of data, that warranted FTC action.

B. *Unauthorized Sharing / Exceeding Scope of Collection*

Most unfair practices the FTC asserts in privacy cases involve the sharing of information with third parties or improper access to already-existing information, even if this information is not shared for value. This may not appear remarkable until one considers the wide range of privacy practices implicated in the FTC's deception analyses. Thus, the willingness of entities to refrain from sharing consumer's sensitive or confidential data with unknown third parties is at the core of fairness in the privacy context. Ensuring that firms do not exploit the power dynamic between themselves and their customers has some early precedent in the FTC's case against All-State Industries.[87] All-State paved the way for recognizing injuries caused by firms acting as impediments to consumers' free exercise of economic choices, finding that it was an unfair practice to assign notes of indebtedness to third parties without consumers' knowledge or consent because such assignment reduced consumers' agency—removing their ability to dispute the debts.[88]

A clear example of unauthorized sensitive data sharing is the Cornerstone and Company enforcement action. In this action, Cornerstone posted Excel spreadsheets full of sensitive customer information that it was attempting to sell unencrypted or redacted in any way on a publicly available website.[89] The file included data on over forty thousand customers, including full name, birthday, employment information, bank account and routing

---

85 *Id.* at 2–3.

86 *Id.* at 3.

87 All-State Indus. of N.C. v. FTC, 423 F.2d 423 (4th Cir. 1970).

88 *Id.*

89 Complaint for Permanent Injunction and Other Equitable Relief, Cornerstone and Co. v. FTC, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014), https://www.ftc.gov/system/files/documents/cases/141001cornerstonecmpt.pdf.

information, and in at least one case, full credit card account numbers.[90] Similarly, Bayview Financial was a debt broker that posted sensitive financial data publicly online without customers' knowledge or consent.[91] This shared data included "first names, cities and states, email addresses, dates of birth, driver's license numbers, full bank account and bank routing numbers, employers' names and contact information, the consumers' status as purported debtors, and the amount of each consumer's purported debt."[92]

The balancing test in these two cases remained straightforward, despite there being no measurable monetary damage to consumers—in both cases there was no evidence that the data had been co-opted by third parties.[93] This is because there is no countervailing benefit to measure in these cases. On balance, even a small harm, especially when paired with a large risk of harm, weighs much more than a complete lack of benefit to consumers and competition. In fact, the FTC concluded that Cornerstone had "no business need to disclose consumers' sensitive personal information in such a public and widespread manner."[94] Finally, consumers in this action could not easily avoid the risk of damage because, again, they had no knowledge of or control over Cornerstone's actions in posting the information for sale.

C. *Unfair Collection*

The case against Aaron's Rent-to-Buy presents the situation in which a company was charged with unfairness for the acquisition, rather than the dispersal, of sensitive consumer information. Aaron's rented computers directly to consumers according to purchase plans wherein the consumer would eventually own the computer.[95] Unbeknownst to consumers, several Aaron's franchisees installed software on the rental computers enabling the company to disable a computer remotely or engage in surveillance that included the ability to log keystrokes, track location, capture screenshots, and make use of the computer's webcam with no indication of the action to the consumers.[96] This activity was undetectable, irreversible, and largely un-

---

[90] *Id.* at 4–5.

[91] Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Bayview Solutions, LLC, No. 1:14-cv-01830 (D.D.C. Oct. 31, 2014), https://www.ftc.gov/system/files/documents/cases/111014bayviewcmp.pdf.

[92] *Id.* at 7.

[93] Press Release, FTC Alleges Debt Brokers Illegally Exposed Personal Information of Tens of Thousands of Consumers on the Internet (Nov. 12, 2014), https://www.ftc.gov/news-events/press-releases/2014/11/ftc-alleges-debt-brokers-illegally-exposed-personal-information.

[94] Complaint for Permanent Injunction and Other Equitable Relief, at 6, Cornerstone and Co. v. FTC, No. 1:14-cv-01479-RC (D.D.C. Aug. 27, 2014).

[95] Complaint at 1–2, Aaron's Inc. F.T.C. No. 122 3264 (Mar. 11, 2014), https://www.ftc.gov/sites/default/files/documents/cases/131022aaronscmpt.pdf.

[96] *Id.* at 2.

disclosed to consumers.[97] This unauthorized and largely undisclosed collection of sensitive data opened consumers to the risk of substantial harm relating to personal, financial, and medical information along with the invasion of consumer's private lives.[98]

This case was pled solely as an unfairness case rather than combining the charge with a deception charge. Here, the importance of the injury or risk of injury to consumers is obvious—invasion of privacy in the home without consent and collection of several forms of sensitive information for numerous consumers constitutes a substantial and potentially very damaging invasion of privacy, even without the sharing of this data. Next, there were few to no offsetting benefits. While Aaron's made the argument that geographic tracking was a useful tool in retrieving devices for which consumers had lapsed in payment, there was no business reason to take images of the consumers, log keystrokes, or even to keep geographic tracking on at all times prior to default on payment. Finally, consumers could not have reasonably avoided this harm. In several cases, the existence of the software was not disclosed to consumers and even if consumers were made aware of it, they had no means of disabling the software or uninstalling it from the device.

This case also illustrates a rare unfairness instance where the perpetrator of the unfair practice had a direct relationship with the consumer. Aaron's did not purchase consumer information or collect it from a third party. Consumers established the relationship by coming into a store or franchise and signing an agreement for use of the device in question. Perhaps this made Aaron's violation all the more egregious. Because it had a direct source of contact with consumers, it could have easily made even greater efforts of disclosure and obtaining consent. It seems that this contravention of consumer expectations is at the core of the substantial injury the FTC identifies in this case.

D. *Non-Financial Injuries*

Recall that the FTC's Unfairness Policy Statement describes the fact that unfairness harms need not be limited to economic harms in order to qualify as substantial injuries.[99] Even so, financial injuries account for the vast majority of privacy unfairness cases brought by the FTC. Yet there remains a number of exceptions, which we explore in this section. In addition to the possibility of an egregious breach of consumer privacy expectations resulting in a de facto substantial injury (as described above), the FTC

---

97 *Id.*

98 *Id.* at 4.

99 Unfairness Policy Statement, *supra* note 26, at 1073.

has included other types of non-financial injury in its pleadings and complaints. The case against Accusearch is one unique example.

Accusearch bought customer phone records (customer proprietary network information under the Telecommunication Act of 1996)[100] and other information (including financial account numbers) using false pretenses, reselling this data to third parties.[101] Though the argument in *Accusearch* is rooted in direct financial injury, similar to other cases brought around the same time,[102] the FTC complaint described more than just financial injury. In fact, the reviewing district court, in its opinion, mentioned non-financial harms to consumers that the FTC had identified, including emotional harm—"sometimes from being stalked or otherwise harassed"—and the indirect financial harms caused by the need to rectify information exposure—"often incurred substantial costs in changing telephone providers."[103] However, Accusearch did not challenge the FTC's substantial injury assessment, so the court's analysis does not directly support the use of non-financial measures of informational injury in unfairness cases.

One other special case is worth mentioning due to the apparently high risk of emotional and reputational injury from sexual privacy exposure. The FTC's case against Craig Brittain for operating a "revenge porn" site included a comparatively large amount of analysis of the substantial injury prong.[104] The FTC mentions a variety of injuries in its analysis of this "revenge porn" site, including reputational harm (others could see the photos by searching for the person's name), potential employment ramifications, and harassment ("some received unwelcome contacts from strangers").[105]

IV. CONCLUSION

Substantial injury is the threshold test to a claim of unfairness. It also represents the most significant element of the "cost" side of a benefit-cost analysis in a consumer protection case. This textual analysis of the Com-

---

100 47 U.S.C. § 222(c)(1). CPNI may only be disclosed "upon affirmative written request by the customer, to any person designated by the customer." 47 U.S.C. § 222(c)(2).

101 FTC v. Accusearch, Inc., No. 06-CV-105, 2007 WL 4356786 (D. Wyo. Sept. 28, 2007), https://www.ftc.gov/sites/default/files/documents/cases/2009/06/090629accusearch10thcirorder.pdf.

102 FTC v. 77 Investigations, Inc., No. EDCV06-0439 VAP (E.D. Cal. May 1, 2006); FTC v. CEO Group, Inc., No. 06-60602 CIV-COHN (S.D. Fla. May 1, 2006); FTC v. Info. Search, Inc., No. 1:06-cv-01099-AMD (D. Md. May 1, 2006); FTC v. Integrity Sec. & Investigation Servs., Inc., No. 206-CV-241-RGD-JEB (E.D. Va. May 3, 2006).

103 *Accusearch*, No. 06-CV-105 at 8–9.

104 Complaint, Craig Brittain, F.T.C. No. 132 3120 (Jan. 8, 2016), https://www.ftc.gov/system/files/documents/cases/160108craigbrittaincmpt.pdf. The FTC included both deception and unfairness claims in this complaint, but the deception claims were only relevant to the subset of posts in which Brittain had directly tricked his victims into sharing their intimate photos.

105 *Id.* at 2.

mission's prior cases shows that consumer privacy injuries are rooted in three factors: (1) the nature of the data at issue—including its sensitivity and quantity, (2) the manner in which data is used (e.g., whether merely collected, paired with other data, or shared with third parties), and (3) the unexpectedness of the data practice, that is, the extent to which consumer expectations are violated by the particular collection or use. Implementing a robust benefit-cost analysis provides the FTC an opportunity to clearly analyze all three of these factors, teasing out which aspects of a company's practice may have caused harm and which were harmless or outweighed by other benefits.

The relative dearth of unfairness cases in the FTC's data privacy cases shows that there is room for an expanded role for unfairness enforcement at the FTC. Unfairness, with its balancing test, has the potential to be a much more precise tool than deception. Such a tool can help to delimit appropriate privacy practices in modern markets driven by emerging technologies—but only if accompanied by robust and transparent benefit-cost analysis that incorporates a modern understanding of consumer perceptions and limitations.

The greatest potential for establishing a robust unfairness test lies in an explicit acknowledgment of the intrinsic value of personal data. The fact that an entity did not sell consumers' personal data in a particular case, but nevertheless violated consumers' established privacy expectations, should not prevent an unfairness case when the value of the data collected, exposed, or shared can in fact be established with reference to the millions of data-fueled transactions taking place every day. Our analysis shows that such factors are not new for the Commission; they simply have not yet been made explicit in public complaints and orders.

A disciplined and robust application of unfairness—along with the requisite benefit-cost analysis—would exemplify FTC enforcement as more empirical, more potent, and vastly more predictable. Such transparent guidance would be invaluable in close cases, particularly when factors of both deception and unfairness are alleged. Without it, companies are left wondering whether eliminating deceptive practices will remove all liability from behavior that was also alleged to be unfair. Benefit-cost analysis that incorporates modern social science principles will provide a robust mechanism for the FTC to determine which trade practices, on balance, are seen by consumers as unfair and harmful.

APPENDIX: TABLE OF DATA PRIVACY UNFAIRNESS CASES

Defendant	Year	Deception	Unfairness
VIZIO, Inc.	2017	x	x
Sequoia One, Inc.	2016		x

General Workings Inc. (Vulcun)	2016	x	x
Craig Brittain	2015	x	x
LeapLab	2014		x
Cornerstone and Company, LLC	2014		x
Bayview Solutions, LLC	2014		x
Aaron's, Inc.	2013		x
Ideal Financial Solutions, Inc., et al.	2013	x	x
DesignerWare, LLC, et al.	2012	x	x
Facebook, Inc.	2011	x	x
Frostwire	2011	x	x
Action Research Group	2007	x	x
Integrity Security & Investigation Services	2006		x
Accusearch (and four related cases)	2006		x
Vision I Properties, LLC	2005		x
Gateway Learning Corp.	2004	x	x
Zachary Keith Hill	2004	x	x
FTC v. Minor	2003	x	x
Smart Data Systems (and two related cases)	2001	x	x
Touch Tone Information	1999	x	x

THE COSTS OF NOT USING DATA: BALANCING PRIVACY AND THE PERILS OF INACTION

Gabe Maldoff[*] *and Omer Tene*[**]

INTRODUCTION

On May 2, 2017, a teenage girl in Macon, Georgia, swallowed a handful of pills, placed a plastic bag over her head, and turned on Facebook Live.[1] Suicide is the second leading cause of death among teens in the United States, and teenage girls are particularly vulnerable.[2] The Georgia teen could have been another statistic, broadcast on Facebook Live for the world to see. But while some critics blame social media for the rise in teen suicides,[3] in this case, the online platform helped save the teen's life. Friends who had seen the broadcast promptly reported it to police. Police also relied on social media to locate the girl (she was at her grandmother's home). Within forty minutes, they were on the scene and the girl was brought to a hospital to recover.

What if the teen's friends had not seen the video and been able to intervene? What if no one was watching? The reality of the online world is that there is always someone—or some*thing*—watching. Entire business models are built around tracking our every move and showing each of us the content best suited to algorithmically determined needs and wants. But, what if Facebook's algorithms had purposefully chosen to bury the livestream below the daily barrage of news stories and cat photos that inundate our feeds? Conversely, if Facebook had the ability to digest the video's content—a growing possibility as voice recognition and machine learning technologies improve—could it have had a duty to intervene?

---

[*] Associate, Bird & Bird, London, formerly Westin Research Fellow, International Association of Privacy Professionals.

[**] Vice President, Research and Education, International Association of Privacy Professionals, and Senior Fellow, Future of Privacy Forum.

[1] *Teen Attempts Suicide on Facebook Live, Saved by Deputies*, USA TODAY (May 5, 2017, 8:01 AM), https://www.usatoday.com/story/news/nation-now/2017/05/04/facebook-live-suicide-attempt-thwarted-deputies/311252001/.

[2] Rae Ellen Bichell, *Suicide Rates Climb In U.S., Especially Among Adolescent Girls*, NPR (Apr. 22, 2016, 12:02 AM), http://www.npr.org/sections/health-shots/2016/04/22/474888854/suicide-rates-climb-in-u-s-especially-among-adolescent-girls.

[3] David D. Luxton, Jennifer D. June & Jonathan M. Fairall, *Social Media and Suicide: A Public Health Perspective*, AM. J. PUB. HEALTH (May 2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3477910/.

The common law has traditionally approached affirmative duties to act cautiously, but in some limited circumstances the law has recognized obligations to act. As data-driven technologies continue to evolve, the boundaries between privacy imperatives, which seek to lock data down, and affirmative data use requirements are beginning to blur. In some circumstances, it will be appropriate to order data users to act.

This article begins, in Part I, by exploring the legal and ethical norms that have caused organizations to limit their use of personal information. In Part II, this article catalogues the increasing number of counter-initiatives, designed to compel data use for the public benefit. Part III explores the emerging concepts of "information fiduciaries" and "digital trust," arguing that these concepts expand beyond the barriers of traditional privacy principles and impose broader duties of care and loyalty, akin to fiduciary and other special relationships. Finally, in Part IV, this article examines the contours of an affirmative duty to use personal information, looking at who could be subject to the duty, who must be protected, and what the duty might require of data users.

I. THE URGE TO LOCK DATA DOWN

The privacy risks of big data, machine learning, and artificial intelligence are well known. Initially, regulatory responses centered on a model of "notice and choice." Notice and choice focused on educating consumers about companies' data practices and binding those companies to their promises.[4] The idea was that informed consumers will choose to provide their personal information only to those companies that implement acceptable data practices, spurring competition for greater privacy protections.[5]

Of course, notice and choice has not always lived up to expectations. In 2013, an exhaustive study of the notice-and-choice model by Omri Ben-Shahar and Carl E. Schneider concluded that the model rested on faulty assumptions about human behavior.[6] Ben-Shahar and Schneider found that rather than actively informing themselves and making rational decisions, consumers generally do not read privacy notices, do not understand them when they do read them, and do not make rational decisions with regard to their privacy protection.[7] One cannot blame consumers—if they were to

---

[4] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7-8 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[5] *Id.* at 7.

[6] Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 651 (2011), https://www.law.upenn.edu/journals/lawreview/articles/volume159/issue3/BenShaharSchneider159U.Pa.L.Rev.647(2011).pdf.

[7] *Id.* at 665.

fully read all the privacy notices they confront online in a year, by some estimates, it would take up to 76 work days.[8]

Some associate the absence of rational consumer decision-making with the low value that consumers place on their privacy.[9] But others point out the abject market failures, information asymmetries, and imbalance of power between individuals and firms, concluding that consumers are "resigned" and emphasizing that notice and choice has not permitted consumers to have genuine control over their data.[10] A study of 248 U.S. privacy notices supports this conclusion, finding that privacy notices "are often silent on a number of important terms, and if they are not, they can be vague and internally contradictory."[11]

Notice and choice also faced a structural challenge. As data collection has become ubiquitous, through smartphones, computers, and the myriad of sensors we encounter in our everyday lives—from smart TVs to smart toasters and lamp posts—providing notice and offering individuals meaningful alternatives has become all but impossible.

In response to these critiques, privacy law and practice shifted its focus to restrictions on the permitted uses of data. The Federal Trade Commission's (FTC) staff report on the "Internet of Things," for example, highlighted the importance of limiting the collection and retention of personal information to what is needed for articulated purposes.[12] The report identified two clear benefits of the so-called "data minimization principle":

> First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.[13]

---

[8] Keith Wagstaff, *You'd Need 76 Days to Read All Your Privacy Policies Each Year*, TIME (Mar. 6, 2012), http://techland.time.com/2012/03/06/youd-need-76-work-days-to-read-all-your-privacy-policies-each-year/.

[9] Gordon Hull, *Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data*, 17 ETHICS & INFO. TECH. 89 (2014).

[10] *See generally* Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation,* Annenberg School for Communication, University of Pennsylvania (Jun. 2015), https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[11] Florencia Marotta-Wurgler, *Does "Notice and Choice" Disclosure Regulation Work? An Empirical Study of Privacy Policies* 30 (2015), https://www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf.

[12] FED. TRADE COMM'N STAFF, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD iv (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[13] *Id.*

Regulators and scholars also increasingly pushed for limitations on use of personal information. They reasoned that a use-based model better addresses the challenges of providing individuals with clear notice and real choice as data is amassed in ways that are not obvious to consumers.[14] In its 2014 Report to the President on Big Data and Privacy, the President's Council of Advisors on Science and Technology (PCAST) highlighted the importance of restricting the use of personal information to what is "acceptable," as determined by context and prevailing social norms.[15] A model based on notice and limitations on collection could not as easily be designed into code and operationalized into technological products. Thus, PCAST's number one recommendation for addressing privacy in the context of big data was: "Policy attention should focus more on the actual *uses* of big data and less on its *collection* and analysis."[16]

The rise of data breach notification laws in the U.S. furthered the aims of data minimization and purpose limitation. By shining a spotlight on data failures, breach notification laws forced organizations to justify the vast stores of personal information they collected.[17] The threat of legal risks exacerbated the reputational risks of data misuse, as courts began to recognize litigants' standing to bring suit for pure privacy harms.[18]

U.S. information privacy norms have not evolved in a vacuum. In 2016, the Australian Department of Health released a data set to researchers that it believed to have been anonymized, but was ultimately used to identify particular doctors and patients.[19] In response, members of Australian Parliament proposed legislation that could make it a crime to disseminate "reidentified" datasets.[20] The government of the United Kingdom proposed a similar measure in August 2017.[21] While the Australian initiative has stalled so far,[22] these legislative measures signaled an increasing awareness

---

14 *See generally* EXEC. OFFICE OF THE PRESIDENT, COUNCIL OF ADVISORS ON SCI. & TECH., REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014), https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

15 *Id.*

16 *Id.* at 49 (emphasis added).

17 SAMUELSON L., TECH. & PUB. POL'Y CLINIC, UNIV. OF CAL.-BERKELEY SCH. OF LAW, *Security Breach Notification Laws: Views from Chief Security Officers* 16 (2007), https://www.law.berkeley.edu/files/cso_study.pdf.

18 *See, e.g.,* Robins v. Spokeo, Inc., 867 F.3d 1108, 1110 (9th Cir. 2017).

19 Paul Farrell, *Research Work Could Be Criminalised Under George Brandis Data Changes*, THE GUARDIAN (Sept. 28, 2016, 11:03 PM), https://www.theguardian.com/world/2016/sep/29/george-brandis-to-criminalise-re-identifying-published-government-data.

20 *Id.*

21 Alex Hern, *New Law Could Criminalise Uncovering Personal Data Abuses, Advocate Warns*, THE GUARDIAN (Aug. 14, 2017, 2:00 AM), https://www.theguardian.com/technology/2017/aug/14/data-protection-bill-criminalise-privacy-research-advocate-warns.

22 Rohan Pearce, *Government Hasn't Given Up on 'Re-Identification' Bill*, COMPUTERWORLD (Aug. 14, 2018, 6:30 AM), https://www.computerworld.com.au/article/645154/government-hasn-t-given-up-re-identification-bill/.

of the risks that exist when personal information is shared without limitations on use.

Developments in Europe, especially as extended to the U.S. through transatlantic privacy arrangements, such as Safe Harbor, Standard Contractual Clauses, and most recently Privacy Shield, also impacted organizations' approaches to the use of personal information. The implementation of the General Data Protection Regulation (GDPR) in the European Union followed this trend. Although based on the same principles as the pre-existing European data protection framework, the GDPR exported those European standard to the U.S. and elsewhere, by explicitly including organizations based anywhere in the world that target European consumers within its territorial scope.[23] Data minimization and purpose limitation were at the core of these updates to the EU framework.[24] These principles found particular expression in the "legitimate interests" balancing test that is set to play an important role in determining lawful uses of personal information. To head off the potential for significant fines on the scale of EU competition law—under which Facebook and Google were fined billions of Euros[25] for data-related competition violations—organizations in the U.S. invested heavily in data compliance.[26]

To be sure, restrictions on use alone, without a concomitant regulation of collection, could amount to a significant deregulation of privacy. While advocates of the use model argued that it is a pragmatic solution to the problem of "data exhaust,"[27] others warned that regulating use alone would allow for the vast accumulation of stockpiles of data, which could become available to overzealous governments or malicious actors.[28] In a prescient example, Chris Hoofnagle pointed out that the Fair Credit Reporting Act of

---

23 EUROPEAN COMMISSION, *What Does the General Data Protection Regulation Govern?* (last visited Nov. 30, 2018), https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en.

24 EUGDPR.ORG, *GDPR Key Changes* (last visited Nov. 30, 2018), https://eugdpr.org/the-regulation/.

25 EUROPEAN COMMISSION, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 27, 2017), http://europa.eu/rapid/press-release_IP-17-1784_en.htm; *see also*, EUROPEAN COMMISSION, Mergers: Commission Fines Facebook €110 Million for Providing Misleading Information about WhatsApp Takeover (May 18, 2017), http://europa.eu/rapid/press-release_IP-17-1369_en.htm.

26 Chris Babel, *The High Costs of GDPR Compliance*, DARKREADING (Jul. 11, 2017, 10:30 AM), https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263 (finding that 83% of U.S. organizations surveyed expected to spend at least $100,000 on GDPR compliance efforts).

27 Craig Mundie, *Privacy Pragmatism*, FOREIGN AFF. (Mar./Apr. 2014), https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism.

28 Chris Jay Hoofnagle, *The Potempkinism of Privacy Pragmatism*, SLATE (Sept. 2, 2014, 8:36 PM), http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html.

1970 (FCRA), a use-based regulation, allowed credit rating agencies to become "large, unaccountable bureaucracies that are notoriously unresponsive to consumers."[29] The dangers of eschewing limits on collection became evident when the credit rating agency, Equifax, announced it was breached in September 2017, exposing the personal information of nearly half of all Americans, many of whom had no knowledge of Equifax's existence.[30] As the example shows, restriction on use, without regulation of collection, can prove counter-productive vast databases are breached and escape controls on use.

Through burgeoning public consciousness of privacy risks, some organizations found reputational benefits in data use limitations. For example, when in 2016, the Federal Bureau of Investigation (FBI) sought Apple's assistance to unlock an iPhone allegedly belonging to one of the terrorists responsible for the San Bernardino attack, Apple refused, citing the risks to privacy.[31] "The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge," Apple CEO, Tim Cook, wrote in an open letter to customers.[32] In days past, one might have expected public opinion to support disclosure in a high-profile terrorism-related investigation.[33] Apple's justification for not assisting the FBI, which relied on the fact that Congress had specifically opted *not* to confer that power upon the government,[34] indicated that enhanced privacy protection could also be good for a company's bottom line.[35]

---

29 *Id.*

30 Lee Matthews, *Equifax Data Breach Impacts 143 Million Americans*, FORBES (Sept. 7, 2017, 10:42 PM), https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#6a4bb720356f.

31 Arju Kharpal, *Apple vs FBI: All You Need to Know*, CNBC (Mar. 29, 2016, 10:54 AM), https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html.

32 Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016) https://www.apple.com/customer-letter/.

33 Lydia Saad, *Americans Generally Comfortable with Patriot Act*, GALLUP (Mar. 2, 2004), http://www.gallup.com/poll/10858/americans-generally-comfortable-patriot-act.aspx.

34 Nancy Gibbs & Lev Grossman, *Here's the Full Transcript of TIME's Interview with Apple CEO Tim Cook*, TIME (Mar. 17, 2016), http://time.com/4261796/tim-cook-transcript/ (speaking of the All Writs Act, Cook said, "And also the act itself doesn't look at the crime, it doesn't look at the reason the government wants it. It looks at the burden to the company that it's asking to do it. So this case was domestic terrorism, but a different court might view that robbery is one. A different once might view that a tax issue is one. A different one might view that a divorce issue would be okay. We saw this huge thing opening and thought, you know, if this is where we're going, somebody should pass a law that makes it very clear what the boundaries are. This thing shouldn't be done court by court by court by court. Particularly looking at the history. The Congress made a conscious decision not to do this. It's not like, oh, this technology is so new, it's never been thought of before. It's not like that. So we saw that being a huge civil liberties slide. We saw us creating a back door—we think it's fundamentally

II. THE RISE OF BIG DATA OBLIGATIONS

As privacy norms and regulation shifted to emphasize limitations on data use, legislators and regulators have been careful to avoid curtailing the most beneficial uses of data. In its January 2017 report, *Privacy in our Digital Lives: Protecting Individuals and Promoting Innovation*, the Obama Administration highlighted the importance of privacy protection for giving individuals the space to develop, interact, and ultimately to innovate free from scrutiny.[36] At the same time, the report recognized that many of the most significant recent innovations, public and private, including the "renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs for the future . . . [were] enabled by novel uses of personal information."[37]

Indeed, privacy laws and norms long promoted this balance by *permitting* the use of personal information for important societal objectives. For example, the Privacy Act of 1974 permitted the use of personal information, without consent, for law enforcement purposes, archival purposes if a record "has sufficient historical or other value to warrant its continued preservation by the United States Government," and even for more mundane but necessary purposes, such as for routine use or other administrative purposes.[38]

The same is true of sectoral federal privacy legislation. The Health Insurance Portability and Accountability Act (HIPAA), which imposed strict obligations on how covered entities may use protected health information, permitted the use of personal information to identify or locate a suspect, fugitive, material witness, or missing person, or to respond to off-site medical emergencies.[39] Likewise, under the Gramm Leach Bliley Act (GLBA), financial institutions were exempt from requirements to provide individuals with notice and a right to opt-out of the sharing of non-public information for the purposes of preventing fraud, responding to judicial process or a subpoena, or complying with federal, state, or local laws.[40] The FTC's regulatory framework, which regulates "unfair" information practices, similar-

---

wrong. And not just wrong from a privacy point of view, but wrong from a public safety point of view."). *Id.*

35 Dana Blankenhorn, *Why Resisting the FBI is Good for Apple Stock?*, AMIGOBULLS (Feb. 22, 2017, 2:52 AM), https://amigobulls.com/articles/why-resisting-the-fbi-is-good-for-apple-stock.

36 THE WHITE HOUSE, PRIVACY IN OUR DIGITAL LIVES: PROTECTING INDIVIDUALS AND PROMOTING INNOVATION 2 (2017), https://epic.org/privacy/Privacy_in_Our_Digital_Lives.pdf.

37 *Id.*

38 5 U.S.C. § 552a.

39 45 C.F.R. § 164.512.

40 15 U.S.C. § 6802.

ly permits a practice if it is "outweighed by countervailing benefits to the consumer or competition."[41]

Even the oldest regulations of personal information recognized the need to permit disclosure in some cases. The common law rule of attorney-client privilege, for example, which dates back to the Elizabethan period in England, is "perhaps, the most sacred of all legally recognized privileges, and its preservation is essential to the just and orderly operation of our legal system."[42] Yet, early English case law recognized the need for the privilege to give way when a communication revealed a client's intention to commit a wrong.[43] For example, in 1743, *Annesley v. Anglesea* held that the privilege did not apply to "a secret, which is contrary to the public good, such as design to commit treason, murder, or perjury"; "a crime"; or "a thing that is 'malum in se,' against the common rules of morality and honesty."[44]

The same approach governs to this day, as reflected in the modern Rules of Professional Conduct.[45] While permissive exceptions to data use limitations have sought to further societal goals, in some cases, mere permission was not enough to achieve desired outcomes. Instead, the law had to recognize a reporting obligation. One striking example derives from the attorney-client relationship. When, at the start of this century, public confidence was shaken by a series of accounting scandals that revealed the deceitful practices of Enron, Tyco, WorldCom, and Parmalat, many wondered how fraud could persist on such a massive scale. Congress turned its attention to the roles of professionals in the scandals. In 2002, Congress passed the Sarbanes-Oxley Act, which, among a series of reforms to corporate and accounting rules sectors, required lawyers to "report evidence of a material violation of the securities laws or a breach of fiduciary duty or similar violation by the company or any of its agents to the chief legal officer or the chief executive officer of the company (or the equivalent thereof)."[46] If the chief legal officer or chief executive officer failed to take appropriate action, a lawyer was required to "report the evidence to the audit committee, another independent committee, or the full board of directors."[47] Just as the Rules of Professional Conduct recognized that lawyers had affirmative du-

---

41 15 U.S.C § 45.

42 United States v. Bauer, 132 F.3d 504, 510 (9th Cir. 1997) (citing Upjohn Co. v. United States, 449 U.S. 383, 389 (1981)).

43 *See generally* Hazard, Geoffrey C. Jr., *An Historical Perspective on the Lawyer-Client Privilege*, YALE L. SCH. (1978), http://digitalcommons.law.yale.edu/fss_papers/2406.

44 *Id.*

45 MODEL RULES OF PROF'L CONDUCT R. 1.6(b) (2017) ("A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary: (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services.").

46 The Sarbanes–Oxley Act of 2002, Pub.L. No. 107–204, 116 Stat. 745 (2002).

47 *Id.*

ties to act on information in their possession, whistleblowers who revealed confidential information were also offered protection.

Around the same time, as part of the USA PATRIOT Act of 2001, Congress imposed requirements on financial institutions to verify the identities of their customers.[48] Although financial privacy laws had already provided exceptions for anti-money laundering purposes,[49] and banks and broker-dealers had been subject to money laundering laws, such as the Bank Secrecy Act of 1970, these had proved ineffective at encouraging financial institutions to share information concerning potential money launderers. The USA PATRIOT Act required financial institutions to follow certain minimum standards in verifying the identities of foreign and domestic customers, despite significant concerns for consumer privacy.[50] These included obtaining sufficient information from would-be customers to identify the ultimate beneficiary of an account-holder, which have been characterized by critics as forcing banks to "spy on their customers."[51] In spite of these privacy concerns, the USA PATRIOT Act nonetheless introduced civil and criminal penalties for institutions that failed to comply.[52]

The disclosure obligations of the USA PATRIOT Act ran counter to deeply-held norms in the financial industry favoring secrecy. It is for this reason that "Know Your Customer" initiatives, which required financial institutions to vet those they do business with, needed to rely on such steep penalties. As organizations have become more accountable for the personal information they collect and use, incentives for using personal information have also arisen in areas not traditionally bound by secrecy. These initiatives have sought to encourage data use for a range of purposes, often where the benefits were less tangible or compelling than in the context of crime and fraud.

One example is the rise of open data initiatives, which have liberated government-held data for research and public transparency purposes, in spite of concerns that personal information could be revealed. Forty-eight states, forty-eight cities and counties, the federal government, and fifty-three other countries have committed themselves to open data principles.[53] These initiatives have driven governments to open their databases in machine-readable formats, sometimes revealing personal information in the

---

48 *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 31 U.S.C. § 5318 (2001).

49 *See generally* The Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2011) *et seq*.; GLBA Privacy Rule, 16 C.F.R. § 313.15.

50 *"Know Your Customer" Rules: Privacy in the Hands of Federal Regulators: Hearing before the S. Comm. on Commercial and Administrative Law*, 106th Cong. 1 (1999) (testimony of Legislative Counsel Gregory Nojeim).

51 *Id.*

52 USA PATRIOT Act §312.

53 *Open Government*, DATA.GOV, https://www.data.gov/open-gov/.

process.[54] Indeed, the effectiveness of open data initiatives at solving endemic problems often depends on providing data that is sufficiently granular to be meaningful to researchers and the public.[55] However, because of the risks inherent in releasing such data, Goroff, Polonetsky, and Tene observed that these initiatives are often bogged down by broad-based privacy and security objections. They claimed that this requires specific measures to salvage data benefits while mitigating the worst of the associated risks.[56]

More recent legislation has aimed to balance these competing interests. In 2015, Congress passed the Cybersecurity Information Sharing Act (CISA) to address the "cyber threat," which President Obama characterized as "one of the most serious economic and national security challenges we face as a nation."[57] CISA aimed to enhance information sharing related to cybersecurity between corporate entities, businesses and the government, and different government agencies.[58] Although information sharing remained voluntary, CISA created incentives for sharing such as immunity from liability for privacy violations and a right to retain privilege for the shared information.[59] CISA also required the federal government to promulgate guidelines to protect privacy while at the same time facilitating monitoring and sharing.[60]

Some in the private sector have also argued that technology companies need to do more to protect the public with the information they possess. In the wake of terrorist attacks in Paris and Brussels, European lawmakers threatened to introduce criminal sanctions for failing to prevent extremism on social networks if these companies would not act voluntarily.[61] In re-

---

54 *See, e.g.,* Latanya Sweeney, *Simple Demographics Often Identify People Uniquely*, CARNEGIE MELLON UNIV. (2000); Anthony Tockar, *Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset,* NEUSTAR RES. (Sept. 15, 2014), https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/.

55 Ben Green et al., *Open Data Privacy*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y RES. AT HARV. U. (2017) https://dash.harvard.edu/bitstream/handle/1/30340010/OpenDataPrivacy.pdf?sequence=5.

56 *See generally* Daniel Goroff, Jules Polonetsky & Omer Tene, *Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data*, 675 ANNALS OF THE AM. ACAD. OF POL. AND SOC. SCI. 46 (2017).

57 THE WHITE HOUSE OFFICE OF THE PRESS SEC'Y, REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE (May 29, 2009), https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

58 Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARVARD L. SCH. FORUM ON CORP. GOVERNANCE AND FIN. REGULATION (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/.

59 *Id.*

60 *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113 (2016).

61 Mark Scott, *Europe Presses American Tech Companies to Tackle Hate Speech*, N.Y. TIMES (Dec. 6, 2016), https://www.nytimes.com/2016/12/06/technology/europe-hate-speech-facebook-google-twitter.html?mcubz=3.

sponse, a number of tech companies, including Google, Facebook, Twitter, and Microsoft, signed a voluntary code of conduct designed to eliminate hate speech online.[62]

Less than a year later, however, those calls were not silenced. After the UK was struck by three terrorist attacks in the spring of 2017, UK Members of Parliament called for imposing stricter measures on these companies to force them to take action.[63] UK Prime Minister Theresa May called on social media companies to develop tools that could automatically identify and remove harmful material based on what it contains and who posted it and tell authorities when harmful material is identified so that action can be taken. In May 2017, this call was echoed by the G7—one of the few points on which all seven members could agree.[64] Forcing further responsibility on tech companies to monitor extremism is notable not just because of the tension it presents with user privacy, but also because it is at odds with the long prevailing legal paradigm online, which absolved intermediaries from liability for content posted by users of their services.[65]

Together these examples weave the fabric of a larger trend across sectors and industries, as well as the public-private divide of increasing regulation surrounding the *use* and the *failure to use* personal information. This trend reflects a broader awareness of the power and centrality of data analysis to modern innovation. It underscores the unease of those who lament the accumulation of vast sums of personal information, which grates against the claim that "too often, data remain[s] locked in corporate coffers weighed down by concerns about individuals' privacy, data security, and re-identification risk, as well as corporate incentives to protect trade secrets and intellectual property and a general inclination to avoid risk by keeping data close."[66] Digital trust will depend on addressing both sets of concerns.

---

62 EUROPEAN COMMISSION, *European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech* (May 31, 2016), http://europa.eu/rapid/press-release_IP-16-1937_en.htm.

63 Anushka Asthana and Sam Levin, *UK Urges Tech Giants to Do More to Prevent Spread of Extremism*, THE GUARDIAN (Aug. 1, 2017, 7:01 PM), https://www.theguardian.com/technology/2017/aug/01/uk-urges-tech-giants-to-do-more-to-prevent-spread-of-extremism.

64 Tom McTague, *G7 Calls on Tech Companies to Tackle Terrorism*, POLITICO (May 26, 2017, 7:05 PM), http://www.politico.eu/article/g7-calls-on-tech-companies-to-tackle-terrorism/.

65 Adam Holland et al., *Intermediary Liability in the United States*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y. AT HARV. U. 1, 6 (Feb 18. 2015), https://publixphere.net/i/noc/page/OI_Case_Study_Intermediary_Liability_in_the_United_States.

66 *See generally* Goroff et al., *supra* note 56.

III. FIDUCIARIES AND DIGITAL TRUST

This article has thus far chronicled two competing trends in the law and ethical norms surrounding the use of personal information. On the one hand, organizations face greater incentives for limiting their use of personal information to protect individual privacy. On the other hand, these same organizations face pressure to do more to act on the information in their possession for public benefit. This dichotomy is not new. Public discourse has long framed privacy regulation as being at odds with security, freedom of speech and innovation. However, a growing body of literature is defining a new conception of privacy, not at odds with innovation, but rather an enabler of it. This new conception of privacy roots the obligations of information-holders in the *trust* of individuals who share their personal information. Here we show that trust compels organizations to not just protect and lock down personal information, but also to use it to protect the public.

A. *Breaking the Impasse*

Privacy is often framed in opposition to the promises of technology. At the World Economic Forum, for example, Klaus Schwab argued that "the possibilities of billions of people connected by mobile devices, with unprecedented processing power, storage capacity, and access to knowledge," were indicators that we are in the midst of a "Fourth Industrial Revolution."[67] Like the three industrial revolutions before it, "it is disrupting almost every industry in every country" and "[t]he speed of current breakthroughs has no historical precedent."[68] While privacy is "[o]ne of the greatest individual challenges posed by new information technologies,"[69] regulating personal information too strictly would hamper the promises of these new technologies.

If we focus on privacy as locking data down, then the conflict between privacy and other societal values is inevitable. There can be no middle ground where privacy calls for restricting data use and innovation calls for data experimentation. In such a paradigm, privacy is "a tax on profits, a drain on innovation, a dangerous and naive assumption, and a burden on the

---

67 Klaus Schwab, *The Fourth Industrial Revolution: What it Means and How to Respond*, WORLD ECON. F. (Jan. 14, 2016), https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

68 *Id.*

69 *Id.*

individual to fend for herself in the digital thicket."[70] Thus, for a conception of privacy to be effective without squandering the opportunity for innovation, it must be fluid enough to enable the promises of data benefits to be fulfilled, without compromising the intangible and essential qualities of privacy—the "inviolate personality."[71] This does not mean that notice and choice, data minimization, and purpose limitation have no place in the regulation of personal information; rather they are only components of broader ethical imperatives that govern the relationship between data users and data subjects. Without consideration of these broader imperatives – without a manageable framework for simultaneously regulating use – privacy regulation is bound to fail.

The risk when talking about the ethics of data use is that actors in the information economy are left with few concrete rules to govern decisions about data uses in practice. But a growing body of literature has begun to anchor these ethical imperatives in the nature of the *relationship* between those who share their personal information and those who use it. For Neil Richards and Woodrow Hartzog, this relationship is characterized as *trust*—"[t]he willingness to accept vulnerability to the actions of others."[72] For Jack Balkin, the relationship takes on a "fiduciary" quality.[73]

These accounts are derived from an awareness of the widening gulf of power between individuals and the organizations that collect their personal information. While privacy discourse has traditionally been framed in individualistic terms—with focus on the individual's ability to *control* and *make choices* about the use of his or her personal information—this conception of privacy does not accord with the way we increasingly interact with the digital world. "In the digital economy," Richards and Hartzog argued, "the real power is not held by individual consumers and citizens using their smartphones and laptops to navigate the twists and turns of their lives . . . [but instead by] the large government and corporate entities who monitor them."[74]

This realization is critical to deciphering the dueling calls for purpose limitation on the one hand and data use imperatives on the other, that seem to grow louder as the market dominance of major data users like Google,

---

[70] Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 434 (2016), https://www-cdn.law.stanford.edu/wp-content/uploads/2017/11/Taking-Trust-Seriously-in-Privacy-Law.pdf.

[71] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. (1890), http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

[72] Richards & Hartzog, *supra* note 70, at 433.

[73] Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016), https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

[74] Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1182 (2016), http://www.yalelawjournal.org/review/privacys-trust-gap-a-review.

Facebook, and Amazon grows.[75] If our experience with the digital economy is characterized by our vulnerability, it follows that the organizations we are vulnerable to owe us an ethical duty not to exploit us or our data. It is this condition which Richards and Hartzog label "trust," and it is from this condition, Balkin argues, that "certain types of online service providers take on fiduciary responsibilities . . . because we trust them with sensitive information."[76]

Richards and Hartzog argued that emphasizing trust allows privacy regulation to move beyond the Fair Information Practices (FIPs) of data minimization and purpose limitation.[77] While these principles cannot be completely brushed aside, they should be "rejuvenated" by emphasizing their role in the larger trust relationship.[78] Thus, "[w]hen viewed through the lens of trust-building[,] the existing FIPs of Confidentiality, Transparency, and Security become the substantive obligations of Discretion, Honesty, and Protection."[79] Most importantly, trust imposes a new obligation on organizations not present in the FIPs: Loyalty.

B. *Loyalty and the Seeds of Action*

Thus far, existing accounts of trust and fiduciary responsibility have focused on preventing the kinds of harms that the privacy literature has long been concerned with. Richards and Hartzog catalogued examples of violations of trust, which included a bank employee leaving account numbers on a laptop in an airport, a search engine turning queries over to the government or the general public, and a retailer guessing someone is pregnant in order to market to her at a time of vulnerability.[80] Brennan-Marquez described the role fiduciary relationships could play in strengthening Fourth Amendment protections.[81] These accounts bear strong resemblances to the privacy harms that continue to be a source of debate in courts around the country, such as fraud, identity theft, embarrassment, vulnerability, and government coercion.[82]

---

75 David McCabe, *The Walls Are Closing in on Tech Giants*, AXIOS (Aug. 18, 2017), https://www.axios.com/the-walls-close-in-on-tech-2473228710.html.

76 Balkin, *supra* note 73, at 1221.

77 Richard & Hartzog, *supra* note 70, at 436.

78 *Id.*

79 Richards & Hartzog, *supra* note 70, at 458.

80 *Id.* at 450.

81 *See generally* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5147&context=flr.

82 Daniel J. Solove and Danielle Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, GWU L. SCH. PUB. L. RESEARCH PAPER NO. 2017-2, 2, 7, 21 (2017), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2499&context=faculty_publications.

However, trust relationships and fiduciary responsibilities also carry the seeds of broader obligations to individuals extending beyond preventing the misuse of personal information. Indeed, trust can be violated as much by the *dis*use of personal information as it can by its *mis*use.

Ethan J. Leib's *Friends as Fiduciaries* is relevant for understanding how fiduciary obligations not only compel individuals and organizations to refrain from taking action that could harm another, but also taking affirmative action to *promote* outcomes in the interest of the beneficiary of a trust relationship.[83] In Leib's example, John and David are old college friends and have shared all their most intimate secrets with one another, including a shared dream they have often discussed of founding an environmentally-friendly beverage company in China together.[84] One day, David was approached by a wealthy acquaintance who was pursuing business opportunities.[85] David, assuming that the dream of establishing a beverage company with John would not come to fruition anytime soon, presented the idea to the acquaintance.[86] They quickly set up the company, without telling John, and it was projected to be hugely profitable.[87] John, of course, only found out later and was furious.[88]

In Leib's example, it is unclear whether David should be held liable to John, but few would disagree that David "betrayed their friendship in selling out their idea"[89]—i.e. that he violated John's trust. On the surface, this story fits into the traditional narrative of the FIPs. According to this telling, David erred in revealing information to a third party that John believed was confidential. To account for the breach of trust as merely a breach of confidentiality, however, would miss the point. Few of us would see it as a betrayal if David had shared their plans with someone with no connections to China and no intention or ability to act on the idea—for example, his retired grandmother. Rather, the betrayal is derived from David benefitting from the shared idea, without including John. Put another way, while the problem could have been avoided had David not disclosed the information, once the opportunity became available, David had an obligation to John to involve him, or at least inform him of the venture. This is supported by John's legal claim (putting aside whether it would prevail), which would focus on the opportunity John lost by *not being involved*, rather than the harm John suffered by having secret information disclosed.

---

83 *See generally* Ethan J. Leib, *Friends as Fiduciaries*, 86 WASH. UNIV. L. REV. 665 (2009), http://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1125&context=law_lawreview.

84 *Id.* at 665-666.

85 *Id.* at 666.

86 *Id.*

87 *Id.*

88 *Id.*

89 *Id.* at 667.

The same principle holds true for online information use. Consumers increasingly understand that their use of "free" services entail fueling those services with their personal information. While consumers are generally comfortable with this bargain, they expect that their information will be protected to certain standards and that organizations' use of personal information will be proportionate to the benefits consumers reap from the free service.[90]

The result is that trust violations can occur when an organization fails to act on information to another's benefit, just as it can when it uses such information to the detriment of another. Consumers feel betrayed not because an organization chooses to use or not to use their personal information, but rather when that choice violates the terms of the basic bargain that sustains their transaction. This bargain is founded on individuals' willingness to accept a degree of vulnerability in exchange for certain services and an expectation of trust and loyalty.

This phenomenon is visible in public reaction to the algorithms that govern social media feeds. From 2006 to 2016, a Twitter user's feed comprised a reverse chronological stream of tweets by the people she followed.[91] But in February 2016, Twitter underwent a radical makeover, borrowing from Facebook's News Feed, and now tweets are displayed in an algorithmically selected hierarchy of relevance.[92] While there was an initial outcry, few, if any, described Twitter's decision as unethical or a violation of trust.[93] Those who were upset mourned the loss of a format they valued, but the change ultimately had little impact on the size of Twitter's user base.[94] The same is true of Instagram's decision to implement an algorithmic feed just months later.[95] Less than one year afterwards, Instagram had experienced record growth.[96]

In contrast to the muted response to Twitter's and Instagram's recent changes, Facebook faced significant backlash when it revealed in 2014 that

---

90 *See generally* Alessandro Acquisti, Curtis Taylor & Liad Wagman, *The Economics of Privacy*, 54 J. ECON. LIT. 442 (2016).

91 Will Oremus, *Twitter's New Order*, SLATE (Mar. 5, 2017, 8:00 PM), http://www.slate.com/articles/technology/cover_story/2017/03/twitter_s_timeline_algorithm_and_its_effect_on_us_explained.html.

92 *Id.*

93 Arjun Kharpal, *#RIPTwitter: User Outrage Over Changes to Tweets*, CNBC (Feb. 8, 2016, 7:00 AM), https://www.cnbc.com/2016/02/08/twitter-users-decry-reported-plan-to-prioritize-tweets.html.

94 Oremus, *supra* note 91.

95 Elle Hunt, *New Algorithm-Driven Instagram Feed Rolled Out to the Dismay of Users*, THE GUARDIAN (June 7, 2016, 12:58 AM), https://www.theguardian.com/technology/2016/jun/07/new-algorithm-driven-instagram-feed-rolled-out-to-the-dismay-of-users.

96 Josh Constine, *Instagram's Growth Speeds Up as it Hits 700 Million Users*, TECHCRUNCH (Apr. 26, 2017), https://techcrunch.com/2017/04/26/instagram-700-million-users/.

it had been experimenting on users' moods.[97] Framed in traditional privacy terms, this result is anomalous. Twitter's and Instagram's transition from "stupid" to "smart" (i.e. data-driven) systems should have triggered an outcry because they used personal information in completely new ways for the services. By contrast, Facebook's experiment was a less dramatic change in the use of personal information. At the time of Facebook's experiment, it already had a personalized feed based on opaque variables tied to personal information. The experiment only slightly tweaked the dials on an already artificial and data-driven system.

Why, then, did the Facebook example result in a more significant backlash? Richards and Hartzog describe this as the "trust gap":

> Missing from the individual view of privacy and security law is the more nuanced understanding that in a connected society, privacy is not just an individual concern, but a major building block for society as a whole. This is privacy's trust gap. Our dominant legal framework is frequently insufficient or incapable of comprehending the real and important injuries to the trust we need to flourish in our networked, digital society.[98]

Reframed as a narrative of trust and loyalty, the seemingly anomalous reactions are predictable. Twitter and Instagram altered their feeds to address the problem of feeds being overwhelmed with information, which impaired the quality of their services.[99] The decision to expand the use of personal information was designed to improve their services for users. Even if some disagreed that the change was an improvement, they had no reason to doubt the motives of these platforms. The platforms also benefitted by driving engagement, and so if users found the service was better, that's part of the deal.

The Facebook study, however, was different. Even if the overall use of data had not changed, the motives of the company apparently had. The experiment was not seen as necessary to improve the service, but rather as an exercise designed to deliberately affect individuals in ways they had not bargained for. In so doing, it violated users' trust. A similar story could be told of the uproar two years later when it was discovered that Facebook's "Trending Topics" was manually curated, and that the curation may have favored stories with left-leaning viewpoints over those that skewed right.[100]

---

97 Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, THE ATLANTIC (June 28, 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/.

98 Richards & Hartzog, *supra* note 74, at 1200-01.

99 *With Instagram's Algorithm Change, Brands Must Double-Down*, ADWEEK (Aug. 10, 2016), http://www.adweek.com/digital/stephan-schambach-newstore-guest-post-instagram-algorithm-change/.

100 Omer Tene & Jules Polonetsky, *Taming the Golem: Challenges of Ethical Algorithmic Decision Making*, 19 N.C.J. OF L. AND TECH. 125, 128 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2981466.

Again, the potential ethical concerns had little to do with whether personal information was used and more to do with the fact that editorial bias could further aims not shared by users and without their knowledge.

Not only is trust agnostic to data action versus inaction, trust obligations in some instances *favor* data action. This is the case when an organization's position of trust compels it to protect the individuals it serves out of a duty of loyalty. In April 2017, for example, when a Cleveland man posted a video to Facebook Live of himself shooting and killing a retiree in the midst of collecting aluminum cans, Facebook was the subject of swift condemnation for failing to remove the video sooner.[101] Experts warned that such violent content could desensitize the public and lead to copycat killings.[102] The backlash was so severe, Mark Zuckerberg acknowledged "if someone's getting hurt, you want to be able to identify what's going to happen and help the right people intervene sooner, and I view that as our responsibility."[103]

This was the recognition of a broader responsibility to *use* an individual's personal information in ways that promote a desired result. In the case of the Cleveland video, Facebook could have prevented the broadcast by doubling down on its systems for analyzing and reporting violent content. Such an effort would require moving to "better artificial intelligence tools to give context of what's going on."[104] Ultimately, this would require deeper analysis of all the content that people post on their social network.[105] These tools, Zuckerberg assured the audience at a software developers' conference, "won't be this year, but I also don't think that's 10 years from now. I do think over a few-year period, this will get better."[106]

As tools built on data analysis continue to improve, the responsibilities of the organizations to use their technology and our personal information in ways that are mutually beneficial will continue to deepen. In Part III, we detailed some of the many ways that legislatures and regulators are increasingly calling on information users to act on the personal information in their possession in the name of security, transparency, and innovation. As the promises of big data, machine learning, and artificial intelligence begin to

---

101 *Facebook Video Killing: Shooting Footage Sparks US Hunt for Suspect*, THE GUARDIAN (Apr. 17, 2017, 4:35 AM), https://www.theguardian.com/us-news/2017/apr/17/facebook-live-killing-cleveland-hunt-suspect.

102 Rick Jervis, *Facebook Live of Chicago Assault Raises Fears of Violence*, USA TODAY (Jan. 7, 2017, 5:41 PM), https://www.usatoday.com/story/news/nation/2017/01/06/chicago-facebook-assault/96254060/.

103 Jessica Guynn, *Zuckerberg: We're Responsible for Halting Violence on Facebook*, USA TODAY (Apr. 18, 2017, 7:13 PM), https://www.usatoday.com/story/tech/news/2017/04/18/mark-zuckerberg-facebook-live-violent-content/100579530/.

104 *Id.*

105 *Id.*

106 *Id.*

materialize, these calls for data action are bound to grow louder. The next section takes a closer look at what these data use imperatives require.

IV. THE CONTOURS OF DATA USE IMPERATIVES

Organizations that collect, use, and analyze personal information owe ethical obligations to the individuals on whose personal information they rely. Those obligations, born out of the relationships of trust between the parties, sometimes compel organizations to use personal information to the benefit of those individuals or the broader public. This section first explores *who* owes affirmative duties to use personal information before discussing *to whom* those duties are owed.

A. *Who Owes Affirmative Duties?*

The literature on information relationships seeks to define which organizations are bound by obligations of trust. As Jack Balkin recognizes, fiduciary obligations "do not apply to everyone. Merely communicating over the Internet does not make [one] an information fiduciary."[107] For Richards and Hartzog, "the law need not face the binary choice of treating information relationships as either 'fiduciary' or 'unprotected.' Surely some middle ground exists between these two extremes."[108]

In information relationships, trust is defined by the willingness to become vulnerable to another—whether a person or organization—by disclosing personal information. While "[v]irtually every disclosure of personal information in the modern age leaves the discloser vulnerable in some way, if even only incrementally," the scope of trust obligations will depend on the degree to which individuals are vulnerable to the data collector.[109]

First, as the scope of the trust relationship will dictate the extent of an information-holder's duties to individuals, the more vulnerable the individual to the information-holder—the more the individual *trusts* that information-holder—the more likely it is that affirmative duties will apply. In this way, affirmative duties differ from existing privacy norms. With privacy, a consumer has the right to expect that any organization that collects her personal information will provide notice and choice, and keep the information confidential. With affirmative duties of trust, the consumer may place a different degree of trust in a start-up whose service she is using for the first time than in an organization with whom she has shared years' worth of data. The consumer might be skeptical when a new mapping ap-

---

107 Balkin, *supra* note 73, at 1225.

108 Richards & Hartzog, *supra* note 70, at 458.

109 *Id.* at 451.

plication proposes a route that defies common sense, but when Google Maps does it, and the consumer has relied on Google Maps many times before, she might be more inclined to follow the unexpected directions.[110]

Second, affirmative duties also depend on the degree to which an organization has the ability to bring about some desired result. Imagine, for example, that a hurricane has ravaged the coastal portion of a state. Authorities want to be able to determine where the worst damage has occurred so they can focus their efforts on rescuing those most likely to be in severe danger. They approach two tech companies for help. Company A is one of the largest companies in the world, with unparalleled visibility through its platforms into users' browsing habits and the way they engage with each other. Company B offers a new fitness-tracking app, which is used primarily by runners and tracks health metrics in order to offer users running and dietary recommendations. Both have the ability to track the location of their users and the information they collect *might* hold clues as to where individuals face the greatest danger.

Does either company have an ethical obligation to assist? Company A is very likely to hold information that could be useful. By understanding how its users are engaging, for example, by analyzing photos they post, Company A could easily identify areas which are badly hit. For Company B, however, it is far from obvious that the data it holds will actually be useful, even though it is potentially more personal and sensitive than the data held by Company A since it includes data about health. To the extent that users trust Company B with such sensitive data, that trust is not likely to extend to a broader duty to protect users from the effects of a hurricane. In contrast, Company A *could* face such a duty. If, for example, it had a feed with trending topics, and users' posts indicating danger was trending in particular regions—they might even include overt calls for help—those users might expect that their calls for help would be answered.

A third criterion for determining when affirmative duties apply is whether the organization in fact has the knowledge required to take the desired action. Where a service acts merely as an intermediary, and the service-provider does not monitor meaningful content of its users, affirmative duties will not attach. In the example above, if Company A is blind to the posts of its users, it cannot be ethically bound to act.

But few data organizations are in fact blind to their users. Facebook's mood experiment was startling not just because of what Facebook had actually done to the unknowing participants, but also because it revealed what Facebook was *capable* of doing. Critics warned it could even rig an elec-

---

[110] Danny Sullivan, *Attorney in Google Maps Lawsuit: It Was Dark; She Thought Google Was Leading Her to Sidewalk*, SEARCH ENGINE LAND (Jun. 1, 2010, 7:21 PM), http://searchengineland.com/attorney-in-google-maps-lawsuit-43349.

tion.[111] Indeed, as revealed by the Cambridge Analytica story that emerged after the Brexit referendum and the election of Donald Trump,[112] digital platforms have immense capacity to potentially manipulate users.

Some believe that Facebook uses mood as an integral component of its ad-serving algorithm, potentially targeting teens that feel "insecure" or "worthless."[113] Going back to the story of teen suicide at the start of this article, if Facebook in fact had a repository of information on vulnerable teens, as these critics claimed, would that change the analysis? It may be that companies should not mine information on vulnerability to begin with, but if they nonetheless do, then that information must also be used more broadly than just to serve corporate interests. The loyalty such organizations owe their users extend to sharing important insights with them—or taking affirmative action when a user is in peril.

Even if an organization's business model is not dependent on advertising, it is nonetheless likely to collect and analyze personal information in order to improve the service. For example, the same logic that required payment service providers to prevent and block fraudulent transactions, also forced intermediaries in the sharing economy, such as Uber and Airbnb, to face intense public pressure to investigate drivers in order to prevent crimes from occurring in cars,[114] and to use the ethnicity of home letters to promote equal opportunities.[115] Consumers even demand greater data use to promote mundane improvements of services they use, such as Netflix, to provide recommendations that are sufficiently tailored to an individual's interests.[116]

Such seemingly benign data frequently reveals important insights when put through the meat grinder of big data analytics.[117] As analytic tools spew out more granular learning about users and groups, these organizations could also owe duties to act in order to protect individuals or to promote important societal interests.

---

111 Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (Jun. 2, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering.

112 Ian Sherr, *Facebook, Cambridge Analytica and Data Mining: What You Need to Now*, CNET (Apr. 18, 2018, 5:10 PM), https://www.cnet.com/news/facebook-cambridge-analytica-data-mining-and-trump-what-you-need-to-know/.

113 Sam Levin, *Facebook Told Advertisers it can Identify Teens Feeling 'Insecure' and 'Worthless'*, THE GUARDIAN (May 1, 2014, 3:01 PM), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

114 Dara Kerr, *How Risky is Your Uber Ride?,Maybe More Than You Think*, CNET (Oct. 8, 2014), https://www.cnet.com/uk/news/how-risky-is-your-uber-ride-maybe-more-than-you-think/.

115 Logan Koepke, *Airbnb, While Pledging to Combat Discrimination, Insulates Itself From Legal Pressure To Do Just That*, MEDIUM (Jun. 23, 2016), https://medium.com/equal-future/airbnb-while-pledging-to-combat-discrimination-insulates-itself-from-legal-pressure-to-do-just-e7c1098ae00.

116 *Why Do Netflix's Recommendations Suck So Bad?*, QUORA (Oct. 17, 2016), https://www.quora.com/Why-do-Netflixs-recommendations-suck-so-bad.

117 *We Experiment on Human Beings! (So Does Everyone Else.)*, OKCUPID (Jul. 28, 2014), https://hackerfall.com/story/we-experiment-on-human-beings.

B. *To Whom Is The Duty Owed?*

When one individual reveals personal information to another, and thereby renders herself vulnerable to that other person (or organization), ethical responsibilities attach, which include responsibilities to take affirmative action when necessary to promote the individual's well being. The relationship of trust between the parties compels the recipient of that trust to act out of loyalty to the beneficiary.[118] But could such a relationship also create ethical responsibilities to others? How about to the public at large?

Tort law provides helpful signposts to unpack to whom users of data could owe affirmative duties. The law of negligence imposes a nearly pervasive duty on individuals to act with reasonable care regarding other persons and their property. Where an individual violates this basic premise, and that violation is the proximate cause of harm to another, the law usually provides a remedy for the injured party. With few exceptions, reasonableness is not defined in advance or formally made apparent to would-be tortfeasors. In this way, negligence law serves as "a massive formal system of second-guessing, of Monday-morning quarterbacking" characterized by "the breadth of human activities it is prepared to formally second-guess."[119]

Yet, an axiomatic feature of American tort law is that individuals usually have no duty to act affirmatively to prevent harm. The duty to take affirmative action to prevent harm occurs only in exceptional cases, where a "special relationship" exists between the actor and the person to be protected. These special relationships come in a variety of forms, such as where a formal relationship exists between the two parties, as in the case of employers and employees and parents and children, or when the conduct of one party causes danger to the other.

As discussed above, the act of providing one's personal information to an organization and making oneself vulnerable to that organization can create "information relationships" that impose affirmative duties. To be sure, we do not argue that all information relationships impose *legal* duties for failing to act. While there may be circumstances where it would be appropriate to assign liability for failing to act, in particular where such a failure proximately causes cognizable harm to individuals, we instead refer to tort liability to inform the outlines of broader ethical and regulatory obligations.

Drawing on the law of special relationships, the duty to take data action applies most firmly where the action would benefit the same individual who provided her data. For example, when pharmaceutical companies con-

---

118 Richards & Hartzog, *supra* note 70, at 468.

119 Marin Roger Scordato, *Understanding the Absence of a Duty to Reasonably Rescue in American Tort Law*, 82 TUL. L. REV. 1447, 1458 (2008), http://scholarship.law.edu/cgi/viewcontent.cgi?article=1045&context=scholar.

duct longitudinal studies on the effects of their drugs, they generally must do so using de-identified data to protect the individuals participating in the study.[120] However, such companies could face legal *requirements* to re-identify individuals if they uncover dangerous trends in the data.[121]

In the example of the fitness app, imagine the app uses artificial intelligence to learn about its users and provide customized training, health, and dietary advice based on information it collects—heart rate and other body metrics—through highly tuned sensors. In that situation, if the app detected something abnormal in one of its regular users, and if it had previously correlated such abnormalities with the onset of a dangerous health condition, then the app could have an obligation to act on that information to prevent the reasonably likely harm. It could, in other words, have responsibility to inform the individual about the risk.

The obligation would also extend to other users of the service. Data driven services rarely compartmentalize the data of individual users. Indeed, the power of such services to make meaningful correlations only exists through the large-scale analysis of trends. In the same example as above, the app's ability to correlate an abnormality with a certain condition depends on the input of *all* its users. The same information that the app could use to inform a runner of her risk of a condition would in fact derive from the personal information supplied by others. Without the ability to make such a correlation, it could not possibly owe a duty towards the individual to act. Thus, distinguishing whether an organization owes a duty to use an individual's personal information only for that same individual's benefit, or whether the duty applies more broadly to *any* individual who has supplied personal information, is difficult. Where a service provider aggregates the information of its various users to derive insights, all of its users could be owed a duty to act.

Consequently, the largest service providers, with millions of regular users, may owe affirmative duties to the public at large. These duties include: taking action by alerting individuals, disclosing personal information to friends or authorities to prevent harm (as in the examples above), and permitting users to share the benefits of their data use. This article has been critical of Facebook's mood experiment for using personal information without notifying individuals in a way that did not equally share the benefits with users. But the study that resulted from the experiment, which has been cited more than 900 times, has contributed to scientific knowledge on emotional contagion and has produced robust debate around the parameters

---

120 Katherine Tucker et al., *Protecting Patient Privacy When Sharing Patient-Level Data From Clinical Trials,* 16 BMC MED. RES. METHODOLOGY 5, 7 (2016), https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-016-0169-4.

121 *Id.*

of ethical research in the age of big data.[122] We do not suggest that publication cured the deficiencies of the study. However, once the study had taken place, it was far better to inform the public of the insights and share the benefits of the knowledge than to retain them for purely private use. We therefore suggest that where an organization's analysis of personal information reveals important insights that would promote the general welfare, that organization may owe a duty to share the insights with those who contributed their personal information to the analysis.

The same principle may require an organization to conduct further analysis of personal information if it knows it is highly likely that the analysis would prevent specific harms and the analysis is of the type the providers of information might expect. Thus, an organization that holds data it knows would be useful in preventing the spread of an epidemic or assisting potential victims of a natural disaster may have obligations to use the data in beneficial ways.

In limited circumstances, affirmative duties could also extend to protecting non-users and the public at large. In *Tarasoff v. Regents of the University of California*, the Supreme Court of California held that a mental health professional owes a duty not only to her patient, but also to known members of the public.[123] The Court reasoned, relying on previous case law, that "by entering into a doctor-patient relationship the therapist becomes sufficiently involved to assume some responsibility for the safety, not only of the patient himself, but also of any third person whom the doctor knows to be threatened by the patient."[124]

Central to the ruling in *Tarasoff* was the fact that the professional could identify the particular victim.[125] The disclosure of confidential information in the course of a "special relationship" thereby created a duty for the professional to warn a victim identified as a result of that relationship. The necessity of having identifiable victims limits the applicability of affirmative duties to the public at large. However, in some cases, it is possible that specific members of the broader public could become known to service providers.

For example, consider a situation where a user makes persistent death threats on a forum monitored by an administrator about a specific individual who is not a member of that forum. This situation would differ from *Tarasoff* if the forum administrator had no way of assessing whether the threats are credible. But if the forum builds detailed profiles about its users

---

122 *See generally* Adam D.I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-scale Emotional Contagion Through Social Networks*, PROC. OF THE NAT'L ACAD. OF SCI. OF THE U.S. OF AM. (Mar. 25, 2014), http://www.pnas.org/content/111/24/8788.full.

123 Tarasoff v. Regents of the Univ. of Cal., 17 Cal. 3d 425, 436, 439 (Cal. 1976).

124 *Id.* at 437 (citing Fleming & Maximov, *The Patient or His Victim: The Therapist's Dilemma* 62 Cal. L. Rev. 1025, 1030 (1974)).

125 *Id.* at 439.

which it uses for advertising purposes, including collecting data from other sources, and it has assessed the individual making the threat as being dangerous or a prior felon, then we might expect the forum to take some affirmative steps to prevent the threats from coming to fruition.

Of course, the scope of such a duty would depend on the ability of the organization to accurately predict that some harm might occur. The court recognized this in *Tarasoff*, but nonetheless concluded that "that professional inaccuracy in predicting violence cannot negate the therapist's duty to protect the threatened victim."[126] While acceptance of the *Tarasoff* rule has not been uniform, twenty-nine states have since adopted rules mandating mental health professionals to report serious threats, and sixteen others provide for permissive reporting.[127] This represents the understanding that as medical science improves, medical professionals can be held to higher standards that may require them to predict and act to prevent harm to identified victims.[128] Likewise, as the fields of analytics, machine learning, and artificial intelligence continue to improve, they too may be held to a higher standard.

CONCLUSION

Privacy law has historically focused on placing limits on the collection of personal information. However, as the tools for data analysis have improved and with them the variety of insights and inferences that can be drawn, how data is used after it is collected requires greater regulatory attention. A new body of scholarship, centered on the roles of information fiduciaries, is beginning to articulate the norms of appropriate data use. While data use regulation may be viewed through the traditional privacy law lens of individual control, this article argued that increasing regulation of data use could create imperatives to *use* data for beneficial effects, rather than just locking it down. Indeed, to foster and maintain the trust of their subjects from whom they collect data, organizations may be expected to act on information in their possession to protect those that entrusted them with their personal information.

The ever-increasing demands and expectations being placed on today's online platforms is a case in point. In the wake of a number of horrific incidents involving Facebook Live, many called on Facebook to take

---

126 *Id.*

127 Mark A. Rothstein, *Tarasoff Duties after Newtown*, 42 J. OF L., MED. AND ETHICS 104, 106 (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324955.

128 John T. Monahan, *Tarasoff at Thirty: How Developments in Science and Policy Shape the Common Law*, UNIV. OF VA. L. SCH. 514, 519 (2007), http://law.bepress.com/cgi/viewcontent.cgi?article=1101&context=uvalwps.

on a more proactive role in regulating the content posted in live videos.[129] Facebook responded by recognizing its "responsibility" to act to protect other users and the public. It has done so by committing to devote more resources to screening offensive content, which superficially clashes with traditional privacy values of notice and choice and purpose limitation. In the case of suicide attempts, Facebook took the affirmative step of instituting a suicide prevention regime that no longer relies exclusively on friends within an individual's network to uncover warning signs.[130] Its efforts follow research suggesting that artificial intelligence is getting better at detecting suicidal tendencies than trained psychiatrists.[131]

Facebook's new programs, and the public pressure that led to them, signal a growing understanding, both within organizations and in the public at large, that obligations to protect information in cyberspace include obligations to protect individuals in the physical world as well. As data-reliant technologies continue to improve, the scope of reasonable care and loyalty to data subjects will come into greater conflict with privacy and data protection norms that emphasize the minimization of data collection and restrictions on its subsequent use. Preserving digital trust will depend not just on protecting data, but also using data to protect those who are vulnerable.

---

129 Samuel Gibbs, *Facebook Under Pressure After Man Livestreams Killing of His daughter*, THE GUARDIAN (Apr. 25, 2017, 11:38 PM), https://www.theguardian.com/technology/2017/apr/25/facebook-thailand-man-livestreams-killing-daughter.

130 Felicity Morse, *Facebook Adds New Suicide Prevention Tool in the UK*, BBC (Feb. 19, 2017), http://www.bbc.co.uk/newsbeat/article/35608276/facebook-adds-new-suicide-prevention-tool-in-the-uk.

131 Megan Molteni, *Artificial Intelligence is Learning to Predict and Prevent Suicide*, WIRED (Mar. 17, 2017, 7:00 AM), https://www.wired.com/2017/03/artificial-intelligence-learning-predict-prevent-suicide/.

WHEN "REASONABLE" ISN'T: THE FTC'S STANDARDLESS DATA SECURITY STANDARD

Geoffrey A. Manne and Kristian Stout[*]

INTRODUCTION

Although the Federal Trade Commission (FTC) is well staffed with highly skilled economists, its approach to data security is disappointingly light on economic analysis. The unfortunate result of this lacuna is an approach to these complex issues lacking in analytical rigor and the humility borne of analysis grounded in sound economics. In particular, the Commission's "reasonableness" approach to assessing whether data security practices are unfair under Section 5 of the FTC Act[1] lacks all but the most superficial trappings of the well-established law and economics of torts, from which the concept is borrowed.

The mere *label* of reasonableness and the *claimed* cost-benefit analysis by which it is assessed are insufficient to meet the standards of rigor demanded by those concepts. Consider this example: in 2016 the Commission posted on its website an FTC staff encomium to "the process-based approach [to data security] that the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency's educational messages to companies."[2] The staff write:

> From the outset, the FTC has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one's security program and defenses. *For that reason, the touchstone of the FTC's approach to data security has been reasonableness* – that is, a company's data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors. Moreover, the FTC's cases focus on whether the company has undertaken a reasonable process to secure data.[3]

---

[*] Geoffrey A. Manne is the founder and president of the International Center for Law & Economics ("ICLE"), a nonprofit, nonpartisan research center based in Portland, OR. Kristian Stout is Associate Director at ICLE. The ideas expressed here are the authors' own and do not necessarily reflect the views of ICLE's advisors, affiliates, or supporters.

[1] 15 U.S.C. § 45 (2006).

[2] Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N: BUSINESS BLOG (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

[3] *Id.* *See also* FED. TRADE COMM'N, COMMISSION STATEMENT MARKING THE FTC'S 50TH DATA SECURITY SETTLEMENT 1 (2014),

In its *LabMD* opinion, the Commission describes this approach as "cost-benefit analysis."[4] But simply listing out some costs and benefits is not the same thing as *analyzing* them. Recognizing that tradeoffs exist is a good start, but it is not a sufficient end, and "reasonableness"—if it is to be anything other than the mercurial preference of three FTC commissioners—must contain analytical content.

A few examples from the staff posting illustrate the point:

> In its action against Twitter, Inc., the FTC alleged that the company gave almost all of its employees administrative control over Twitter's system. According to the FTC's complaint, by providing administrative access to so many employees, Twitter *increased the risk that a compromise of any of its employees' credentials could result in a serious breach*. This principle comports with the [NIST] Framework's guidance about managing access permissions, incorporating the principles of least privilege and separation of duties.[5]

Twitter's conduct is described as having "increased the risk" of breach.[6] In this example even a *recitation* of the benefits is missing. But regardless, the extent of increased risk sufficient to support liability, the cost of refraining from the conduct, and any indication of how to quantify and weigh the costs and benefits is absent. Having disclaimed a belief in "perfect data security,"[7] the staff, wittingly or not, effectively identifies actionable conduct as virtually *any* conduct, because virtually any decision can "increase the risk" above a theoretical baseline. Crucially, this extends not only to actual security decisions, but also to decisions regarding the amount and type of regular business practices that involve any amount of collection, storage, or use of data.

In another example, the staff write, "Likewise, in Franklin's Budget Car Sales, Inc., the FTC alleged that the company didn't inspect outgoing Internet transmissions to identify unauthorized disclosures of personal information. *Had these companies used tools to monitor activity on their networks, they could have reduced the risk of a data compromise or its breadth*."[8]

Can "reasonable" data security require firms to do *anything* that "could have reduced the risk" of breach? Again that means that virtually no conduct need be sufficient, because there is almost always *something* that could further reduce risk—including limiting the scope or amount of nor-

---

https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf [hereinafter COMMISSION STATEMENT] (emphasis added).

4 LabMD, Inc., Docket No. C-9357 at 11 (F.T.C. July 29, 2016) [hereinafter FTC LabMD Opinion], overruled by LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018).

5 Arias, *supra* note 2 (emphasis added).

6 *Id.*

7 *Id.*

8 *Id.* (emphasis added).

mal business activity; surely it reduces the "risk" of breach to, for instance, significantly limit the number of customers, eschew the use of computers, and conduct all business in a single, fortified location.

But of course, "reasonable" data security can't really require these extremes. But such unyielding uncertainty over its contours means that companies may be required to accept the reality that, no matter what they do *short* of the extremes, liability is possible. Worse, there is no way reliably to judge whether conduct–short of obvious fringe cases–is even *likely* to increase liability risk.

The FTC's recent *LabMD* case[9] highlights the scope of the problem and the lack of economic analytical rigor endemic to the FTC's purported data security standard. To be sure, other factors also contribute to the lack of certainty and sufficient rigor–*i.e.*, matters of process at the agency–but at its root is a "standardless" standard, masquerading as an economic framework.[10] LabMD, a small diagnostics laboratory, was (up until the FTC got involved) in the business of providing cancer-screening services to patients.[11] As part of this business—and as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations—LabMD retained patient data, including personally identifiable information (PII).[12] In 2008, Tiversa, a "cyberintelligence" company that employed custom algorithms to exploit peer-to-peer (P2P) network vulnerabilities, downloaded from the computer of a LabMD employee a file, dubbed the "1718 file," that contained PII of approximately 9,300 LabMD patients.[13] Shortly thereafter, Tiversa engaged in what LabMD has characterized (in our opinion, fairly) as a shakedown to induce LabMD to pay Tiversa for "remediation" services.[14] LabMD refused and fixed the P2P vulnerability itself.[15]

Following some fairly questionable interactions between the FTC and Tiversa,[16] LabMD came under investigation by the agency for over three years. In its enforcement complaint the FTC ultimately alleged two sepa-

---

9 *See generally* FTC LabMD Opinion, *supra* note 4.

10 *See, e.g.,* Maureen K. Ohlhausen, *Opening Keynote at the ABA Consumer Protection Conference* 2-3, FED. TRADE COMM'N (Feb. 2, 2017), https://www.ftc.gov/system/files/documents/public_statements/1069803/mko_aba_consumer_protection_conference.pdf.

11 Allison Frankel, *There's a Big Problem for the FTC Lurking in the 11th Circuit's LabMD Data-Security Ruling*, REUTERS (Jun. 7, 2018, 4:26 PM), https://www.reuters.com/article/us-otc-labmd/theres-a-big-problem-for-the-ftc-lurking-in-11th-circuits-labmd-data-security-ruling-idUSKCN1J32S2.

12 Brief of Petitioner at 2, LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (No. 16-16270) [hereinafter LabMD 11th Cir. Petitioner Brief].

13 *Id.* at 3.

14 *Id.* at 3.

15 *Id.* at 2-3.

16 *See* STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 113TH CONG., *Tiversa, Inc.: White Knight or Hi-Tech Protection Racket?* 5-7 (Jan. 2, 2015).

rate security incidents: the downloading of the 1718 file by Tiversa, and the mysterious exposure of a cache of "day sheets" allegedly originating from LabMD and discovered in Sacramento, CA.[17] The FTC alleged that each incident was caused by LabMD's "failure to employ 'reasonable and appropriate' measures to prevent unauthorized access to personal data," and "caused, or is likely to cause, substantial harm to consumers . . . constitut[ing] an unfair practice under Section 5(a) of the Federal Trade Commission Act . . . ."[18]

The FTC brought the complaint before one of its administrative law judge (ALJ), who ruled against the Commission in his initial determination, holding, among other things, that the term "likely" means "having a high probability of occurring or being true," and that the FTC failed to demonstrate that LabMD's conduct had a high probability of injuring consumers.[19] The ALJ put down a critical marker in the case, one that gave some definition to the FTC's data security standard by demarcating those instances in which the Commission may exercise its authority to prevent harms that are *actually* likely to occur from those that are purely speculative.

Unsurprisingly, the FTC voted to overturn the ALJ's decision in LabMD, finding, among other things:

> 1. That "a practice may be [likely to cause substantial injury] if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low;"
>
> 2. That the FTC established that LabMD's conduct in fact "caused or was likely to cause" injury as required by Section 5(n) of the FTC Act;
>
> 3. That substantiality "does not require precise quantification. What is important is obtaining an overall understanding of the level of risk and harm to which consumers are exposed;" and
>
> 4. That "the analysis the Commission has consistently employed in its data security actions, which is encapsulated in the concept of 'reasonable' data security" encompasses the "cost-benefit analysis" required by the Act's unfairness test.[20]

In actuality, however, the Commission's manufactured "reasonableness" standard—which, as its name suggests, purports to evaluate data security practices under a negligence-like framework—actually amounts in

---

[17] Initial Decision at 2, *In re* LabMD Inc., 160 F.T.C. No. 9357, 2015 WL 7575033 (Nov. 13, 2015) [hereinafter ALJ LabMD Initial Decision].

[18] Brief of Complainant at 5, LabMD, Inc., 160 F.T.C. No. 9357, 2015 WL 7575033 (Nov. 13, 2015) [hereinafter FTC Complainant Brief].

[19] ALJ LabMD Initial Decision, *supra* note 17, at 42 (The day sheets were ultimately excluded from evidence because the FTC couldn't prove whether the documents had ever been digital records, nor could it prove how the day sheets made their way out of LabMD and to Sacramento.).

[20] FTC LabMD Opinion, *supra* note 4, at 10-11

effect to a rule of strict liability for any company that collects personally identifiable data.

When LabMD appealed the case to the Eleventh Circuit, the court ruled against the FTC.[21] The opinion does not address most of the problems we identify in this article, which thus remain problems, uncorrected (as yet) by the courts. But it does nicely reinforce a core underpinning of our analysis, the common law negligence basis of the requisite analysis under the Commission's Section 5 unfairness authority, and thus the apparent applicability of our broader arguments:

> The Commission must find the standards of unfairness it enforces in "clear and well-established" policies that are expressed in the Constitution, statutes, or the common law. The Commission's decision in this case does not explicitly cite the source of the standard of unfairness it used in holding that LabMD's failure to implement and maintain a reasonably designed data-security program constituted an unfair act or practice. It is apparent to us, though, that the source is the common law of negligence.[22]

The court ultimately declined to explore the contours of how a proper negligence-like analysis would apply to the Commission's Section 5 unfairness authority.[23] Yet, in oral arguments, as noted below, the court suggested that multiple deficiencies exist in the Commission's Section 5 data security enforcement when viewed through a negligence lens.[24] This article explores these and other defects in the FTC's LabMD decision and its approach to data security enforcement under Section 5 more generally.

I. THE INHERENT AMBIGUITY OF "REASONABLE" DATA SECURITY, PARTICULARLY AT THE FTC

There is a great deal of ambiguity about how the law should treat data and data breaches.[25] Within antitrust, for instance, there is a movement to incorporate firms' collection and use of data into standard merger and conduct analyses.[26] But in this context, it remains unclear how, and whether, to

---

21 *See* LabMD, Inc., 894 F.3d at 1237.

22 *Id.* at 1231.

23 The court described the Commission's actions as relying upon negligence law, but, in order to reach its holding, simply assumed that its negligence-like analysis was broadly correct, and limited its analysis to the appropriateness of the Commission's particular remedy sought in light of the harms alleged. *Id.*

24 *See, e.g., infra*, note 24 and accompanying text.

25 *See generally* D. Daniel Sokol & Roisin E. Comerford, *Does Antitrust Have a Role to Play in Regulating Big Data?*, CAMBRIDGE HANDBOOK OF ANTITRUST, INTELLECTUAL PROPERTY AND HIGH TECH 293 (Roger D. Blair & D. Daniel Sokol eds., 2017).

26 *See, e.g.*, ALLEN P. GRUNES AND MAURICE E. STUCKE, BIG DATA AND COMPETITION POLICY 69 (2016).

do so.[27] The ways in which firms collect and use data are plausibly relevant components of non-price competition, but non-price components, like reputation, are notoriously difficult to quantify, and especially difficult with respect to data because consumers have heterogeneous risk and privacy preferences when it comes to the collection and use of information about themselves.[28] So, too, data *security* practices can contribute to the perceived value of a product or service from the consumer perspective, but quantifying that value with any degree of precision is difficult, if not impossible.

Similarly, when there is a data breach, the calculation of the extent of harm, if any, to consumers is difficult to measure. This is complicated, of course, by the fact that, even assuming that particularized harm can be accurately assessed, that harm needs to be balanced against the benefits conferred by decisions within the firm to optimize a product or service for lower prices or in favor of other consumer-valued features, such as ease-of-use, performance, and so forth.

Additionally, some, including the FTC, have asserted that exposure of information is, in and of itself, a harm to individuals, apart from any economic consequences. In the FTC's *LabMD* opinion, for instance, the Commission asserted that:

> the disclosure of sensitive health or medical information [that] causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n). For instance . . . disclosure of the mere fact that medical tests were performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm."[29]

Legally, data security issues are addressed through either, or both, of two categories of law: public law, by regulatory agencies enforcing consumer protection statutes or provisions, and private law, typically by private litigants asserting tort claims like negligence and trespass, as well as contract and fraud claims.

The FTC—obviously a consumer protection agency engaged in the enforcement of public law—nevertheless evinces a curious pattern of enforcement that seems to uneasily mix nominal principles derived from the common law of torts with an asserted authority under Section 5 largely unbounded by precedent, strict adherence to statutory language, or common law principles.

---

[27] *See generally* Geoffrey A. Manne and R. Ben Sperry, *The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework*, CPI ANTITRUST CHRON. (2015), https://www.competitionpolicyinternational.com/assets/Uploads/ManneSperryMay-152.pdf.

[28] *See* James C. Cooper*, Privacy and Antitrust: Underpants Gnomes, The First Amendment, and Subjectivity*, 20 GEO. MASON L. REV. 1129 (2013).

[29] FTC LabMD Opinion, *supra* note 4, at 17.

The Eleventh Circuit, in fact, took note of the problematic "heads I win, tails you lose" character of this interpretation of Section 5 during oral argument in LabMD's appeal from the FTC *LabMD* opinion:

> Judge Robreno: [T]here is a difference between tort law . . . [in] the common law application in a government . . . rule as to what is reasonable and not reasonable. I think that's the essence . . . it seems to me, of what you're saying, is that on limited license to figure out what is reasonable and unreasonable in the economy. And the [C]ommissioners will sit around and decide what is reasonable and I don't believe that's a good public policy objective.
>
> FTC: Well I believe that's exactly what Congress intended when . . . .
>
> Judge Tjoflat: [E]very time something happens, which heretofore was thought to be reasonable in the industry, say, all of a sudden becomes unreasonable because in hindsight you realize, well, this could have been avoided . . . .
>
> FTC: The Commission doesn't act in terms of hindsight. The Commission acted here in terms of what was reasonable at the time . . . .
>
> Judge Tjoflat: I'm talking about your just plain unreasonable standard.
>
> FTC: It's certainly true that something that could be reasonable today might not be reasonable tomorrow.
>
> Judge Wilson: Doesn't that underscore the importance of or the significance of rulemaking? Otherwise, you're regulating data security on a case-by-case basis . . . .
>
> FTC: We are regulating data security on a case-by-case basis, and that's exactly what the Supreme Court says in *Bell Atlantic* and *Chenery*, that the agency is entitled to do . . . .
>
> Judge Tjoflat: And it doesn't matter whether the subject has any notice at all.
>
> FTC: Correct, correct.[30]

While the FTC's scattershot approach could be deemed to reflect the intensely fact-specific nature of reasonableness for data security, in practice it results largely in excessive ambiguity, which further reinforces its discretionary authority. One 2014 study, for example, combed through the then-existing 47 FTC data security actions and cobbled together a list of 72 "reasonable practices" that might constitute a relevant benchmark.[31] Reviewing

---

[30] Transcript of Oral Argument at 35-37, LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (No. 16-16270) [hereinafter LabMD 11th Circuit Oral Argument].

[31] *See* Patricia Bailin, *What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, INT'L ASS'N OF PRIVACY PROFS./WESTIN RES. CTR. STUDY, 1 (Oct. 30, 2014), https://iapp.org/resources/article/study-what-ftc-enforcement-actions-teach-us-about-

the FTC's own "guidance"—purportedly encompassing its approach to data security—the study found that:

> [T]he standard language that the FTC uses is terse and offers little in the way of specifics about the components of a compliance program. Consequently, anyone seeking to design a program that complies with FTC expectations would have to return to the complaints to parse out what the FTC views as "unreasonable"—and, by negation, reasonable—privacy and data security procedures.[32]

At the same time, at least one former Federal Trade Commissioner has described the 2014 NIST Cybersecurity Framework[33] as "fully consistent with the FTC's enforcement framework."[34] And yet the NIST Framework itself is a compendium of five separate industry standards, each comprising, respectively, only 66, 48, 28, 24, or 21 of the 72 "reasonable" data security practices that a firm could derive from the FTC's consent orders.[35]

In other words, even the most comprehensive industry standards—the "fully consistent" NIST Framework—is *inconsistent* with the set of "reasonable" practices that might be derived from the FTC's consent orders between 2002 and 2014.[36] As one commenter noted, "no company could possibly execute every industry standard in the 400-plus-page NIST 800-53, even with a full IT department and certainly not without one."[37] Moreover, data security covers a wide scope of activities beyond technological measures, including such mundane practices as implementing password-change policies, searching employee bags on the way out of work, and best-practices education.

The primary problem is that, unlike the common law, the FTC's catalogue of possible practices does not have a discernible analytical framework to guide its application to specific facts. But, according to the Eleventh Circuit's recent opinion overturning the Commission's *LabMD* order, under the FTC's own understanding of its general Section 5 authority, it is not

---

the-features-of-reasonable-privacy-and-data-security-practices-2/; Kristina Rozan, *How Do Industry Standards for Data Security Match Up with the FTC's Implied "Reasonable" Standards—And What Might This Mean for Liability Avoidance?*, INT'L ASS'N OF PRIVACY PROFS. (Nov. 25, 2014), https://iapp.org/news/a/how-do-industry-standards-for-data-security-match-up-with-the-ftcs-implied-reasonable-standards-and-what-might-this-mean-for-liability-avoidance/.

32 Bailin, *supra* note 31, at 1.

33 NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 3-6 (2014), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [hereinafter NIST FRAMEWORK].

34 Julie Brill, Keynote Address before the Center for Strategic and International Studies Conference, FED. TRADE COMM'N (Sep. 17, 2014) (emphasis added).

35 *See* Rozan, *supra* note 31.

36 *See* NAT'L INST. OF STANDARDS & TECH., SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (NIST Special Publication 800-53 Rev.4, Apr. 2013), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [hereinafter NIST 800-53].

37 Rozan, *supra* note 31.

nearly so unconstrained in its discretion to adjudicate unfairness.[38] In its Unfairness Policy Statement, the FTC acknowledged that it did not have an open-ended mandate to create new public policies, but instead must rely on "clear and well-established" policies in its exercise of its "unfairness" authority.[39] Such policies are "declared or embodied in formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values."[40] Thus, as the Eleventh Circuit recently observed, "an act or practice's 'unfairness' must be grounded in statute, judicial decisions—*i.e.*, the common law—or the Constitution. An act or practice that causes substantial injury but lacks such grounding is not unfair within Section 5(a)'s meaning."[41]

Without some sort of identifiable basis for its "reasonableness" determinations, the FTC's data security decision-making cannot operate in a manner analogous to the common law. To see this, imagine that a group of academics, lawyers, and judges were asked to draft a "Restatement of the Law of Data Security" based on the FTC's "common law" of consent decrees, guidance documents, and blog posts. Would it be possible to render an informative compendium describing the logic of the cases and the application of their outcomes to a range of factual, procedural, and legal circumstances? Would it, in other words, come close to looking like the Restatement of Torts?

The FTC has, to our knowledge, never attempted to do any analysis that approaches the rigor of a judicial decision. Frequently, relevant facts are lumped together or elided entirely into complaints and investigation notices, and rarely, if ever, does the Commission identify which facts were essential to its unfairness determination; certainly it never identifies the relative importance, scale, or impact of any of those facts on the FTC's decision to undertake an enforcement action or the specific elements of the resulting consent order. For example, none of the Commission's settlements or other statements address the basic question of how a target's size, or even the size of the data breach in question, bears on the company's failure to undertake and pay for any particular data security practices.[42] Yet, without that basic data, it is next to impossible to build something like a "Restatement of Data Security" sufficient to enable a lawyer to assess the

---

38 *See generally* LabMD, Inc., 894 F.3d 1221.

39 *See* FED. TRADE COMM'N, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness [hereinafter Unfairness Statement] (appended to *In re* Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984)).

40 *Id.*

41 LabMD, Inc., 894 F.3d at 1229.

42 Geoffrey A. Manne & Ben Sperry, *FTC Process and the Misguided Notion of an FTC "Common Law" of Data Security*, ICLE DATA SECURITY & PRIVACY WORKING PAPER 12-13 (2014), https://laweconcenter.org/resource/ftc-process-misguided-notion-ftc-common-law-data-security.

likely liability risk of a firm's particular conduct given its particular circumstances.

As a result, because of the FTC's "flexible" and evolving standards, and because its standards are developed through one-sided consent decrees with limited application, and little, if any, legal analysis:

> *[W]e don't know what we don't know*, that is, whether other practices that have not yet been addressed by the FTC are "reasonable" or not. (In fact, we don't even know whether there is . . . a comprehensive FTC data security standard). Even in those cases that have been pursued, we don't know how high the reasonableness bar is set. Would it be enough for a company to elevate its game by just an increment to clear the reasonableness standard? Or does it have to climb several steps to clear the bar?[43]

B. *The FTC's Unreasonable "Reasonableness" Approach to Data Security*

Consumer welfare is the lodestar of Section 5. Like the consumer-welfare-oriented antitrust laws, Section 5 does not proscribe specific acts but it is a general standard, designed to penalize and deter "unfair" conduct that harms consumers on net—*without* sweeping in pro-consumer conduct that does not cause demonstrable harm, or that is "reasonably avoidable" by consumers themselves.[44]

In form, Section 5(n) and the Unfairness Statement from which it is derived incorporate a negligence-like standard,[45] rather than a strict-liability rule. Section 5(n) states that:

---

[43] Omer Tene, *The Blind Men, the Elephant and the FTC's Data Security Standards*, PRIVACY PERSPECTIVES BLOG (Oct. 20, 2014), https://iapp.org/news/a/the-blind-men-the-elephant-and-the-ftcs-data-security-standards/ (emphasis in original).

[44] *See* FTC LabMD Opinion, *supra* note 4, at 26 (quoting Unfairness Statement, *supra* note 39, at 1073 ("A 'benefit' can be in the form of lower costs and . . . lower prices for consumers, and the Commission 'will not find that a practice unfairly injures consumers unless it is injurious in its net effects.'").

[45] *LabMD, Inc.*, 894 F.3d at 1231. But, in point of fact, Section 5 most likely contemplates *more* than mere negligence—i.e., recklessness. As LabMD's initial merits brief argues: "While the FTC correctly recognized that something more than satisfaction of Section 5(n) is required, the Opinion erred in using "unreasonableness" as that something more. Instead, culpability under Section 5 requires a showing that the practice at issue was not merely negligent (i.e., "unreasonable"), but instead involved more egregious conduct, such as deception or recklessness—namely, that the practice was "unfair." "The plain meaning of 'unfair' is 'marked by injustice, partiality, or deception.'" LeBlanc v. Unifund CCR Partners, 601 F.3d 1185, 1200 (11th Cir. 2010) (quoting Merriam-Webster Online Dictionary (2010)); *see* FTC v. Wyndham Worldwide, Inc., 799 F.3d 236, 245 (3d Cir. 2015) (suggesting that, to the extent "these are requirements of an unfairness claim," such requirements were met based on defendant's allegedly deceptive statements); In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 496-97 (1st Cir. 2009) (analyzing unfairness under Massachusetts consumer protection statute, which incorporates "FTC criteria"; concluding that the statute covers only "egregious conduct"; and finding defendant's alleged "inexcusable and protracted reckless conduct" met the "egregious conduct" test). Here, the FTC made no finding that LabMD's failure to employ the Additional Security Measures was deceptive

> The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[46]

Congress plainly intended to constrain the FTC's discretion in order to avoid the hasty assumption that imposing nearly *any* costs on consumers is "unfair."[47] Unfairness thus entails a balancing of risk, benefits, and harms, and a weighing of avoidance costs consistent with a negligence regime–or at least, with respect to the last of these, strict liability with contributory negligence.[48] Easily seen and arguably encompassed within this language are concepts from the common law of negligence such as causation, foreseeability, and duty of care. As one court has described it in the data security context, Section 5(n) contemplates "a cost-benefit analysis . . . [that] considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[49]

And the FTC itself has asserted that this language leads to a "reasonableness" approach that specifically eschews strict liability:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities . . . [T]he Commission . . . does not require perfect security; reasonable and appropriate security is a continuous pro-

---

or reckless or otherwise involved conduct sufficiently culpable to be declared "unfair." The absence of any finding that LabMD's conduct fell within the definition of the term "unfair" rendered the FTC's Section 5 analysis fatally incomplete." LabMD 11th Cir. Petitioner Brief, *supra* note 12, at 28. Although we agree with the thrust of this argument, in this article we contend that the "something more" contemplated by Section 5 can be incorporated into the FTC's "reasonableness" approach (assuming it were ever properly deployed). In particular (and as discussed below), "likely to cause substantial injury," properly understood (e.g., as interpreted by the ALJ in LabMD) clearly entails a level of risk beyond that implied by mere negligence. Moreover, logic and, arguably, the constitutional requirement of fair notice demand that the duty of care to which companies are properly held for data security purposes be defined by standards known or presumptively known to companies (e.g., widely accepted industry standards).

46 15 U.S.C. § 45(n) (2012).

47 No market interaction is ever without costs: paying any price, waiting in line, or putting up with advertising are all "costs" to a consumer.

48 *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 291 (AM. LAW INST. 1965) ("Where an act is one which a reasonable man would recognize as involving a risk of harm to another, the risk is unreasonable and the act is negligent if the risk is of such magnitude as to outweigh what the law regards as the utility of the act or of the particular manner in which it is done.").

49 Wyndham, 799 F.3d at 255.

> cess of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[50]

Giving purchase to a reasonableness approach under the Commission's own guidance would seem to require establishing: (1) a clear baseline of appropriate conduct, (2) a company's deviation from that baseline, (3) proof that its deviation caused, or was significantly likely to cause, harm, (4) significant harm, (5) proof that the benefits of–e.g., the cost savings from–its deviation didn't outweigh the expected costs, and (6) a demonstration that consumers' costs of avoiding harm would have been greater than the cost of the harm.[51]

Indeed, as noted above, the Commission has itself previously declared that its Section 5 authority must be derived from "formal sources such as statutes, judicial decisions, or the Constitution as interpreted by the courts, rather than being ascertained from the general sense of the national values."[52] Sifting the tealeaves of the Commission's ambiguous complaint and Order, the Eleventh Circuit believed, as do we, that this meant that the common law of negligence was the natural source of law–and, by implication, constraint–to apply in the *LabMD* case.[53]

But the Commission seems to disagree that a predictable analysis, or even notice of how any analysis would work, is required at all. During oral arguments before the Eleventh Circuit, the court questioned the FTC about what "reasonableness" entails and how litigants are expected to understand their obligations:

> Judge Tjoflat: [A]nd the business industries have got to figure out what the Commission means by reasonably . . . They'll never know what the Commission means. Something happens and the Commission will say it's unreasonable.
>
> FTC Attorney: Well, let me say this is not a closed case at all. This is a case where we have . . . .
>
> Judge Tjoflat: I'm not talking about this closed case, just the plain unreasonableness test. . . . And the industry [is] going to think it's reasonable and something happens and the Commission will say it's unreasonable. In hindsight, you should have done such and such.
>
> FTC Attorney: That happens to businesses in tort law all the time . . . People say "I didn't realize this is unreasonable." Well, you know, the things that you need to do to establish that you're acting reasonably are the kind of things that are laid out in the available guidances.

---

50 COMMISSION STATEMENT, *supra* note 3, at 1.

51 *Id.*; *see also* 15 U.S.C. § 45(n).

52 Unfairness Statement, *supra* note 39.

53 LabMD, Inc., 894 F.3d at 1231.

> Judge Tjoflat: [T]here is a difference between tort law and the common law application in a government rule as to what is reasonable and not reasonable. I think that's the essence. The public policy implications, it seems to me, of what you're saying, is that on limited license to figure out what is reasonable and unreasonable in the economy. And the [C]ommissioners will sit around and decide what is reasonable and I don't believe that's a good public policy objective.
>
> FTC Attorney: Well . . . I believe that's exactly what Congress intended . . . .[54]

Thus, in the view of the FTC, it need not engage with the distinct elements of a case, nor offer an analysis of past cases, adequate to give sufficient notice to investigative targets beyond their need to act "reasonably."

Yet, by eliding the distinct elements of a Section 5 unfairness analysis in the data security context, the FTC's "reasonableness" approach ends up ignoring Congress' evident requirement that the Commission demonstrate duty, causality and substantiality, and perform a cost-benefit analysis of risk and avoidance costs. While the FTC pays lip service to addressing these elements, its inductive, short-cut approach of attempting to define reasonableness by reference to the collection of practices previously condemned by its enforcement actions need not—and, in practice, does not—actually entail doing so. Instead, we "don't know . . . whether . . . practices that have not yet been addressed by the FTC are 'reasonable' or not,"[55] and we don't know how the Commission would actually weigh them in an actual rigorous analysis.

In its *LabMD* opinion, for instance, the FTC claims that it weighed the relevant facts.[56] But if it did, it failed to share its analysis beyond a few anecdotes and vague, general comparisons. Moreover, it failed in *any* way to adduce how specific facts affected its analysis, demonstrate causation, or evaluate the relative costs and benefits of challenged practices and its own remedies. The Commission asserted, for example, that the exposed data was sensitive,[57] but it said nothing about: (1) whether any of it (e.g., medical test codes) could actually reveal sensitive information, (2) what proportion of LabMD's sensitive data was exposed, (3) the complexity or size of the business, (4) the indirect costs of compliance, such as the opportunity costs of implementation of the FTC's required remedies, and (5) the deterrent effect of its enforcement action, among other things.

Perhaps more significantly, the FTC conducted an inappropriately *post hoc* assessment that considered only those remedial measures it claimed would address the specific breach at issue. But this approach ignores the overall compliance burden on a company to avoid excessive risk without knowing, *ex ante*, which specific harm(s) might occur. Actual compliance

---

54 LabMD 11th Circuit Oral Argument, *supra* note 30, at 34-36.

55 Tene, *supra* note 43.

56 *See generally* FTC LabMD Opinion, *supra* note 4.

57 FTC LabMD Opinion, *supra* note 4, at 16.

costs are far more substantial, and require a firm to evaluate which of the universe of possible harms it should avoid, and which standards the FTC has and would enforce. This is a far more substantial, costlier undertaking than the FTC admits.

Implicitly, the Commission assumes that the specific cause of unintended disclosure of PII was the only–or the most significant, perhaps–cause against which the company should have protected itself. It also violates a basic principle of statistical inference by inferring a high prior probability, or even a certainty, of insufficient security from a single, post hoc occurrence. In reality, however, while the conditional probability that a company's security practices were unreasonable given the occurrence of a breach may be *higher* than average, assessing by how much, or indeed if at all, requires the clear establishment of a baseline and a rigorous evaluation of the contribution of the company's practices to any deviation from it. The FTC's approach woefully fails to accomplish this, and, as discussed in more detail below, imposes an effective strict liability regime on companies that experience a breach, despite its claim that "the mere fact that a breach occurred does not mean that a company has violated the law."[58]

C. *A Duty Without Definition*

Section 5(n) plainly requires a demonstrable connection between conduct and injury.[59] While the anticompetitive harm requirement that now defines Sherman Act jurisprudence was a judicial construct,[60] Section 5(n) itself demands proof that an "act or practice causes or is likely to cause substantial injury" before it may be declared unfair.[61] But the FTC's reasonableness approach, as noted, is not directed by the statute, which nowhere defines actionable conduct as "unreasonable"; rather, the statute requires the agency to engage in considerably more in order to identify unreasonable conduct. [62] But even taking the FTC at face value and assuming "reasonableness" is meant as shorthand for the full range of elements required by Section 5(n), the FTC's approach to reasonableness is fatally deficient.

The FTC purports to engage in a case-by-case approach to unreasonableness, eschewing prescriptive guidelines in an effort to avoid unnecessarily static definitions. While agencies have authority to issue regulations through case-by-case adjudication,[63] that ability is not without limit. And despite the FTC's reliance upon the Supreme Court's *Chenery* case for the

---

58 *Id.* at 10.

59 15 U.S.C. § 45(n) (2012).

60 *See, e.g.,* Cont'l T.V., Inc. v. GTE Sylvania, Inc., 433 U.S. 36 (1977).

61 15 U.S.C. § 45(n).

62 *See generally* 15 U.S.C. § 45(n).

63 Sec. & Exch. Comm'n v. Chenery Corp., 332 U.S. 194, 203 (1947).

principle that it is entitled to "develop behavioral standards by adjudication" on a case-by-case basis,[64] *Chenery* does not provide the support that the FTC claims.

To begin with, *Chenery* held that agencies may not rely on vague bases for their rules or enforcement actions and expect courts to "chisel" out the details:

> If the administrative action is to be tested by the basis upon which it purports to rest, *that basis must be set forth with such clarity as to be understandable. It will not do for a court to be compelled to guess at the theory underlying the agency's action*; nor can a court be expected to chisel that which must be precise from what the agency has left vague and indecisive. In other words, 'We must know what a decision means before the duty becomes ours to say whether it is right or wrong.'[65]

In the data security context, the FTC's particular method of case-by-case adjudication, reliance upon a purported "common law" of ill-detailed consent orders, entails exactly the sort of vagueness that the *Chenery* court rejected as a valid basis for agency action. The FTC issues complaints based on the "reason to believe" that an unfair act has taken place. Targets of these complaints settle for myriad reasons and no outside authority need review the sufficiency of the complaint. And the consent orders themselves are, as we have noted, largely devoid of legal and even factual specificity. As a result, the FTC's authority to initiate an enforcement action based on any particular conduct is effectively based on an ill-defined series of previous hunches, hardly a sufficient basis for defining a clear legal standard.

But the FTC's reliance upon *Chenery* is even more misguided than this, however. In *Chenery*, the respondent, a company engaged in a corporate reorganization, was governed by statutory provisions that explicitly required it to apply to the Securities and Exchange Commission (SEC) for permission to amend its filings in order to permit the conversion of its board members' preferred stock into common stock in the new corporation.[66] In upholding the SEC's authority to block the proposed amendment, the Court opined that:

> The absence of a general rule or regulation governing management trading during reorganization did not affect the Commission's duties in relation to the particular proposal before it. The Commission . . . could [act] only in the form of an order, entered after a due consideration of the particular facts in light of the relevant and proper standards. That was true regardless of whether those standards previously had been spelled out in a general rule or regulation. Indeed, if the Commission rightly felt that the proposed amendment was inconsistent

---

64 Brief of Respondent at 49, LabMD, Inc. v. FTC, 894 F.3d 1221 (11th Cir. 2018) (No. 16-16270) [hereinafter FTC 11th Cir. Respondent Brief]

65 Chenery Corp., 332 U.S. at 196–97 (emphasis added).

66 *Id.* at 201.

> with those standards, an order giving effect to the amendment merely because there was no general rule or regulation covering the matter would be unjustified.[67]

The Court thus based its holding on the fact that the SEC was, without question, responsible for approving these sorts of transactions, and the parties understood that they had to apply to the SEC for approval. Accordingly, the Court held that the SEC could not help but act and would have to rely upon either a prior rulemaking or a case-by-case assessment based on previously established standards.[68] There is no such certainty with respect to FTC enforcement of Section 5. Instead, the FTC seeks targets for investigation and exercises prosecutorial discretion without disclosure of the basis upon which it does so. Targets have no particular foreknowledge of what the FTC expects of them in the data security context. Thus, when the FTC undertakes enforcement actions without clearly defined standards and under constraints that ensure that it will not undertake enforcement against the vast majority of unfair acts—and without any guidance regarding why it decided *not* to undertake these actions—it does not set out a reasonable regulatory standard. Rather, from the target's point of view, any action would seem more predatory and effectively arbitrary than it is regulatory.

This is not to say that reasonableness must be defined with perfect specificity in order to meet the requirements of *Chenery*; reasonableness is necessarily a somewhat fuzzy concept. But courts have developed remarkably consistent criteria for establishing it. Thus, under typical negligence standards, an actor must have, and breach, a duty of care before its conduct will be deemed unreasonable.[69] This requires that the actor's duty be defined with enough specificity to make it clear when her conduct breaches it.

In most jurisdictions, "care" is defined by reference to standard industry practices, specific legislative requirements, contractual obligations, or a prior judicial determination of what prudence dictates.[70] Moreover, in most jurisdictions, the appropriate standard of care reflects some degree of foreseeability of harm; there is no duty to protect against unforeseeable risks.[71]

In some other (non-data-security) contexts, the FTC *has* developed something approaching a duty analysis for its unfairness cases. In *In re Audio Communications, Inc.*, for instance, the Commission pursued a company that specifically targeted children with an advertisement bearing a cartoon rabbit that encouraged them to surreptitiously call a 900 number

---

67 *Id.*

68 *Id.* at 208.

69 *See* STUART M. SPEISER ET AL., 2A AMERICAN LAW OF TORTS § 9:3 (2016).

70 RESTATEMENT (SECOND) OF TORTS § 285 (1965).

71 *Id.* at § 302. *See also* David Owen, *Duty Rules*, 54 VAND. L. REV. 767, 778 (2001) ("In general, actors are morally accountable only for risks of harm they do or reasonably should contemplate at the time of acting, for the propriety of an actor's choices may be fairly judged only upon the facts and reasons that were or should have been within the actor's possession at the time the choice was made.").

that would end up applying charges to their parents' phone bills.[72] In part, the Commission pursued the unfairness claim on the basis that children are relatively more vulnerable, and firms therefore owe a greater duty of care when marketing to them.[73] As FTC Commissioner Leary noted about the case in a later speech:

> Some "unfairness" cases seem primarily dependent on the particular vulnerability of a class of consumers. Children are the most conspicuous example . . . . Because children were directly targeted through television ads on otherwise innocuous programs, parents had no reasonable way to avoid the charges. There was no claim of misrepresentation and the conduct might well have been entirely legal had the marketing appeals been directed at adults. Moreover, there is no suggestion that it is inherently wrong to advertise these particular services, or any others, in a way that appeals to children.[74]

But the FTC has established no concrete benchmark of due care for data security, nor has it properly established any such benchmark in any specific case. To be sure, the Commission has cited to some possible sources in passing,[75] but it has failed to distinguish among such sources, to explain how much weight to give any of them, or to distill these references into an operable standard. Not only was this true at the time of LabMD's alleged conduct, but it remained the case six to seven years later when the case was adjudicated, and still holds true today.[76]

Crucially, because "perfect" data security is impossible, not all data security practices that "increase" a risk of breach are unfair.[77] *Some* amount of harm, to say nothing of *some* number of breaches, is fully consistent with the exercise of due care, of "reasonable" data security practices. For the statute to be meaningful, data security practices must be shown to fall outside of customary practice—i.e., to increase the risk of unauthorized exposure and the resulting harm above some "customary" level—before they are deemed unreasonable.

The FTC's decision in *LabMD* asserted that this standard is sufficiently well defined, that LabMD's failure to engage in certain, specific actions enabled the data breach to occur, and thus that LabMD must have deviated from an appropriate level of care.[78] But it is not the case that LabMD had *no* data security program. Rather, "LabMD employed a comprehensive security program that included a compliance program, training, firewalls,

---

72 *In re* Audio Commc'ns Inc., 114 F.T.C. 414, 415 (1991).

s 73 *Id.* at 416.

74 Thomas B. Leary, *Unfairness and the Internet*, FED. TRADE COMM'N (Apr. 13, 2000), https://www.ftc.gov/public-statements/2000/04/unfairness-and-internet.

75 *See, e.g.,* FTC LabMD Opinion, *supra* note 4, at 12 (referring to HIPAA as "a useful benchmark for reasonable behavior").

76 As the 11th Circuit has pointed out. *See* LabMD, Inc., 894 F.3d 1221.

77 *See* COMMISSION STATEMENT, *supra* note 3, at 1.

78 FTC LabMD Opinion, *supra* note 4, at 17-25.

network monitoring, password controls, access controls, antivirus, and security-related inspections."[79] While the Commission disputed some of these practices, for every practice the FTC claims LabMD did *not* engage in, there were other practices in which it inarguably *did* engage.[80] And the FTC did not establish that, taken together and even absent the specific practices discussed by the FTC, these practices were outside of the normal range of customary data security protections.[81]

Importantly, where, as in *LabMD*, the FTC focused on the sufficiency of precautions relating to the *specific* harm that occurred, it failed to establish the requirements for an overall data protection scheme, which is the relevant consideration. The general security obligations under which any company operates prior to a specific incident are not necessarily tied to that incident. *Ex ante*, in implementing its security practices, LabMD would not necessarily have focused particularly on the P2P risk, which was, at the time, arguably not generally well understood nor viewed as very likely to occur. Before Tiversa's incursion, LabMD surely faced different security risks, and undertook a range of measures to protect against them. Given this, the existence of P2P software on one computer, in one department, and against LabMD's policy, was not inherently unreasonable in light of the protections LabMD *did* adopt. Yet the Commission invalidated all of LabMD's data protection measures because of the single unlikely breach that *did* occur.[82]

The truth is that the FTC simply did not establish that LabMD's practices were insufficient to meet its duty of care.[83] At best, the Commission argued that LabMD failed to engage in *some* conduct that *could* be part of the duty of care. But even if LabMD failed to engage in every practice derived from FTC consent decrees, most of which post-date the relevant time period in the case, or some of the practices described in one or more of the industry standard documents to which the FTC refers,[84] the FTC failed to

---

79 LabMD 11th Cir. Petitioner Brief, *supra* note 12, at 2 (citations to the record omitted).

80 *Id.*

81 *See generally id.*

82 *See generally* FTC LabMD Opinion, *supra* note 4

83 The Eleventh Circuit agreed that the FTC had failed to connect the allegations in the complaint, as well as the remedy sought, to LabMD's actual conduct:

> The proposed cease and desist order, which is identical in all relevant respects to the order the FTC ultimately issued, identifies no specific unfair acts or practices from which LabMD must abstain and instead requires LabMD to implement and maintain a data-security program "reasonably designed" to the Commission's satisfaction.
>
> . . .
>
> In the case at hand, the cease and desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable.

LabMD, Inc., 894 F.3d at 1230, 1236.

84 FTC LabMD Opinion, *supra* note 4, at 12 n. 23.

establish that LabMD's practices, *as a whole*, were insufficient to meet a reasonable standard of care.

The failure to establish a baseline duty of care also means that companies may lack constitutionally required fair notice of the extent of the data security practices that might be deemed unreasonable by the FTC.[85]

The Eleventh Circuit, in fact, zeroed in on the fair notice issues at oral argument:

> Judge Tjoflat: Well, but the problem — the reason for rulemaking is there's no notice for any of these things in the past . . . that's why you use rulemaking . . . You're going to set prophylactic rules in the future. Nobody knows they've been violating anything. We're going to create something and you will violate . . . .
>
> FTC Attorney: Right. Well, I . . . agree that . . . that's one reason why . . . an agency might use prophylactic rulemaking, of course. The Supreme Court made very clear in *Bell Aerospace* and in the *Chenery* case that the agency is entitled to proceed on a case-by-case adjudication, particularly in situations like this where it's difficult to formulate *ex ante* rules. And the rule that the Commission has set forth here . . . is that companies have a duty to act reasonably under the circumstances . . . .
>
> Judge Tjoflat: That's about as nebulous as you can get, unless you get industry standards.[86]

This absence of fair notice resulting from the FTC's chosen procedures is crucially important, as it is a cornerstone of constitutional due process:

> The fair notice doctrine requires that entities should be able to reasonably understand whether or not their behavior complies with the law. If an entity acting in good faith cannot identify with "ascertainable certainty" the standards to which an agency expects the entity to conform, the agency has not provided fair notice.[87]

The FTC's approach, by contrast, effectively operates in reverse, by inferring unreasonableness from the existence of harm, without clearly delineating a standard first. If the common law of torts had developed accord-

---

85 Gerard Stegmaier and Wendell Bartnick, *Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements*, 20 GEO. MASON L. REV. 673, 675-77 (2013).

86 LabMD 11th Circuit Oral Argument, *supra* note 30, at 23-24.

87 Stegmaier & Bartnick, *supra* note 85, at 677. Note that the fair notice doctrine has not been incorporated into any Supreme Court cases to date. Thus, this formulation comes from the D.C. Circuit's jurisprudence, and represents a relatively stronger version of the doctrine. *Id.* at 680. By contrast, some other circuits require little more than actual notice. While the Fifth Circuit "may be consistent with the D.C. Circuit," the Seventh Circuit requires that regulations are not "incomprehensibly vague." *Id.* at 15 n. 45; Tex. E. Prods. Pipeline Co. v. OSHRC, 827 F.2d 46, 50 (7th Cir. 1987). And "[t]he Second, Ninth, and Tenth Circuits have used a test that asks whether 'a reasonably prudent person, familiar with the conditions the regulations are meant to address and the objectives the regulations are meant to achieve, has fair warning of what the regulations require.'" *Id.*

ing to FTC practice, duty of care would be defined, in effect, as conduct that does not allow–or has not, in clearly analogous contexts, allowed–injury to occur. Not only does such an approach fail to provide actors with a reliable means to determine the specific conduct to which they must adhere, it fails even to provide a discernible and operable *standard* of care.

Far from establishing what conduct constitutes "reasonable" data security *ex ante*, the FTC's approach is tantamount to imposing a strict liability regime in which "reasonableness" is largely unknowable at the time conduct is undertaken and is reliably determined only in reference to whether or not an injury-causing breach occurs *ex post*. This is in marked contrast to the negligence-like regime that Congress implemented in Section 5(n).

II. THE DIFFICULTY OF ESTABLISHING A DUTY OF CARE TO PREVENT THE ACTS OF THIRD PARTIES—AND THE FTC'S FAILURE TO DO SO

An important peculiarity of data security cases is that many of them entail intervening conduct by third parties; in other words, information is disclosed to unauthorized outside viewers as a result of a breach by third parties, rather than removal or exposure by employees of the company itself. There is, in fact, some question whether the FTC Act contemplates conduct that merely facilitates, or fails to prevent, harm caused by third parties, rather than conduct that causes harm to consumers directly.[88] But even if the FTC does have authority to police third-party breaches, and thus the appropriate security measures to reduce their risk,[89] the fit between such conduct and Section 5 remains uneasy.

The FTC has traditionally used its "unfairness power" to police coercive sales and marketing tactics, unsubstantiated advertising, and other misrepresentations to consumers. In such cases, there is a more direct line between conduct and harm.[90] In data security cases, however, the alleged unfairness is a function of a company's failure to take precautions sufficient to *prevent* a third party's intervening, harmful action, i.e., hacking.

In cases of negligence, third parties can certainly create liability when the defendant has some special relationship with the third-party—such as a parent to a child, or an employer to an employee—and thus is reasonably on notice about the behavior of that particular party. The law also imposes liability in certain circumstances despite the intervening behavior of totally unpredictable and uncontrollable third parties, e.g., in some strict product liability cases.

---

88 *See generally* Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127 (2008).

89 *See*, *e.g.*, Wyndham, 799 F.3d at 248-49.

90 *See generally* Richard Craswell, *Identification of Unfair Acts and Practices by the Federal Trade Commission*, 1981 WISC. L. REV 107 (1981).

But, in part because intervening conduct does frequently negate or mitigate liability, establishing duty, and, of course, causation, where a company's conduct is not the proximate cause of injury entails a different and more complex analysis than in a "direct harm" case. Yet the FTC typically pays scant attention to the nature of third-party conduct, despite its assertion that "reasonable and appropriate security is a continuous process of assessing and addressing [precisely such external] risks."[91]

In *LabMD*, for example, the breach at issue was effected by a third-party, Tiversa, employing an unusual and unusually invasive business model based upon breaching firms' networks in order to coerce them to buy its security services.[92] Despite Tiversa's problematic behavior–let alone its subsequent, rather suspicious conduct in working with FTC investigators to develop the case–the FTC did not–at least in its public presentations of its analysis–assess the particularities of Tiversa's conduct, the likelihood that a company would fall prey to it, and the likelihood of other, more-typical risks that could have arisen but been prevented by protecting against Tiversa's conduct.[93] Assessing whether LabMD's conduct was appropriate in light of Tiversa's conduct requires, among other things, assessing how likely was Tiversa's–or a similar, malicious, third-party's–conduct before it occurred and the extent to which LabMD's necessarily imperfect protections against *other* conduct reasonably protected against Tiversa's, as well. The fact that Tiversa succeeded in obtaining PII from LabMD does not, of course, mean that LabMD's overall data security regime, nor even its P2P-specific elements, was "unfair."

While the FTC's decision discusses more general risks of P2P file-sharing services, it fails to distinguish between the risk of inadvertent disclosure through "normal" P2P conduct and Tiversa's intentional hacking.[94] The decision asserts that "there was a high likelihood of harm because the sensitive personal information contained in the 1718 file was exposed to millions of online P2P users, many of whom *could* have easily found the file."[95] But even if typical P2P users "could" have found the file, this says little about the likelihood that they would do so, or, having "found" it, that they would bother to look at it. As the FTC *LabMD* opinion notes, the 1718 file was only one of 950 files on a single employee's computer being shared over LimeWire, a P2P file-sharing program, the vast majority of which were music or videos.[96] Certainly, just because Tiversa identified

---

91 FTC LabMD Opinion, *supra* note 4, at 11.

92 *See generally* FTC LabMD Opinion, *supra* note 4.

93 *See generally* FTC LabMD Opinion, *supra* note 4.

94 *See generally* FTC LabMD Opinion, *supra* note 4.

95 FTC LabMD Opinion, *supra* note 4, at 21 (emphasis added).

96 FTC LabMD Opinion, *supra* note 4, at 4.

and accessed the file says next to nothing about the likelihood that a typical P2P user would.[97]

To be sure, the FTC was correct to discuss this risk, and other risks, that did *not* give rise to the specific alleged injury at issue in the case. And it is likewise appropriate to question security practices that could give rise to breach even if they did not (yet) do so. But the FTC cannot establish that the protections that LabMD employed to ameliorate inadvertent exposure of PII left documents unreasonably protected on the basis that non-hackers "could" have accessed them. LabMD had a policy against installation of P2P programs and it periodically checked employees' computers, among other things. Given the actual *ex ante* risk of inadvertent P2P exposure, this may well have been sufficient. Indeed, at minimum the evidence in the case suggests that LabMD's security practices were sufficient to confine P2P file sharing to a single computer from which very little sensitive information was taken, and from which *no* information was taken by "typical" P2P users. But we simply don't know whether LabMD's practices were sufficient to meet its reasonable duty of care because the FTC never assessed this.[98]

---

[97] Importantly, while Tiversa used proprietary software to scour P2P networks for precisely such inadvertently shared files, typical P2P users (the "millions of online P2P users" referred to by the Commission) use(d) programs like LimeWire to search for specific files or file types (e.g., mp3s of specific songs or specific artists), rarely if ever viewing a folder's full contents. LimeWire itself (and other programs like it) segregated content by type, so that users would have to look specifically at "documents" (as opposed to "music" or "videos," e.g.) in order to see them (and even then a user would see only a file's name, not its contents). Given the prevalence of malware and viruses being shared via P2P networks, typical users were generally reluctant to access any strange files. And, although it is true that a user would not need to search for the exact filename in order to be able to see it, the file at issue in this case, named "insuranceaging_6.05.071.pdf," would not likely have aroused anyone's interest if they happened upon it—least of all typical P2P users searching for music and videos.

[98] Interestingly, the FTC notes in its opinion that:

> Complaint Counsel argues that LabMD's security practices risked exposing the sensitive information of all 750,000 consumers whose information is stored on its computer network and therefore that they create liability even apart from the LimeWire incident. We find that the exposure of sensitive medical and personal information via a peer-to-peer file-sharing application was likely to cause substantial injury and that the disclosure of sensitive medical information did cause substantial injury. Therefore, we need not address Complaint Counsel's broader argument.

FTC LabMD Opinion, *supra* note 4 at 16. In theory, however, the FTC should have been able to make out a stronger case (and one that would have addressed the company's overall duty of care with respect to all *ex ante* threats against all of its stored PII) if its allegations were true and it had assessed the full extent of LabMD's practices and risks to all of its data. Presumably the reason it did not choose to do this is that it was unable to adduce any such evidence beyond the risk to the 1718 file from Tiversa. As the ALJ noted: "[Complaint Counsel's expert] fails to assess the probability or likelihood that Respondent's alleged unreasonable data security will result in a data breach and resulting harm. Mr. Van Dyke candidly admitted that he did not, and was not able to, provide any quantification of the risk of identity theft harm for the 750,000 consumers whose information is maintained on LabMD's computer networks, because he did not have evidence of any data exposure with respect to those individuals, except

A. *The FTC's Effective Disregard of Causation*

Section 5(n) unambiguously requires that there be some causal connection between the allegedly unfair conduct and injury.[99] While the presence of the "likely to cause" language complicates this, as we discuss at length below, causation remains a required element of a Section 5 unfairness case. However, the FTC seems content to assume causation from the existence of an unauthorized disclosure coupled with virtually any conduct that deviates from practices that the Commission claims could have made disclosure less likely. As we have discussed, this sort of inductive approach unaccompanied by an assessment of *ex ante* risks, costs, and benefits is insufficient to meet any reasonable interpretation of the limits placed upon the FTC by Section 5(n).

But the FTC's apparent disregard for its obligation to prove causation is even starker; in *LabMD*, instead of establishing a causal link between LabMD's conduct, i.e., its failure to adopt specific security practices, and even the breach itself, let alone the alleged harm, the FTC offers a series of *non sequiturs*, unsupported by evidence.[100] The FTC's opinion cites allegedly deficient practices,[101] but establishes no causal link between these and Tiversa's theft of the 1718 file—nor *could* it, at least for many of the practices it mentions, because the theft had nothing to do with, for example, password policies, operating system updates, or firewalls, all of which are mentioned in the opinion. Moreover, things like integrity monitoring and penetration testing, also mentioned, at best "'*might* have' aided detection of the application containing the P2P vulnerability," in the FTC's own words.[102] LabMD's alleged failure to do these things cannot be said to have caused the alleged harm. Even with respect to other security practices that *might* have a more logical connection to the breach, e.g., better employee training, the Commission offers no actual evidence demonstrating that failure to employ these actually caused, or even were likely to cause, any *harm*.

Whatever the standard for "unreasonableness," there must be a causal connection between the acts, or omissions, and injury. Even for "likely" harms this requires not merely *any* possibility but some high *probability* at the time the conduct was undertaken that it would cause future harm.[103] Instead, the Commission merely asserted that harm was sufficiently "likely" based on its own *ex post* assessment, in either 2012 or 2017, of the risks of

---

as to those that were listed on the 1718 File or in the Sacramento Documents." ALJ LabMD Initial Decision, *supra* note 17, at 83-84.

99 15 U.S.C. § 45(n).

100 *See generally* FTC LabMD Opinion, *supra* note 4

101 *See, e.g.*, FTC LabMD Opinion, *supra* note 4, at 2.

102 *Id.* at 31, 4 n.13 (emphasis added).

103 *See* ALJ LabMD Initial Decision, *supra* note 17, at 54.

P2P software in 2007, without making any concrete connections between the generalized risk and the specific circumstances at LabMD.

The FTC's Chief ALJ found this assertion manifestly wanting, and ruled that the Commission had failed to establish a sufficient connection between LabMD's conduct and the data that was actually removed from the company.[104] But with respect to Complaint Counsel's assertion that, in effect, *all* data held by LabMD was at risk, the ALJ found that:

> Complaint Counsel's theory that harm is likely for all consumers whose Personal Information is maintained on LabMD's computer network, based on a "risk" of a future data breach and resulting identity theft injury, is without merit. First, the expert opinions upon which Complaint Counsel relies do not specify the degree of risk posed by Respondent's alleged unreasonable data security, or otherwise assess the probability that harm will result. To find "likely" injury on the basis of theoretical, unspecified "risk" that a data breach will occur in the future, with resulting identity theft harm, would require reliance upon a series of unsupported assumptions and conjecture. Second, a "risk" of harm is inherent in the notion of "unreasonable" conduct. To allow unfair conduct liability to be based on a mere "risk" of harm alone, without regard to the probability that such harm will occur, would effectively allow unfair conduct liability to be imposed upon proof of unreasonable data security alone. Such a holding would render the requirement of "likely" harm in Section 5(n) superfluous, and would contravene the clear intent of Section 5(n) to limit unfair conduct liability to cases of actual, or "likely," consumer harm.[105]

But the Commission disagreed: "The ALJ's reasoning comes perilously close to reading the term 'likely' out of the statute. When evaluating a practice, we judge the likelihood that the practice will cause harm at the time the practice occurred, not on the basis of actual future outcomes."[106] This is true, as far as it goes, and, as we have noted above, a proper reasonableness assessment would address expected risk, cost, and benefit of all harms and security practices, including those that don't factor into the specific circumstances at issue in the case. But even such an undertaking requires some specificity regarding expected risks and some proof of a likely causal link between conduct and injury.

More importantly, judgments about the likelihood that past conduct would cause harm must be informed by what has actually occurred. By the time the FTC filed its complaint, and surely by the time the FTC rendered its opinion, facts about what *actually* happened over the course of LabMD's existence should have informed the Commission about what was *likely* to occur.

Although the ALJ's Initial Decision focused heavily on the FTC's lack of evidence of actual harm, the judge went to great lengths to explain why this lack of harm is *also* relevant when evaluating "likely" harms:

---

104 *Id.* at 53.

105 ALJ LabMD Initial Decision, *supra* note 17, at 81.

106 FTC LabMD Opinion, *supra* note 4, at 23.

> Complaint Counsel presented no evidence of any consumer that has suffered NAF, ECF, ENCF, medical identity theft, reputational injury, embarrassment, or any of the other injuries . . . . Complaint Counsel's response—that consumers may not discover that they have been victims of identity theft, or even investigate whether they have been so harmed, even if consumers receive written notification of a possible breach, as LabMD provided in connection with the exposure of the Sacramento Documents—does not explain why Complaint Counsel's investigation would not have identified even one consumer that suffered any harm as a result of Respondent's alleged unreasonable data security. Complaint Counsel's response to the absence of evidence of actual harm in this case, that it is not legally necessary under Section 5(n) to prove that actual harm has resulted from alleged unfair conduct, because "likely" harm is sufficient . . . fails to acknowledge the difference between the burden of production and the burden of persuasion. The express language of Section 5(n) plainly allows liability for unfair conduct to be based on conduct that has either already caused harm, or which is "likely" to do so. However . . . the absence of any evidence that any consumer has suffered harm as a result of Respondent's alleged unreasonable data security, even after the passage of many years, undermines the persuasiveness of Complaint Counsel's claim that such harm is nevertheless "likely" to occur. That is particularly true here, where the claim is predicated on expert opinion that essentially only theorizes how consumer harm could occur. Given that the government has the burden of persuasion, the reason for the government's failure to support its claim of likely consumer harm with any evidence of actual consumer harm is unclear.[107]

Moreover, the ALJ pointed out how reviewing courts are hesitant to allow purely speculative harms to support Section 5 actions:

> In light of the inherently speculative nature of predicting "likely" harm, it is unsurprising that, historically, liability for unfair conduct has been imposed only upon proof of actual consumer harm. Indeed, the parties do not cite, and research does not reveal, any case where unfair conduct liability has been imposed without proof of actual harm, on the basis of predicted "likely" harm alone. . . . In Southwest Sunsites v. FTC, 785 F.2d 1431, 1436 (9th Cir. 1986), the court interpreted the Commission's deception standard, which required proof that a practice is "likely to mislead" consumers, to require proof that such deception was "probable, not possible . . . ." Based on the foregoing, "likely" does not mean that something is merely possible. Instead, "likely" means that it is probable that something will occur. . . . Moreover, although some courts have cited the "significant risk" language from the Policy Statement, the parties have not cited, and research does not reveal, any case in which unfair conduct liability has been imposed without proof of actual, completed harm, based instead upon a finding of "significant risk" of harm.[108]

That the only available facts point to the complete *absence* of any injury suggests at the very least that injury was perhaps not "likely" caused by any of LabMD's conduct. It is thus the Commission that is in danger of reading "likely" out of the statute and replacing it with something like "could conceivably have contributed to any increase in the chance" of injury. It simply cannot be the case that Congress added the "likely to cause" language so that the Commission might avoid having to demonstrate a causal link between conduct and injury, even "likely" injury.

Moreover, if the FTC's "likely" authority is to have any meaningful limit, it must be understood *prospectively*, from the point at which the FTC

---

107 ALJ LabMD Initial Decision, *supra* note 17, at 52-53.

108 *Id.* at 53-55.

issues its complaint. Thus, if an investigative target has *ceased* practices that the Commission claims "likely" to cause harm by the time a complaint is issued, the claim is logically false and, in effect, impossible to remedy; Section 5 is not punitive and the FTC has no authority to extract damages, but may only issue prospective injunctions. In other words, because Section 5 is intended to *prevent*, not punish, unfair practices that harm consumers, if a potential investigative target has *already ceased* the potentially unfair practices, Section 5 could be considered to have been achieved a deterrent effect by the omnipresent threat of FTC investigation. This is, in fact, the statute working properly. By contrast, the Commission's reading of its "likely to cause" authority—which would allow it to scan a company's *past* behaviors, regardless of when its complaint was issued, and force them through expensive investigations and settlements—would in effect grant it punitive powers.

B. *An Abuse Of The FTC's "Likely To Cause" Authority: The HTC Case*

The Commission's 2013 *HTC* complaint and settlement exemplifies its willingness to infer causation under the "likely to cause" language of Section 5(n) from the barest of theoretical risks and without connecting it in any concrete way to injury. In *HTC*, HTC America had customized its Android mobile phones in order to include software and features that would differentiate them from competing devices.[109] In doing so, however, HTC had, in the FTC's opinion, "engaged in a number of practices that, taken together, failed to employ reasonable and appropriate security in the design and customization of the software on its mobile devices."[110] The end result was that HTC's engineers had created security flaws that *theoretically* could be used to compromise user data.[111]

There were not, however, *any* known incidents of data breach arising from consumers' use of the approximately ten to twelve million devices at issue.[112] Nonetheless, HTC's practice was still found to be "likely" to injure consumers despite the *practical* unlikeliness of finding zero flaws in a sample of ten million.[113] In the Commission's view:

> [M]alware placed on consumers' devices without their permission could be used to record and transmit information entered into or stored on the device . . . . Sensitive information exposed on the devices could be used, for example, to target spear-phishing campaigns, physi-

---

109 *In re* HTC Am. Inc., 155 F.T.C. 1617, 2 (2013) [hereinafter HTC Complaint].

110 *Id.* at 2.

111 *Id.* at 2-6.

112 Alden Abbot, *The Federal Trade Commission's Role in Online Security: Data Protector or Dictator?*, HERITAGE FOUND. (Sept. 10, 2014), http://www.heritage.org/report/the-federal-trade-commissions-role-online-security-data-protector-or-dictator.

113 HTC Complaint, *supra* note 109, at 6.

> cally track or stalk individuals, and perpetrate fraud, resulting in costly bills to the consumer. Misuse of sensitive device functionality such as the device's audio recording feature would allow hackers to capture private details of an individual's life.[114]

Interestingly, not only does the FTC in *HTC* infer causation from a deviation from its idealized set of security protocols despite the absence of any evidence of breach, in doing so it also necessarily incorporates its own inferences about the magnitude of the risk of third-party conduct. It incorporates these inferences regardless of whether HTC's assumptions regarding the likelihood of third-party intervention were lower, and without–publicly, at least–assessing whether those assumptions were reasonable. At minimum, there is absolutely no way to infer from the FTC's guidance or previous consent orders what an appropriate estimate would be; again, the FTC fails to establish a baseline duty of care. Instead, it appears that the FTC believes that any risk of third-party intervention would be sufficient to merit protective security measures.

But there is not a network-connected device in the world about which it could not be said that there is *some* risk of breach. Even the National Security Agency—America's top spy shop and, presumably, among the very least likely to be hacked by an outside party—was subject to a third-party data breach that resulted in the release of a large amount of confidential information.[115]

HTC also represented a fundamental shift in the Commission's approach. In that case, it moved rather dramatically from policing fraud and deception to interjecting itself into the engineering process.[116] HTC America was not accused of purposely creating loopholes that could be used to harm consumers; it was, in essence, found to be negligent in how it designed its software.[117]

III. THE FTC'S UNREASONABLE APPROACH TO HARM

There is a close connection between the problems with the FTC's approach to causation and its approach to injury, especially with respect to conduct that is deemed "likely to cause" injury.

---

114 *Id.*

115 *See, e.g.*, Matt Burgess, *Hacking the Hackers: Everything You Need to Know About Shadow Brokers' Attack on the NSA*, WIRED (Apr. 18, 2017), http://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers.

116 *See generally* HTC Complaint, *supra* note 109.

117 HTC Complaint, *supra* note 109, at 2.

A. *Breach Is Not (Or Should Not Be) The Same Thing As Harm*

One of the core errors committed by the FTC in *LabMD*–particularly by Complaint Counsel before the ALJ, but also, although less obviously, by the Commission itself in its *LabMD* Opinion–is the assertion that breach alone can constitute harm. Similarly flawed–and flowing from this error–is the assertion that conduct giving rise to the *possibility* of breach, even without an actual breach, can be deemed "likely to cause" harm.

Of course, as we have noted, the Commission's explicit statements hold that a mere breach alone is *not* harm.[118] And for most of its history, the Commission's decisions have also suggested that a breach alone cannot constitute harm. Two watershed cases in the evolution of the FTC's data security enforcement practices help to illustrate this.

First, in 2002, the FTC entered into a consent order with Eli Lilly, holding the company responsible under Section 5 for deceptive conduct, based on its disclosure of the names of 669 patients who were taking Prozac to treat depression, in contravention of its stated policy.[119] That they were users of Prozac was apparent from the context of the disclosure, and, today at least, it is readily apparent why the disclosure itself, as opposed to any subsequent action taken as a consequence of the disclosure, might constitute actionable harm.[120]

Although brought as a deception case, the conduct at issue was "failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information."[121] The case, commonly considered to be the FTC's first data security case, marked something of an evolution in the FTC's view of what constituted harm under Section 5's Unfair or Deceptive Acts or Practices language by finding purely *non-monetary* harm, the public disclosure of information in a potentially compromising and unambiguous context, to be material.[122]

The underlying theory of materiality or harm in *Eli Lilly*—while not in any way explicated by the FTC, even in the accompanying Analysis of Pro-

---

118 *See, e.g.,* COMMISSION STATEMENT, *supra* note 3, at 1. ("The mere fact that a breach occurred does not mean that a company has violated the law.").

119 *In re* Eli Lilly & Co., 133 F.T.C. 763, 766-767 (May 8, 2002).

120 *See generally id*.

121 *Id.*

122 *See* FED. TRADE COMM'N, POLICY STATEMENT ON DECEPTION (1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception [hereinafter DECEPTION POLICY STATEMENT]. While "harm" is not a required showing in a deception case, materiality is meant to be a *proxy* for harm in the context of deception cases. The FTC's Deception Policy Statement, itself a compromise between then-Chairman Miller's preference for an explicit finding of harm and the *Colgate-Palmolive* Court's holding that deception required nothing more than a misleading statement, explicitly joins the two concepts together when it explains that "the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, *to the consumer's detriment*." *Id.* at 2 (emphasis added).

posed Consent Order to Aid Public Comment—never mentions the word materiality.[123] It also never seeks to defend its implicit assertion of either materiality or "detriment," nor does it even acknowledge the novelty of the theory of harm involved (although the theory is arguably recognizable, with origins in Warren & Brandeis' *The Right to Privacy* and common law concepts like the tort of intrusion upon seclusion).[124] But it seems clear that mere exposure of just *any* information alone would not be sufficient to cause harm, or establish materiality; rather, harm would depend on the context, and only embarrassing or otherwise reputation-damaging disclosures caused by certain people viewing certain information would suffice.

Second, in 2005, the Commission entered into a consent order with BJ's Wholesale Club, in its first unfairness-based data security case.[125] While hardly a model of rigorous analysis assessing all of the required elements of an unfairness case under Section 5(n), the FTC in *BJ's Wholesale Club* at least tried to identify concrete harms arising from the breach at issue:

> [F]raudulent purchases . . . were made using counterfeit copies of credit and debit cards the banks had issued to customers . . . [P]ersonal information . . . stored on respondent's computer networks . . . was contained on counterfeit copies of cards that were used to make several million dollars in fraudulent purchases. In response, banks and their customers cancelled and re-issued thousands of credit and debit cards that had been used at respondent's stores, and customers holding these cards were unable to use their cards to access credit and their own bank accounts.[126]

Problematic though both of these examples may be (and they are), they have one thing in common: *harm*, or materiality, is something different than *breach*; rather, it is a *consequence* of a breach. It need not be monetary, and it need not be well defined (which is bad enough). But there is a clearly contemplated sequence of events that gives rise to potential liability in a data security case:

1. A company collects sensitive data;

2. It purports to engage in conduct to keep that data secret, either in an explicit statement or by an implicit guarantee to use "reasonable" measures to protect it;

---

123 ELI LILLY AND CO., *Analysis to Aid Public Comment*, 67 Fed. Reg. 4963 (Feb. 1, 2002) https://www.ftc.gov/policy/federal-register-notices/eli-lilly-and-co-analysis-aid-public-comment.

124 *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195-97 (1890). *See also* Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 206-07 (2012).

125 *In re* BJs Wholesale Club, Inc., 2005 WL 1541551, at *2 (F.T.C June 16, 2005).

126 *Id.*

3. The information is nevertheless disclosed (i.e., there is a security breach) because of conduct by the company that enables the disclosure/breach; and

4. The context or content of the disclosure significantly harms (or is used to harm) consumers, or is likely to lead to significant harm to the consumer.

The last element, significant harm/materiality, and its separation from the third element, breach, is key. As Commissioner Swindle noted in 1999 in his dissent from the Commission's complaint in *Touch Tone* (a precursor case to the FTC's current line of data security cases involving clearly fraudulent conduct by an "information broker"): "[W]e have never held that the mere disclosure of financial information, without allegations of ensuing economic or other harm, constitutes substantial injury under the statute."[127]

But by 2012, in its Privacy Report, the Commission asserted that disclosure itself of private information could give rise to harm, or, presumably, materiality, *regardless* of any other consequences arising from a breach. The harm and the breach became the same thing:

> These harms may include the unexpected revelation of previously private information, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties . . . . [A] privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[128]

This connection between "unexpected revelation" and harm is not obvious, and certainly should be demonstrated by empirical evidence before the FTC proceeds on such a theory. Yet, without any such evidence, the FTC in *LabMD* brought this theory to fruition.

As it admitted, the Commission "does not know"[129] whether any patient encountered a single problem related to the breach, and thus never articulated any actual injury caused by LabMD's conduct.[130] The Commission instead asserted that mere exposure of information suffices to establish

---

127 *In re* Touch Tone, 1999 WL 233879, at *3 (F.T.C Apr. 22, 1999) (Orson Swindle, Comm'r, dissenting).

128 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS 8 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC PRIVACY REPORT].

129 FTC LabMD Opinion, *supra* note 4, at 14.

130 And although the Commission effectively blames LabMD for its (the FTC's) lack of knowledge of harm, that burden does not rest with LabMD. Moreover, the Commission had ample opportunity to collect such evidence if it existed, e.g., by actually asking at least a sample of patients whose data was in the 1718 file or subpoenaing insurance companies to investigate possible fraud. That the Commission still cannot produce any evidence suggests strongly that none exists.

harm.[131] But this amounts to saying that any conduct that causes breach causes harm. That not only violates the FTC's own claims that breach alone is not enough, it is insufficient to meet the substantial injury requirement of Section 5(n).

The examples the Commission has adduced to support this point all entail not merely exposure, but actual dissemination of personal information to large numbers of unauthorized recipients who *actually read* the exposed data.[132] Even if it is reasonable to assert in such circumstances that "embarrassment or other negative outcomes, including reputational harm" result from that sort of public disclosure,[133] no such disclosure occurred in *LabMD*. That the third-party responsible for exposure of data itself viewed the data—which is effectively all that happened in that case—cannot be the basis for injury without simply transforming the breach itself into the injury.

B. *Purely Informational Harms Present Further Difficulties*

Complicating any analysis of harm in the data security context is the fact that many, if not most, of the alleged harms are what the Commission has termed "informational injuries."[134] Such harms are "injuries . . . that consumers may suffer from privacy and security incidents, such as data breaches or unauthorized disclosure of data"[135] and which typically extend beyond the easily quantifiable economic harms such as unauthorized use of credit cards.

At the root of any concept of informational injury is the assertion that the unauthorized exposure of private information may be, in and of itself, a harm to individuals, apart from any concrete economic consequences that may result from the exposure. In the FTC's opinion *in LabMD*, for instance, the Commission asserted that:

---

131 *See* FTC LabMD Opinion, *supra* note 4, at 15 ("Indeed, the Commission has long recognized that the unauthorized release of sensitive medical information harms consumers"). True, it limits this to "sensitive medical information," but disclosure of any number of types of "sensitive" medical information, especially if limited to a vanishingly small number of viewers, may not cause distress or other harm.

132 *See generally In re* MTS, Inc., 137 F.T.C. 444 (2004) (providing that Tower Records was liable for software error that allowed 5,225 consumers' billing information to be read by anyone, which actually occurred).

133 FTC LabMD Opinion, *supra* note 4, at 15.

134 *See, e.g.,* FED. TRADE COMM'N, *FTC Informational Injury Workshop* (October 2018) https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf.

135 *Id.* at 1.

> the disclosure of sensitive health or medical information causes additional harms that are neither economic nor physical in nature but are nonetheless real and substantial and thus cognizable under Section 5(n)…. [D]isclosure of the mere fact that medical tests were performed irreparably breached consumers' privacy, which can involve "embarrassment or other negative outcomes, including reputational harm.[136]

Defining and evaluating these types of informational harms, however, is impossible until many of the fundamental flaws in the Commission's approach to Section 5 are resolved.

The task of defining "informational" injury is fraught in a way that traditional analysis of harm is not. Traditional harms are analyzed against largely objective criteria such as monetary value, physical damage, and the like; their very nature allows for a more or less satisfactory definition of the harm involved.

Although it is certainly possible that the incidence and magnitude of physical harms can be ambiguous—among other things, deception and time can make these assessments more difficult—fundamentally, and certainly relative to intangible injury, determining both is fairly–although far from perfectly–straightforward. So, too, by and large, is the framework for assessing causality and liability readily understood. Moreover, these objectively observable harms exist largely without reference to context; it does not depend on whether you are a CEO or a cashier in determining whether money was lost, it is irrelevant whether one is male or female in determining whether one's car was struck and whiplash was suffered.

Informational injuries, by contrast, are based substantially on *subjective* effects, and are often heavily dependent upon the context in which they were incurred, context that invariably changes over time and place. Whether one feels shame, anxiety, embarrassment, or other "psychic" effects from the unauthorized disclosure of personal information depends, in many instances, on the prevailing social conventions and mores surrounding the disclosed information and its recipients.

In *Eli Lilly*, for instance, the Commission asserted, although certainly without rigorously proving, that the somewhat broad disclosure of the fact that someone was taking an antidepressant in 1999 could lead to harm, e.g., shame, even absent other, concrete effects.[137] That may well have been true in 1999. The difficulty is that, even in 1999, there would have been at least *some* people who would not feel such shame, yet the Commission seems to have assumed that all affected individuals did so.

Absent objective criteria to assess such psychic effect, however, the fact of it occurring as a result of the disclosure cannot simply be assumed. Moreover, the *extent* of harm, even to people who did indeed experience it, would vary widely and be difficult, if not impossible, to measure. Although

---

136 FTC LabMD Opinion, *supra* note 4, at 17.

137 *In re* Eli Lilly, 133 F.T.C. 763.

the Commission does not assess damages for such injuries, determination of the magnitude of harm is still crucial for assessing both whether victims suffered net harm, and whether a Commission action would satisfy the cost-benefit test of Section 5(n).

To make things more complicated, whatever the incidence and magnitude of the effects in 1999, there is no reason to think they would be the same 19 (or 29, or 39) years later. Today, although *some* would surely feel shame at certain other people (but perhaps not total strangers) knowing that they take an antidepressant, the vast popularity of pharmacological treatment for emotional problems means that shame is surely both less likely and less significant–although, at the same time, that same popularity surely means that the aggregate magnitude of harm could actually be greater than in 1999.[138]

And not all informational injuries are the same. Some injuries are psychic in nature, like shame or embarrassment, for example. Others uneasily mix what the FTC typically analyzes as "likely" injuries—inchoate harms such as the exposure of sensitive information that *could* be used to steal an identity, access a bank account, or otherwise lead to more concrete harms—with the psychic consequences of bearing that risk. A purely psychic harm like anxiety arising from exposure of information that could lead to identify theft is, from another point of view, a "likely" harm, with the actual, concrete harm being the financial loss. Thus the "anxiety harm" merges with the likely harm of financial loss, and evaluating the magnitude of such harm would require evaluating both the objective likelihood of the loss, as well as each individual's subjective assessment of that risk. None of these is a straightforward measurement and, to our knowledge, the FTC has never undertaken such a measurement.

C. *Social Context*

Indeed, a major impediment to properly basing data security cases on the psychic flavor of informational injury is the difficulty of establishing a rigorous method, e.g., representative and comprehensive consumer surveys, of determining the baseline expectations that members of society have surrounding the protection of their personal information. And this method,

---

[138] Today, in fact, many people are not only unashamed at taking antidepressants, they are quite open about it. Some even write publicly about how antidepressant use has improved their lives. *See, e.g.,* Kimberly Zapata, *This Is Why Taking Antidepressants Makes Me a Better Mother*, PSYCHCENTRAL (Feb. 13, 2016) https://psychcentral.com/blog/archives/2016/02/13/this-is-why-taking-antidepressants-makes-me-a-better-mother/. For these people it would, surely, be difficult to infer harm from additional, even unauthorized, disclosure.

moreover, will need to be regularly updated to ensure that the standards of, say, two years ago do not govern the changed notions of "today."[139]

There are a number of critical components that would have to factor into establishing this baseline, none of them yet identified comprehensively by the Commission. Among many other things, these will necessarily include, e.g. to whom the information is disclosed, the nature of consumer expectations regarding the release or use of the information, whether the information is itself somehow harmful or could lead to a real concrete harm–like a bank account number or social security number, consumers' perception of the risk of harm, and, if the information could lead to a more concrete harm, the nature of that harm.

The necessary aim of attempting to establish such a baseline is to bring an administrable order to the chaos of subjectivity (if possible). The incidence and magnitude of these subjective effects will undoubtedly change rapidly as technology and society evolve, but a careful periodic analysis might be able to reveal which subjective harms rise to the level of common social acceptance. But such a regular analysis and public guidance on its results would be required because, without a carefully crafted and constantly calibrated standard, using subjective harms as the basis for regulatory or legal actions could quickly result in a race to the bottom where those relative few who are most sensitive to informational injuries dictate policy to the detriment of overall social welfare. Under Section 5's cost-benefit standard, in some cases this cost, coupled with the uncertainty of the underlying alleged harm, will mean the FTC must refrain from bringing an enforcement action.

D. *Calculating Benefits*

Further complicating matters, in the informational context, because often the same conduct that may lead to psychic harm may also confer *concrete* benefits, and because the effects of the conduct on each individual are subjective and variable, determining if conduct results in cognizable injury must entail a careful assessment of the benefits of the conduct to each individual, as well, in order to determine if the *net* effect is negative. In other words, even if, in the abstract, unanticipated disclosure of private information to, say, an advertiser might impose psychic costs on some consumers, it also confers actual benefits on some of them by enabling better-targeted ads. Determining if there is injury on net requires assessing *both* of these effects.

---

[139] The FTC has some experience in establishing guidance like this. See, for example, FED. TRADE COMM'N, GREEN GUIDES, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-issues-revised-green-guides/greenguides.pdf (last viewed Dec. 7, 2018).

Importantly, this is different than the cost-benefit assessment required by Section 5(n), which demands a weighing of costs and benefits not only for the potentially injured parties, but also a weighing of those net costs against the overall benefits of the conduct in question, where consumers who do not experience the costs enjoy those benefits. Here, instead, the very same consumers may in fact, realize both the costs and benefits.

Many of these informational harms may be bound up in the nature of the relevant industry itself. Even though there may exist an unexpected use that some individuals feel harm them, there may also exist a larger justification for the practice in overall increased social welfare. The benefit of having, for instance, certain valuable attributes of a platform like Gmail, Facebook, or Snapchat necessarily must be factored into the cost-benefit calculation. This is not to say that *any* unexpected use of data should be beyond reach, but that the benefit of the existence and optimal operation of the system, firm, or other analytically relevant entity must be taken into account.

E. *Revealed Preferences*

Important in evaluating informational injuries is the fact that, for at least some classes of injury, consumers themselves self-evidently engaged in the services that subsequently caused the injury. With the growing frequency of data compromises, it certainly must be a factor of any informational injury analysis that consumers, knowing that there was some chance that their information could be exposed, chose to engage with those services anyway. Thus, the cost to themselves in informational injury terms was to some extent "priced" into the cost of accessing services in exchange for their personal information.

This is important particularly from the perspective of Section 5(n), as its balancing test requires that harms incurred were not "reasonably avoidable" by consumers.[140] Where users a) voluntarily choose to give their data to a service, b) with sufficiently accurate knowledge of the risk of harm, and c) where there are reasonable substitutes, including not engaging at all, it may, in fact, be reasonable to view their specific choice as prima facie evidence of reasonable avoid-ability in the event of unauthorized disclosure of their data.

And, critically, at least with tech platforms and apps, it is important to recognize that the reason these services become important is *because* so many users choose to adopt them. Sometimes there may not be an obvious alternative. In *LabMD*, for example, it is doubtful that consumers were either informed about or directly choosing among diagnostics laboratories. But, for many services, competitors are available and meaningful consumer choice is viable; it is trivially easy to choose a fully encrypted and secure

---

[140] 15 U.S.C. § 45(n).

email service instead of Gmail, or to opt for DuckDuckGo instead of Google Search. Consumers, however, opt for what they perceive as more accurate or convenient because they value that over privacy to some significant extent. In such circumstances it would be a mistake to deem generally customary practices unfair, even if consumers appear to be harmed *ex post*.

IV. THE TROUBLING IMPLICATION OF THE FTC'S APPROACH: MERE STORAGE OF SENSITIVE DATA CAN CONSTITUTE CONDUCT "LIKELY TO CAUSE" HARM

A crucial and troubling implication of the Commission's position—compounded by its willingness to infer "psychic" harm from the mere risk of disclosure—is that it effectively permits the FTC to read Section 5 as authorizing an enforcement action against any company that merely *stores* sensitive data, virtually regardless of its security practices or even the existence of a breach:

1. The standard adopted by the FTC permits it to infer injury from any unanticipated or unauthorized disclosure (regardless of concrete harm).

2. It makes this inference not necessarily because of the intervention of a third-party, but merely because data is exposed to anyone unauthorized to view it; third-party breach may often be the proximate cause of exposure, but it is unauthorized exposure per se that gives rise to injury, not the fact of a third-party's incursion.

3. This means that information leaving the company in *any* unauthorized manner would be sufficient to demonstrate harm.

4. As noted, the FTC has established a standard by which it may infer that conduct is *likely* to cause injury virtually regardless of the extent of increased risk of exposure attributable to the conduct: *any* increased risk may suffice.

5. Relative to not collecting data at all, or to collecting some lesser amount of data deemed "reasonable" by the FTC, any amount of data collection necessarily increases the risk of its exposure.

6. Thus merely a *potential* of data leaving the company (again, *ex ante* in any unauthorized manner, and not dependent upon a third-party) could amount to *likely* harm.

7. Because that potential *always* exists even with the most robust of security practices, the only thing limiting the Commission's authority to bring an enforcement action against *any* company that collects PII is prosecutorial discretion.

To be sure, the Commission is unlikely to bring a case absent *some* unauthorized disclosure of sensitive data. But the FTC's interpretation of

its authority effectively removes any identifiable limits on its discretion to bring a data security action under Section 5.

In order to properly infer unreasonable security (even from evidence as "strong" as a single instance of unexpected exposure as with the 1718 file, let alone the absence of evidence of any exposure as with the rest of LabMD's data), the FTC should have to demonstrate that such exposure always or almost always occurs *only* when security is unreasonably insufficient. Although there may be specific circumstances in which this is the case, it manifestly is not the case in general. If every breach allows the FTC to infer unreasonableness without showing anything more, it can mean only one of two things: (1) that either the collection or storage of that data was so unambiguously perilous and costly in the first place that a strict liability standard is appropriate as a matter of deterrence, or else (2) that breach always, or nearly always, correlates with unreasonable security practices and the inference is warranted. Because we know the latter to be untrue, the FTC's theory of causation and harm places it in the unreasonable position of implicitly asserting that the data collection and retention practices crucial to the modern economy are inherently "unfair."

A. *The FTC's Reading of "Likely To Cause" Gives it Unfettered Discretion Not Contemplated by Section 5*

In its *LabMD* decision the FTC attempts to mitigate this position to a degree, demurring on the ALJ's holding regarding the inadequacy of Complaint Counsel's assertion that LabMD's security practices were likely to cause harm related to LabMD data *not* found in the 1718 file. But this is a small and insufficient concession.

The FTC reads a sort of superficial "cyber Hand Formula" into the language of Section 5, sufficient to permit it to find liability for conduct that it deems in *any way* increases the chance of injury, even absent an actual breach or any other affirmative indication of "unreasonable" risk, provided the magnitude of potential harm is "significant"–which is, itself, almost entirely within the Commission's discretion to so label:

> Unlike the ALJ, we agree with Complaint Counsel that showing a "significant risk" of injury satisfies the "likely to cause" standard. In arriving at his interpretation of Section 5(n), the ALJ found that Congress had implicitly "considered, but rejected," text in the Unfairness Statement stating that an injury "may be sufficiently substantial" if it "raises a significant risk of concrete harm." . . . Yet the legislative history of Section 5(n) contains no evidence that Congress intended to disavow or reject this statement in the Unfairness Statement. Rather, it makes clear that in enacting Section 5(n) Congress specifically approved of the substantial injury discussion in the Unfairness Statement and existing case law applying the Commission's unfairness authority. . . . We conclude that the more reasonable interpretation

of Section 5(n) is that Congress intended to incorporate the concept of risk when it authorized the Commission to pursue practices "likely to cause substantial injury."[141]

Thus, the Commission concludes: "In other words, contrary to the ALJ's holding that 'likely to cause' necessarily means that the injury was 'probable,' a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low."[142]

When establishing causality, however, Section 5(n) is not focused on the magnitude of the injury itself.[143] Instead, the *likelihood* of injury and the *substantiality* of the injury are distinct concepts. Conduct does not become more *likely* to cause injury in the first place just because it might make whatever injury results more *substantial*.

This is clear from the statute: "substantial" modifies "injury," not "likely."[144] Either conduct *causes* substantial injury, or it is *likely* to cause substantial injury, meaning it creates a sufficiently heightened risk of substantial injury. In each case the "substantial injury" is *literally* the same. The statute does not use a separate phrase to describe the range of harm relevant to conduct that "causes" harm and that relevant to conduct that is "likely to cause" harm; it uses the phrase only once.[145] To reimport the risk component into the word "substantial" following the word "likely" makes no syntactic sense: "likely to cause" already encompasses the class of injuries comprising increased risk of harm. The only viable reading of this language is that conduct is actionable only when it both *likely* causes injury and when that injury is *substantial*.

Although the Unfairness Statement does note in footnote 12 that "[a]n injury may be sufficiently substantial . . . *if it raises a significant risk of concrete harm,*"[146] "raises" clearly does not mean "increases the degree of" here, but rather "stirs up" or "gives rise to."[147] If it meant the former it would refer to injury that "raises the risk of harm" or that "raises the significance of the risk of harm." Additionally, the relevant risk in footnote 12 is deemed to be "significant," not "substantial," suggesting it was intended to be of a different character.[148] Moreover, that passage conveys the Commission's direction to address inchoate harms under Section 5—conduct "likely" to cause harm.[149] As such, footnote 12 was incorporated into Section 5(n) by inserting the words "or is likely to cause" in the phrase "causes . . .

---

141 FTC LabMD Opinion, *supra* 4, at 21.

142 FTC LabMD Opinion, *supra* 4, at 21.

143 *See generally* 15 U.S.C. § 45(n).

144 *See generally* 15 U.S.C. § 45(n).

145 *See generally* 15 U.S.C. § 45(n).

146 FTC LabMD Opinion, *supra* 4 (quoting Unfairness Statement, at 1073 n.12) (emphasis added).

147 *Raise*, MERRIAM-WEBSTER DICTIONARY (New Ed., 2016).

148 Unfairness Statement, *supra* note 39, at 1073 n.12.

149 Unfairness Statement, *supra* note 39, at 1073 n.12.

substantial harm."[150] Importing it *again* into the determination of substantiality is a patently unreasonable reading of the statute and risks writing the substantial injury requirement out of the statute.

At first blush, the FTC's proposed multiplication function may sound like the first half of footnote 12, but these are two very different things. Indeed, the fact that the footnote proposes a multiplication function for interpersonal aggregation of harms, but then, in the next breath, says no such thing about multiplying small risks times large harms,[151] can have only one meaning: the Policy Statement requires the FTC to prove the substantiality of harm, independent of its risk. Had Congress intended for the rather straightforward strictures of 5(n) to accommodate the large loophole proposed by the FTC, it surely would have spoken affirmatively. But, it did not. Instead, as is evident from the plain text of the statute, Congress structured Section 5(n) as a meaningful limitation on the FTC's potentially boundless unfairness authority.

The Commission claims that:

> [T]he Third Circuit interpreted Section 5(n) in a similar way in Wyndham.[152] It explains that defendants may be liable for practices that are likely to cause substantial injury if the harm was 'foreseeable,' . . . focusing on both the 'probability and expected size' of consumer harm.[153]

But the *Wyndham* court did *not* declare that the first prong of Section 5(n) requires that the magnitude of harm be multiplied by the probability of harm when evaluating its foreseeability; instead, the court included the magnitude of harm as one consideration in the *full* cost-benefit analysis implied by the *entirety* of Section 5(n):

> [T]his standard informs parties that the relevant inquiry here is a cost-benefit analysis . . . that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity.[154]

This is not the same as the Commission's proffered approach. The Third Circuit essentially recited the elements of a complete evaluation of Section 5(n), *not* the requirements for evaluating the first prong of the test.[155]

---

150 *See generally* Unfairness Statement, *supra* note 39.

151 Unfairness Statement, *supra* note 39, at 1073 n.12.

152 FTC LabMD Opinion, *supra* 4, at 21 (internal citations omitted).

153 *Id.* (internal citations omitted).

154 Wyndham, 799 F.3d at 255 (internal citations omitted).

155 *See generally id*.

Consequently, under the Commission's view of Section 5, the FTC has the power to punish entities that *have never had a breach*, since the mere *possibility* of a breach is a "likely" harm to consumers, provided the harm is substantial enough—and it invariably is.[156] As the Commission claims:

> Finally, given that we have found that the very disclosure of sensitive health or medical information to unauthorized individuals *is itself a privacy harm*, LabMD's sharing of the 1718 file on LimeWire for 11 months was also highly likely to cause *substantial* privacy harm to thousands of consumers, in addition to the harm actually caused by the known disclosure.[157]

The position that the Commission upholds in the *LabMD* opinion was plainly put forward by Complaint Counsel in its oral arguments before the ALJ, and rejected by him: merely storing sensitive data and "plac[ing data] at risk, "*any risk*, is all that is required to meet the standard of unfairness under Section 5.[158] Consider the following exchange between ALJ Chappell and Complaint Counsel:

> JUDGE CHAPPELL: So again, mere failure to protect, is that a breach of or is that a violation of section 5?
>
> COMPLAINT COUNSEL: A failure to protect, Your Honor, that places at risk consumer data—and by "consumer data" of course I don't just mean any data but the most sensitive kinds of consumer data, Social Security numbers, dates of birth, health insurance information and laboratory test codes—that increases the risk that that information will be exposed."[159]
>
> Under this interpretation, merely collecting data "increases the risk that information will be exposed" beyond the risk if data is not collected; storing it for n+1 days increases the risk beyond storing it for n days, and so on.

B. *The Absence of Any Real Substantiality Of Harm Requirement (Whether It Is "Likely" Or Not)*

Of course, even under the FTC's interpretation of Section 5, the magnitude of the threatened injury must be "substantial."[160] As noted, however, the FTC's logic implies that breach alone, even absent specific injury to consumers, monetary or otherwise, can constitute injury—and, in circular fashion, a heightened *risk* of breach, from merely collecting data, can constitute likely injury. Even more troublingly, such a risk can itself constitute a *psychic* harm.

---

156 *See generally* FTC LabMD Opinion, *supra* note 4.

157 FTC LabMD Opinion, *supra* note 4, at 25 (emphasis added).

158 Transcript of Oral Argument at 4-5, LabMD, Inc., Docket No. C-9357 (Sept. 16, 2015), https://laweconcenter.org/wp-content/uploads/2018/10/Lab-MD-Admin-Judge-Closing-Args.pdf.

159 *Id.* (emphasis added).

160 *See generally* FTC LabMD Opinion, *supra* note 4.

Although we cannot be sure from either the Commission's opinion or the Complaint Counsel's closing arguments before the ALJ *how large* a data collection practice is sufficient to be deemed "substantial," [161] there is some evidence in the FTC's consent decrees suggesting that it's not very much. On the one hand, some consent decrees don't even identify how much data is at issue—suggesting either that the FTC did not know or did not care. On the other, some of the cases clearly, or explicitly, involve small amounts of data.[162]

But the FTC Act does not explicitly grant the FTC authority to pursue "trivial or merely speculative harms," regardless of how likely they are to arise.[163] And in a 1982 letter to Senators Packwood and Kasten, FTC Chairman Miller further defined the Commission's approach to unfairness as "concern[ed] . . . with substantial injuries[,]" noting that the Commission's "resources should not be used for trivial or speculative harm."[164] Congress has similarly recognized the need for some meaningful limitation on the requirements of what counts as a likely harm: "In accordance with the FTC's December 17, 1980, letter, substantial injury is not intended to encompass merely trivial or speculative harm . . . . Emotional impact and more subjective types of harm alone are not intended to make an injury unfair."[165]

Commissioner Swindle did recognize in his *Touch-Tone* dissent some "subjective" contexts in which the disclosure of sensitive data could be a harm, even without tangible financial injury.[166] For instance, he noted that in other contexts the Commission had identified a "substantial injury stemming from the unauthorized release of children's personally identifiable information as being the risk of injury to or exploitation of those children by pedophiles."[167] Thus, while Section 5 unfairness authority isn't limited to cases where there is only tangible harm, at least some minimal level of analysis is required in order to connect challenged conduct with alleged harm.

Among settled cases, however, the line between what is a harm and what is not can often be rather blurred. In theory, proper economic analysis of the actual and expected costs and benefits of conduct can illuminate the

---

161 *See generally* FTC LabMD Opinion, *supra* note 4; ALJ LabMD Initial Decision, *supra* note 17.

162 Manne & Sperry, *supra* note 42, at 22.

163 Unfairness Statement, *supra* note 39, at 1073 (Similarly, the Unfairness Statement notes that "[u]njustified consumer injury is the primary focus of the FTC Act" and such injury cannot be "trivial or merely speculative.")

164 Letter from FTC Chairman J.C. Miller, III to Senator Packwood and Senator Kasten (March 5, 1982), reprinted in H.R. REP. No. 156, Pt. 1, 98th Cong., 1st Sess. 27, 32 (1983).

165 S. REP. NO. 103-130, at 13 (1994).

166 FED. TRADE COMM'N, Statement of Commissioner Orson Swindle, *In re* Touch Tone, File No. 982-3619 at 3-4 (Apr. 22, 1999).

167 *Id.* at 3 n. 7.

distinction—and do so in accordance with the statute. Yet the FTC regularly falls short of meaningful analysis.

Even in *Wyndham*, where the FTC had a relatively strong set of facts to work with, it couldn't resist the urge to manufacture elements of consumer harm.[168] The Commission asserted that every consumer whose information was exposed was harmed because, among actual harms like identity theft, there were losses associated with "cash-back, reward points, and other loyalty benefit programs."[169] It is not that the loss of these amenities *cannot* constitute harm; it is, rather, that the harm was simply asserted, and asserted across the board, without any effort to quantify or even evaluate whether or how much such inchoate losses might affect different cardholders.

And although not in an enforcement context, the FTC's 2014 Data Brokers Report at many points captures the FTC's general approach to highly speculative harms; for instance, it recommended that Congress enact legislation to prevent possible harms to consumers when having their identity verified as part of applications for things like mobile phones.[170] But the report explicitly notes that:

> The Commission does not have any information on the prevalence of errors in the consumer data that underlie data brokers' risk mitigation products. In a different context, a recent Commission Report assessed the accuracy of consumer information in credit reports and found that 5.2% of consumers had errors on at least one of their three major credit reports that could lead to them paying more for products such as auto loans and insurance.[171]

As Commissioner Wright noted in "dissenting" from various assertions in the Data Brokers Report "this recommendation is premature because there is no evidence about the existence or scope of this hypothetical problem. As noted in supra note 95, the Commission does not have any information on the prevalence of errors in the consumer data that underlie data brokers' risk mitigation products."[172]

Nevertheless, the Commission felt confident to recommend legislation that could affect millions of consumers and thousands of businesses without any direct support for its feared harms, and where, even in the meager evidence it drew from a "related" context, only a small handful of consumers experienced an unknown degree of harm. As Commissioner Wright further noted, "[I am] wary of extending FCRA-like coverage to other uses and

---

168 *See generally* Wyndham, 799 F.3d 236.

169 Plaintiff's Responses and Objections to Defendants' Fourth Set of Requests for Admissions at 12, FTC v. Wyndham Worldwide Inc., 799 F.3d 236 (3d Cir. 2015).

170 FED. TRADE COMM'N, Statement, Data Brokers: A Call for Transparency and Accountability (May 2014) [hereinafter Data Brokers Report].

171 *Id.* at 53 n. 95.

172 *Id.* at 54 n. 96.

categories of information without first performing a more robust balancing of the benefits and costs associated with imposing these requirements."[173]

C. *Section 5 "Harms": Costs Without Benefits*

The Commission's willingness to regard the existence of harm, or the risk of harm, without more, as the beginning and end of liability under Section 5's authority is also decidedly problematic. While a firm that does a poor job protecting users' data may deserve to be penalized, such a conclusion is impossible absent evaluation of the benefits conferred by the same conduct that risks consumers' data and the benefits the firm may confer by investing the saved costs of heightened security elsewhere. As the Commission has itself committed, it "will not find that a practice unfairly injures consumers unless it is injurious in its *net* effects."[174] In practice there is little or no evidence that the Commission evaluates net effects.

Of crucial importance, the FTC's unbalanced approach to evaluating the costs and benefits of data security dramatically over-emphasizes the risks of data exposure–not least by treating even the most trivial risk as potentially actionable–and fails to evaluate at all, at least publicly, the constraints on innovation and experimentation imposed by its effectively strict-liability approach. Even if one concludes that the FTC has the correct approach in general—i.e., that it is preferable for the agency to adopt an approach that errs on the side of preventing data disclosure—this still says nothing about how this approach should be applied in specific instances. Unless we are to simply accede to the construction of Section 5 as a strict liability statute, the Commission must put down some markers that clearly allow for a consideration of the *benefits* of imperfect data protection along with the attendant costs.

Consider the recent FTC complaint against D-Link in which it claims that:

> [D-Link] repeatedly . . . failed to take reasonable software testing and remediation measures to protect their routers and IP cameras against well- known and easily preventable software security flaws, such as "hard-coded" user credentials and other backdoors, and command injection flaws, which would allow remote attackers to gain control of consumers' devices; Defendant D-Link has failed to take reasonable steps to maintain the confidentiality of the private key that Defendant D-Link used to sign Defendants' software, including by failing to adequately restrict, monitor, and oversee handling of the key, resulting in the exposure of the private key on a public website for approximately six months; and . . . Defendants have failed to use free software, available since at least 2008, to secure users' mobile app login

---

173 *Id.* at 52 n. 88.

174 Unfairness Statement, *supra* note 39, at 1075 (emphasis added).

> credentials, and instead have stored those credentials in clear, readable text on a user's mobile device.[175]

What the complaint assiduously avoids is describing the calculation that led the FTC to determine that D-Link failed to take "reasonable steps."[176] It is possible, of course, that D-Link's security design decisions that, for instance, led it to avoid using encrypted credentials versus storing them locally in plain text were unsupported by any business case. But the opposite is also true, and the cost savings, or other possible benefits, of such decisions may outweigh the costs. Yet the complaint fails to evidence any evaluation of relative costs and benefits, concluding simply that D-Link's actions "caused, or are likely to cause, substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition."[177] As D-Link's Motion to Dismiss notes:

> Pleading this element as a legal conclusion, as the FTC has done here, is insufficient. With the sole exception of a passing reference to "free software," the Complaint contains no factual allegations whatsoever regarding the monetary costs, let alone the time- and labor-related costs, of conducting whatever "software testing and remediation measures" and other actions the FTC believes Defendants should have implemented.[178]

So too the FTC avoids recognizing that the security decisions made for an Internet-connected appliance used behind a Wi-Fi network would have a different set of security and safety considerations than a camera that streams to the open Internet. And, most important, it completely fails to address whether and how D-Link's behavior objectively failed to live up to an identifiable standard of conduct, because, as noted, the FTC has never offered any such standard to begin with.

The FTC's claims are thus insufficient both to meet even its own "reasonableness" standard—let alone Section 5's cost-benefit requirement—as well as to provide, or reflect, any sort of discernible standard that, applied here, would permit a firm to determine what conduct that may lead to harm will nevertheless offer sufficient benefit to avoid liability. And, indeed, the court recognized precisely this failing and dismissed many of the FTC's claims from the case:

> The pleading problem the FTC faces concerns the first element of injury. The FTC does not allege any actual consumer injury in the form of a monetary loss or an actual incident where sensitive personal data was accessed or exposed. Instead, the FTC relies solely on the likeli-

---

175 Complaint at 5, FTC v. D-Link Corp., No. 3:17-CV-00039-JD (N.D. Cal. Mar. 20, 2017) [hereinafter D-Link Complaint].

176 *See generally id.*

177 *Id.* at 29.

178 Defendant Motion to Dismiss at 8, FTC v. D-Link Corp., No. 3:17-CV-00039-JD (N.D. Cal. Jan. 31, 2017).

> hood that DLS put consumers at "risk" because "remote attackers could take simple steps, using widely available tools, to locate and exploit Defendants' devices, which were widely known to be vulnerable."[179]

Echoing the ALJ's Initial Decision in the *LabMD* case, the court goes on to note that these are "effectively the sum total of the harm allegations, and they make out a mere possibility of injury at best."[180] Relying on *Twombly*, the court noted the insufficiency of the FTC's unfairness pleading because "[t]he absence of any concrete facts makes it just as possible that [D-Link's] devices are not likely to substantially harm consumers, [on net,] and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor."[181] And again, highly reminiscent of the problematic theory of harm in *LabMD*, the judge noted that "[t]he lack of facts indicating a likelihood of harm is all the more striking in that the FTC says that it undertook a thorough investigation before filing the complaint . . . ."[182]

In fact, the Commission consistently avoids taking seriously the thoroughness of the required investigation and analysis sufficient to determine whether the costs, i.e., foregone benefits, of incremental increases in harm avoidance are merited. In its Privacy Report, for instance, the Commission says that "[i]n terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace."[183] In other words: there are costs to the data security requirements we might adopt, and there are benefits. Because we assert that *some* benefit exists, the magnitude of the costs we impose do not matter. One would search the document in vain for a more-rigorous statement of how, or whether, the FTC will weigh the costs and benefits of data security practices; it just is not there, which is odd for a purported "framework" adopted in accordance with a statute that *explicitly* demands such a weighing. As Commissioner Rosch pointedly noted, dissenting from the FTC Privacy Report:

> There does not appear to be any . . . limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world. That is not only paternalistic, but it goes well beyond what the

---

179 FTC v. D-Link Sys., Inc., No. 3:17-CV-00039-JD, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017)

180 *Id.* at 5.

181 *Id.*

182 *Id.*

183 FTC PRIVACY REPORT, *supra* note 128, at 8.

> Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[184]

But the FTC Privacy Report was just that—a report, in theory at least. Although replete with language that the contents represent "best practices" and are meant to assist companies in devising their own privacy and security practices, in reality the FTC Privacy Report reads like a set of vague commands from the Commission that will undoubtedly form the basis for enforcement actions in the future. The Commission does assert in the FTC Privacy Report that "the privacy framework is designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue."[185] But as we have shown elsewhere, the FTC's past actions and imposed remedies belie this claim:

> What is clear is that, almost without regard to *any* underlying characteristics, size of injury, number of injured parties, etc., an almost identical set of practices is prescribed by the agency to remedy alleged unreasonableness in data security, meaning, no matter what industry, size, or extent of possible harm, every business regulated by the FTC should know what is expected of it. The FTC has been remarkably consistent in this.
>
> Now, we believe this is actually a *bad* thing. The absence of any apparent connection between different circumstances and different remedies—or, put differently, the absence of any explanation why very different circumstances are properly addressed by the very same data security processes—is never much explained and hasn't evolved in over a decade. The likelihood that this consistency reflects the optimal outcome is extremely low.[186]

Emblematic of the FTC's failure to account for benefits of challenged conduct as well as harms is the Commission's *Apple* product design case.[187] In that case, the Commission brought charges against Apple for allegedly designing the iOS app store in a way that led to "unfair" billing practices.[188] Historically, the Commission would bring such cases where a defendant affirmatively endeavored to mislead consumers, including cases of outright fraud, unauthorized billing, and cramming.[189] In the *Apple* case, however, the Commission alleged not that Apple engaged in irredeemably bad conduct, but rather that it had designed the App Store in a way that made it too easy for children to make purchases without parental consent[190] by permit-

---

184 *Id.* at C-5 (J. Thomas Rosch, Comm'r, dissenting).

185 *Id.* at 9.

186 Manne & Sperry, *supra* note 42, at 12-13.

187 *In re* Apple Inc., 112-31008, 2014 WL 253519, at *1 (MSNET Jan. 15, 2014).

188 *Id.* at *5.

189 *See generally id.*

190 *Id.* at *1.

ting password-free purchases and downloads during a 15 minute window once a user had entered her password.[191]

This case highlights a crucial part of the FTC's mandate embodied in Section 5(n) that is all too frequently ignored: a likely harm can be deemed "unfair" only if there are insufficient countervailing benefits from the challenged practice, and if consumers could not themselves reasonably avoid the harm.[192] But in *Apple* the FTC did not evaluate the potential, broad benefits of Apple's design decisions and essentially replaced its own judgment for that of Apple's—a company whose very existence depends upon it making products for which consumers are willing to pay.

In other words, the Commission completely failed to perform an adequate analysis to determine if the "harm" suffered by the relatively small number of parents of children who were able to make a purchase within the 15-minute window was counterbalanced by the greater degree of convenience that an overwhelming number of consumers enjoyed by virtue of the feature. Moreover, there was scant attention paid to assessing whether parents themselves were actually unable to avoid the potential harm, despite the likelihood of their proximity to their phones and their children. Nonetheless, Apple settled, despite the fact that the company had likely performed a wealth of its own consumer research in order to discover the optimal balance of features for its products. It would be surprising indeed if the ambiguity implicit in the loosely interpreted unfairness standard played no part in the decision to settle.

D. *On Occasion, Only The Barest Of Benefits*

Even where the Commission does advert to possible benefits from a firm's risk-increasing conduct, it does so in a crabbed and insufficient fashion. In its *LabMD* opinion, for instance, the Commission stated that:

> A "benefit" can be in the form of lower costs and then potentially lower prices for consumers, and the Commission "will not find that a practice unfairly injures consumers unless it is injurious in its net effects.". . . This cost-benefit inquiry is particularly important in cases where the allegedly unfair practice consists of a party's failure to take actions that would prevent consumer injury or reduce the risk of such injury . . . . When a case concerns the failure to provide adequate data security in particular, "countervailing benefits" are the foregone costs of "investment in stronger cybersecurity" by comparison with the cost of the firm's existing "level of cybersecurity." . . . [W]e conclude that whatever savings LabMD reaped by forgoing the expenses needed to remedy its conduct do not outweigh the "substantial injury to consumers" caused or likely to be caused by its poor security practices.[193]

---

191 *Id.* at *5.

192 15 U.S.C. § 45(n).

193 FTC LabMD Opinion, *supra* note 4, at 26.

This construction assumes that the inquiry into countervailing benefits is strictly limited to the question of the direct costs and benefits of the data security practices themselves. Of course this can't be correct. The potential benefits to consumers are derived from the business *as a whole*, and the data security practices of the business are just one component of that. The proper tradeoff isn't between more or fewer resources invested in making data security practices "reasonable," as if those resources materialize out of thin air. Rather, the inquiry must assess the opportunity costs that a business faces when it seeks to further a certain set of aims—chief among them, serving customers—with limited resources.

A proper standard must also take account of the cost to LabMD, not only of adopting more stringent security practices, but also of identifying and fixing its security practices *in advance* of the breach. It may be relatively trivial to identify a problem and its solution after the fact, but it's another matter entirely to ferret out the entire range of potential problems ex ante and assign the optimal amount of resources to protect against them based on necessarily unreliable estimates of their likelihood and expected harm. And this is all the more true when the "problem" is an unknown thief intent on quietly constructing exactly the sort of problems that would catch the attention of the FTC.

No doubt LabMD could have done *something* more to minimize the likelihood of the breach. But it's not clear that any reasonable amount of time or money could have been spent in advance to identify and adopt the *right* something under the FTC's strict-liability-like standard. As former Commissioner Wright noted in his dissent in the *Apple* case:

> When designing a complex product, it is prohibitively costly to try to anticipate *all* the things that might go wrong. Indeed, it is very likely impossible. Even when potential problems are found, it is sometimes hard to come up with solutions that that one can be confident will fix the problem. Sometimes proposed solutions make it worse. In deciding how to allocate its scarce resources, the creator of a complex product weighs the tradeoffs between (i) researching and testing to identify and determine whether to fix potential problems in advance, versus (ii) waiting to see what problems arise after the product hits the marketplace and issuing desirable fixes on an ongoing basis . . . . The relevant analysis of benefits and costs for allegedly unfair omissions requires weighing of the benefits and costs of discovering and fixing the issue that arose *in advance* versus the benefits and costs of finding the problem and fixing it *ex post*.[194]

Moreover, while *some* LabMD patients might have net benefited from heightened data security along with higher prices or reduced quality along some other dimension in exchange for it, it is by no means clear that all LabMD patients would so benefit. As Commissioner Wright also discussed at length in his *Apple* dissent, an appropriate balancing of countervailing benefits would weigh the costs of greater security to marginal patients–

---

[194] *In re* Apple, Inc., 15-16 (Jan. 15, 2014) (No. 12-31008) (Joshua D. Wright, Comm'r, dissenting), https://www.ftc.gov/sites/default/files/documents/cases/140115applestatementwright_0.pdf.

those for whom LabMD's services plus the FTC's asserted "reasonable" security practices at a higher price would have induced them to forego using LabMD– against the benefits to infra-marginal patients who would have been willing to pay more to have the FTC's imposed security practices.

> Staff has not conducted a survey or any other analysis that might ascertain the effects of the consent order upon consumers. The Commission should not support a case that alleges that [LabMD] has underprovided [data security] without establishing this through rigorous analysis demonstrating – whether qualitatively or quantitatively – that the costs to consumers from [LabMD's data security] decisions have outweighed benefits to consumers and the competitive process.
>
> . . .
>
> The Commission has no foundation upon which to base a reasonable belief that consumers would be made better off if [LabMD] modified its [security practices] to conform to the parameters of the consent order. Given the absence of such evidence, enforcement action here is neither warranted nor in consumers' best interest.[195]

Unfortunately for the FTC, making this assessment would require surveying consumers or estimating the harm caused–or likely to be caused, and discounted by the likelihood–and its magnitude, as well as the *ex ante* costs of identifying the possible harm and preventing it. But because the FTC has steadfastly adopted its "all inferences without evidentiary support" framework, it neither has, nor is it willing to entertain even estimating, that evidence. Thus, again, in the end, the practical effect is to convert Section 5 into a strict liability statute in which any breach or potential breach runs the risk of FTC scrutiny, regardless of what steps were taken or could have been taken.

E. *The FTC's Interpretation of "Likely to Cause" Gives it a Temporally Unbounded Power Over Every Company*

Finally, LabMD (in our opinion, correctly) argued that the scope of a "likely to cause" authority must be bounded in some fashion in order to create some meaningful limitation on the FTC's power to police conduct.[196] In essence, the phrase "likely to cause" needs to be constrained in a way that focuses the FTC's authority on a contextually relevant period of time. LabMD argued that the relevant time period begins upon the issuance of an order; if conduct was no longer ongoing at the time an order was issued, the

---

195 *Id.* at 14, 17.

196 LabMD 11th Cir. Petitioner Brief, *supra* note 12, at 22-23.

Commission had no power to find that a respondent was "likely to cause" harm.[197]

In its turn, the Commission offered a textual analysis suggesting that the whole of Section 5 taken together indicates that the "likely to cause" language does not restrict the FTC to a persistently forward-looking analysis.[198] Further, the Commission argued that allowing respondents to alter their conduct in expectation of an investigation would permit "malfeasors to evade FTC enforcement by stopping their illegal behavior upon learning of an FTC investigation."[199]

The FTC has some basis for the textual argument that it has the ability under Section 5 to assess prospective conduct by looking at a past time period; surely past conduct and its consequences are relevant to the Commission's assessment of current or future conduct and *its* likely consequences. But it goes too far to suggest that this examination must be unbounded in order to prevent malfeasors from acting with impunity.

Once a complaint has been issued, any conduct that is "is likely to cause" harm is a proper target of action for the Commission. But it stretches the limits of language to say that conduct that "*is* likely *to cause*" harm may also be read to encompass conduct that "*was* likely to *have* caus*ed*" harm. Other than, as noted, in the sense that past conduct and its effects may inform the Commission's assessment of the likely effect of current or future conduct, it seems impossible to read such retroactivity into the plain language of the statute. Such an unbounded reading would—dangerously—allow the FTC regulate any behavior, of any company, that has possessed data since the creation of Section 5, or at least since it started policing data security.

In *LabMD*, the FTC used its authority to pursue a company that was "likely to [have] cause[d]" harm *after* the company had already remedied its behavior, and before the FTC ever instituted an investigation.[200] Under this reading of Section 5, there is nothing to stop the FTC from looking back at, for instance, Amazon in the year 2001 and issuing a new complaint against it because something it had done then could have injured consumers but didn't, and even though Amazon had long since identified and rectified the alleged harm. On the FTC's account, if a firm has remedied its conduct *even before the FTC investigates it*, that firm should be liable under an "is likely to cause" harm theory.

As noted above, however, the FTC does not have the power to exact punitive remedies, e.g., fines, from its enforcement power, but only to correct wrongful conduct and, by so doing, prospectively to deter future bad conduct. But where bad conduct has stopped, whether because of the

---

197 *Id.* at 23.

198 FTC 11th Cir. Respondent Brief, *supra* note 58, at 35-36.

199 *Id.* at 36.

200 *See generally* FTC LabMD Opinion, *supra* note 4.

FTC's enforcement or because of the threat of it, there is no ongoing harm to consumers for the Commission to correct.

Thus, absent the ability to deter malfeasors through the imposition of fines, the Commission's concern that placing temporal bounds on its "likely to cause" authority will allow malfeasors to evade enforcement seems perverse. At least theoretically, the purpose of the FTC is to encourage private firms to do the right thing in the first place, to induce them not to injure consumers without need of a specific FTC enforcement action. Yet the FTC appears to be concerned that if a firm fears an investigation and remedies its bad conduct, the Commission will be powerless to perform its mission, as if to say that a firm that voluntarily remedies its conduct because of the risk of an enforcement action is "getting away" with something. Such a reading would require one to believe that voluntary, desirable conduct undertaken in the shadow of the law somehow constitutes actionable, illicit activity—a perversity that Congress cannot have intended.

V. CONCLUSION

The FTC aims to develop its data security enforcement practices as a kind of common law, and this is a laudable goal. But the procedural and substantive problems with its enforcement of data security cases to date provides the worst of both worlds: cases are brought under the opaque preferences of regulators, with the final results of such enforcement actions published to the world in allegedly binding "precedent" that actually contains none of the necessary connections between conduct and injury sufficient to guide actors in the economy at large. As the Eleventh Circuit noted in *LabMD*, the Commission is apparently aiming at something like a negligence standard[201]—which we support—but in order to usefully operationalize that standard, the Commission needs to better elaborate the claims it brings, and seek to use those cases to establish real, binding precedent.

Although there are a number of procedural reforms that would undoubtedly help,[202] the FTC is currently perfectly capable of conducting its data security investigations and enforcement actions in a way that would comport with traditional negligence analysis and thereby cure many of the defects in its current process. To begin with, it seems apparent that the FTC must introduce some concrete, publicly available standards–and well-defined safe harbors–from which firms can reliably determine whether their

---

201 *See generally* LabMD, Inc., 894 F.3d 1221.

202 *See* Berin Szóka & Geoffrey Manne, *The Federal Trade Commission: Restoring Congressional Oversight of the Second National Legislature, An Analysis of Proposed Legislation,* (FTC: TECHNOLOGY & REFORM PROJECT, May 2016), https://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf.

conduct comports with their duties with respect to data they possess and the likely risk of harm of a breach, given the relevant facts of their business activities. Included among these should be a clear statement regarding whether and how mere possession of data could lead to liability, the magnitude of increased risk that will constitute "likely" harm, and clear standards for measuring it. We are sympathetic to the criticism of published guidelines that technology changes quickly and thus published, ex ante standards may be both under- and over-inclusive, especially over time. But merely telling firms to behave "reasonably" without more given the virtually unconstrained scope of the FTC's discretion and its current processes seems woefully insufficient as a guide to firms' increasingly important duties under the law with respect to their customers' data.

Perhaps most critically, the FTC should both enunciate and follow clear standards of proof of causation in its data security enforcement decisions. It is impossible to have perfect data security, and some number of breaches will always occur, even under the best of circumstances. Without true guidance as to when a particular breach was proximately "caused" by insufficient security, FTC enforcement will continue to appear arbitrary. This is even more important in cases where the FTC chooses to rely on its "likely to cause" authority: Without a well-established connection between any given set of data security practices and their ability to constitute a proximate cause of "likely" harm, Section 5 becomes an unbounded source of enforcement authority, virtually regardless of the measures that firms take to protect data.

Without this guidance, the Commission's enforcement philosophy will remain decidedly fatalistic and effectively imply that data security practices sufficient to meet the standard of Section 5 are impossible. This status quo is untenable insofar as it means that once a company collects sensitive data it may be presumptively in violation of the statute, with only the vagaries of prosecutorial discretion to separate legal and illegal conduct. Likewise when breaches actually occur, the FTC's position is improper: Inferring unreasonable security practices from the fact of unauthorized disclosure alone, without any demonstration of concrete harm or even rigorous assessment of the *likelihood* of harm, effectively converts Section 5 into a strict liability standard, in clear contravention of the statute.

HOW MUCH SHOULD WE SPEND TO PROTECT PRIVACY?: DATA BREACHES AND THE NEED FOR INFORMATION WE DO NOT HAVE

Robert H. Sloan[*] *and Richard Warner*[**]

INTRODUCTION

A cost/benefit analysis approach to privacy concerns raises two tradeoff issues. One is making appropriate tradeoffs between privacy and the many goals served by the collection, distribution, and use of information. The other is making tradeoffs between investments in security, that is, in preventing unauthorized access to information, and a variety of other goals. Much has been written about the first tradeoff. We focus on the second. The issue is critical. Data breaches occur at the rate of over three a day.[1] The aggregate social cost is high. One recent study puts the average cost of a breach for a business at $4 million.[2] Such estimates are controversial,[3] but it is clear that breaches impose significant losses on businesses,[4]

---

[*] Professor and Head, Department of Computer Science, University of Illinois at Chicago. Partially supported by National Science Foundation Grant No. DGE-1069311.

[**] Professor of Law, Chicago-Kent College of Law, Visiting Foreign Professor, University of Gdańsk, Poland.

[1] IDENTITY THEFT RESOURCE CENTER, *Data Breaches*, https://www.idtheftcenter.org/data-breaches/ (last viewed Dec. 4, 2018). The Identify Theft Resource Center (ITRC) uses a narrow definition of a breach: a data breach is "an incident in which an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure." Unauthorized access to computers and networks can be "potentially put at risk because of exposure" a great deal of other sorts of sensitive information, so data breaches would be even more common on the correspondingly broader understanding of breach. Whatever the exact breach rate, there are enough breaches to impose significant costs on society.

[2] PONEMON INST., COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (2016), https://www.ibm.com/security/data-breach/ [hereinafter *Cost of Data Breach Study*]. That $4 million is Ponemon's estimate of *data breach* costs as defined in the study and is up from its estimates in previous years. Its 2015 study of *cybercrime* costs defines those costs more broadly and estimates them at $7.7 million per business annually. PONEMON INST., 2015 COST OF CYBER CRIME STUDY: GLOBAL ANALYSIS (2015), http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

[3] *See, e.g.*, Maria Korolov, *$154 or 58 cents -- what's the real cost of a breached data record?*, CSO ONLINE (Jun 5., 2015, 6:29 AM), http://www.csoonline.com/article/2931839/data-breach/154-or-58-cents-whats-the-real-cost-of-a-breached-data-record.html.

[4] In 2014, the aggregate loss in the United States from identity theft was around $15.4 billion. Erika Harrell, *Victims of Identity Theft, 2014* 7 (Bureau of Just. Stat., Sept. 2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf. Earlier United States estimates of the cost of identity

consumers,[5] and society.[6] Security experts have long explained how to better defend against security breaches.[7] So, why does society tolerate a significant loss that it has the means to avoid?

Some may object that society does *not* tolerate breaches. After all, laws—current and proposed—impose requirements aimed at improving information security. However, there are information security laws that "obligate companies to establish and maintain 'reasonable' or 'appropriate' security procedures, controls, safeguards, or measures, but give no further direction or guidance."[8] The courts have not clarified the situation; there are no cases that establish what standards of care an organization must adopt with regard to data security.[9]

---

theft alone are also in the billions. For a summary of relevant studies, *see* Fred H. Cate, *Information Security Breaches and the Threat to Consumers* 6, (Ctr. for Info. Pol'y Leadership at Hunton & Williams, Sept. 2005), http://www.repository.law.indiana.edu/facpub/1291
(reporting 10.1 million victims of identity theft in 2003 and total losses to consumers of over 50 billion). Identity theft estimates ignore non-identity theft losses from, for example, ransomware, denial of services attacks, botnets engaged in fraud and other illegal activities, and viruses. A United Kingdom government study with a broader focus estimates the yearly cost of data breaches to be £21bn to businesses, £2.2bn to government and £3.1bn to citizens. DETICA, THE COST OF CYBERCRIME 2 (Feb. 2011), http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf. For a follow-up study, *see* Ross Anderson et al., *Measuring the Cost of Cybercrime*, (Eleventh Workshop on Econ. of Info. Security, 2012), http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.

[5] Lillian Ablon et al., *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information*, (Rand Corp., 2016), https://www.rand.org/pubs/research_reports/RR1187.html.

[6] Society as a whole incurs costs as businesses and consumers spend time and effort responding to data breaches instead of directing that time and effort toward more productive ends. Governments also incur costs from funding criminal enforcement efforts and from the taxes they would have collected on revenue from projects that were not undertaken because the funding for them was spent on responding to data breaches.

[7] There are numerous undergraduate and graduate textbooks on computer security discussing how best to defend. *See, e.g.*, ROSS J. ANDERSON, SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS (2nd ed. 2008); CHARLES P. PFLEEGER, SHARI LAWRENCE PFLEEGER & JONATHAN MARGULIES, SECURITY IN COMPUTING (5th ed. 2015); WILLIAM STALLINGS & LAWRIE BROWN, COMPUTER SECURITY: PRINCIPLES AND PRACTICE (3rd ed. 2014); WILLIAM STALLINGS, NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS (6th ed. 2016). Both the SANS institute and Australian Department of Defense publish fairly short lists of critical security controls, and the Australian Department of Defense argues that simply adopting its top four would vastly improve the information security posture of most organizations, eliminating about 85 percent of all incidents. *See, e.g.*, Australian Cyber Security Centre, *Strategies to Mitigate Cyber Security Incidents*, https://acsc.gov.au/infosec/mitigationstrategies.htm (last visited Dec. 4, 2018); SANS Institute, *The CIS Critical Security Controls for Effective Cyber Defense,* http://www.sans.org/critical-security-controls/ (last visited Dec. 4, 2018).

[8] Thomas J. Smedinghoff, *Defining the Legal Standard for Information Security: What Does "Reasonable" Security Really Mean?*, SECURING PRIVACY IN THE INTERNET AGE 19, 23 (Chander, Gelman & Radin eds., 2008).

[9] Mark C. Mao, Ronald I. Raether, Jr. & Sheila M. Pham, *Data Privacy: The Current Legal Landscape* 9 (Troutman Sanders LLP, 2016),

Laws currently fail to provide an adequate incentive to improve information security. Why? One answer is that they fail to provide sufficient detail about what counts as reasonable precautions against data breaches. That answer is more wrong than right. Perhaps greater detail is called for in some cases, but the more fundamental problem is that businesses lack sufficient information to make the cost/benefit judgments on which reasonableness in this context largely depend. An essential part of adequately defending online data is ensuring that business have the necessary information.

In Section I, we distinguish between businesses protecting consumers from data breach losses and businesses protecting themselves from those losses. We focus on the latter in this section and identify three problems that partially explain businesses' poor self-defense. Only one of those problems, vulnerabilities in networks, raises lack of information concerns. We focus on that problem in Sections II to V. We turn to the defense of consumers in Section II. We argue that businesses should bear a considerable part of the defensive burden, and that they are unlikely to do so with some form of legal liability for consumer losses. We also argue, however, that imposing legal liability will be ineffective without a solution to the lack of information problem that plagues businesses' self-defense. Section III considers ways of improving data breach defenses without immediately acquiring the necessary information about data breaches. We consider relying on expert opinions, outsourcing security, and data breach notification laws. None of those items are fully adequate as a solution to defending against data breaches. Section IV proposes a regime of mandatory anonymous reporting of relevant information about data breaches.

I. INADEQUATE DEFENSE

Businesses fail to defend adequately against data breaches on two fronts. They fail to adequately defend consumers, and they fail to adequately defend themselves. The failure to defend consumers is hardly surprising. The problem is, of course, negative externalities. Profit driven businesses ignore customers' and third-parties' losses, unless those losses also impose significant losses on the business.[10] The point applies to cybersecurity. Organizations have

insufficient incentives to invest in strong data security and accountable privacy practices because, in essence, they didn't have to. Consider that lost or "stolen" customer or employee data often does not deprive an organ-

---

https://www.troutmansanders.com/files/Uploads/Documents/TS_Article_DataPrivacy-TheCurrentLegalLandscape_OCT_2016.pdf.

[10] Benjamin Dean et al., *Sorry Consumers, Companies Have Little Incentive to Invest in Better Cybersecurity*, QUARTZ (Mar. 5, 2015), http://qz.com/356274/cybersecurity-breaches-hurt-consumers-companies-not-so-much/.

ization of its continued availability or use, as would loss or theft of physical property. Further, the (negative) consequences of poor security and misused data fall mainly if not entirely upon individual victims, often at a later date.[11]

The result is that businesses fail to adequately approximate the following *consumer risk management goal*: choose the most effective defense meeting the condition that the defense investment is not greater than the expected consumer losses thereby avoided (over some appropriate time period).[12] We address the failure to defend consumers in Section II. This section considers business *self*-defense. The self-defense failure reveals the critical lack of information needed for adequate defense, and that same failure also plagues the defense of consumers.

A. *Business Self-Defense*

Businesses' self-defense is typically inadequate. As one commentator summed up the situation, "the bad guys basically go where they want to go and do what they want to do, and they're not being stopped. Maybe for every one organization that's effectively stopping attacks, there are 100 that are being breached."[13] Why is this happening? The puzzle is that the profit maximizing approach is to pursue the following *business risk management goal*: choose the most effective defense meeting this condition—the defense cost is not greater than expected business losses thereby avoided (over some appropriate short- or long-term time period).[14]

Why do businesses typically fail—and often fail badly—to meet the business risk management goal? There are different answers for different problems. The problems correspond, more or less, to three types of vulnerabilities. A vulnerability is a property of a program, computer, or network that hackers can exploit to gain unauthorized access. We divide vulnera-

---

11 Ann Cavoukian, *A Discussion Paper on Privacy Externalities, Security Breach Notification and the Role of Independent Oversight* 5-6 (Eight Workshop on Econ. of Info. Security, 2009), https://www.ipc.on.ca/wp-content/uploads/Resources/privacy_externalities.pdf.

12 Expected losses are the (estimated) actual losses discounted by the probability of their occurrence. For our purposes, it does not matter whether one interprets probability "objectively" as frequencies of occurrence or "subjectively" as degrees of belief. For an excellent discussion of the types of probability, *see* IAN HACKING, AN INTRODUCTION TO PROBABILITY AND INDUCTIVE LOGIC (2001).

13 George V. Hulme, *Security Spending Continues to Run a Step Behind the Threats*, CSO ONLINE (Oct. 16, 2013, 8:00 AM), http://www.csoonline.com/article/2134074/strategic-planning-erm/security-spending-continues-to-run-a-step-behind-the-threats.html.

14 Implementing this strategy faces significant problems in practice. It can be difficult to evaluate the effectiveness of various security measures. Relevant costs and benefits may not be quantifiable, and those that are may only be roughly and approximately so. In addition, costs and benefits may be quite difficult to predict.

bilities into these groups: software, human, and network. We focus on networks, as that is where the critical need for information arises.

B. *Three Types of Vulnerabilities, Three Different Problems*

1. Software Vulnerabilities

Mass-market software programs currently contain an unacceptable number of vulnerabilities. That is not inevitable. Software engineers know how to minimize, though alas not how to totally eliminate, vulnerabilities.[15] How to write individual computer programs well, and the basics of software engineering are fairly well-settled subjects.[16] The basics of high-quality code construction and software engineering generally form a significant fraction of the required core portion of the model computer science bachelor's degree curriculum jointly published by the two main professional societies for computer science in 2013,[17] and in earlier model curricula.[18]

---

15 Software is different from other engineered products in that sufficiently complex software inevitably has some programming flaws. As far back as the 1980s, a panel convened to study the issues with software for President Reagan's Strategic Defense Initiative noted, "Simply because of its inevitable large size, the software capable of performing the battle management task for strategic defense will contain errors. *All systems of useful complexity contain software errors.*" STRATEGIC DEF. INITIATIVE ORG., DEP'T OF DEF., 19980819-140, EASTPORT STUDY GROUP: SUMMER STUDY 1985, A REPORT TO THE DIRECTOR, 14 (1985), http://www.dtic.mil/dtic/tr/fulltext/u2/a351613.pdf (emphasis added). Software engineering expert Capers Jones notes that one goal of software engineering best practices is to increase the percentage of bugs removed prior to delivery from 85 percent to something that "approach[es] 99 percent," (*not* that it approaches 100 percent). CAPERS JONES, SOFTWARE ENGINEERING BEST PRACTICES: LESSONS FROM SUCCESSFUL PROJECTS IN THE TOP COMPANIES xxvi (2010). In contrast, design flaws are not inevitable in, for example, refrigerators, batteries, and bridges even when they exhibit considerable complexity. Software alone combines complexity and inevitable flaws. Thus, no matter how much one invests in development procedures designed to reduce programming flaws, flaws—and perhaps vulnerabilities—will remain.

16 However, the choice of *which* software engineering methodology is the best one for managing various sorts of projects is contentious. In particular, there is debate about the relative merits of a traditional methodology called the Waterfall Model, with its origins in the late 1960s, versus various other methodologies, such as Spiral or Agile. *See, e.g.*, David L. Parnas, *A Rational Design Process: How and Why to Fake it* 3, http://www.cs.tufts.edu/~nr/cs257/archive/david-parnas/fake-it.pdf (criticizing the Waterfall Model); Kent Beck et al., *Manifesto for Agile Software Development* (2001), http://agilemanifesto.org/ (outlining the Agile Model).

17 JOINT TASK FORCE ON COMPUTING CURRICULA, ASS'N FOR COMPUTING MACHINERY, IEEE COMPUTER SOC'Y, COMPUTER SCIENCE CURRICULA 2013: CURRICULUM GUIDELINES FOR UNDERGRADUATE DEGREE PROGRAMS IN COMPUTER SCIENCE (2013), https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf.

18 *See, e.g.*, JOINT TASK FORCE ON COMPUTING CURRICULA, ASS'N FOR COMPUTING MACHINERY, IEEE COMPUTER SOC'Y, COMPUTING CURRICULA 2001: COMPUTER SCIENCE (2001), https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf.

Years of studies confirm the common wisdom among experts in software development that proper attention to software development leads to lower defect rates.[19] So why is software so full of vulnerabilities? In large part because reducing vulnerabilities requires a longer and more costly development process. Consumers have been unwilling to pay for the added value of security through slightly higher retail prices and companies, dependent on consumer sales, don't offer what consumers don't want. "Businesses are profit-making ventures, so they make decisions based on both short- and long-term profitability,"[20] and the "market often rewards first-to-sell and lowest cost rather than extra time and cost in development."[21] The typical profit-maximizing strategy is to keep costs down and be the first to offer a particular type of software, even if it is imperfect in a variety of ways, including having vulnerabilities.[22] We discuss software vulnerabilities and a possible remedy in detail elsewhere.[23]

2. Human Vulnerabilities

The main human vulnerability is the human propensity to trust. Think of human vulnerabilities as an unwitting invitation to enter. Vampire movies are a nice analogy. In classic vampire movies, vampires can't enter a house unless invited in, so the audience cringes when some innocent person unwittingly asks the obvious-to-the-audience vampire to cross the threshold. Far too many invite hackers to cross the thresholds of their computers and networks allowing them to gain "access to buildings, systems or data

---

19 *See generally* Anthony Hall, *Seven Myths of Formal Methods*, 7 IEEE SOFTWARE 11, 11–19 (Sept. 1990) (discussing Praxis studies and the CASE project). *See also* I. J. Hayes, *Applying Formal Specification to Software Development in Industry*, SE-11 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 169, 175–76 (Feb. 1985) (discussing the usefulness of software engineering techniques in some particular projects); Alan MacCormack et al., *Trade-offs Between Productivity and Quality in Selecting Software Development Practices*, 20 IEEE SOFTWARE 78, 81–84 (Sept.–Oct. 2003) (comparing various software engineering techniques).

20 Bruce Schneier, *Information Security and Externalities*, SCHNEIER ON SECURITY (Jan. 2007), https://www.schneier.com/essays/archives/2007/01/information_security_1.html.

21 Eugene H. Spafford, *Remembrances of Things Pest*, 53 COMM. ACM 35, 36 (2010).

22 *See generally* C. SHAPIRO & H. R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 50–51 (1999). The economics and information security community has developed Shapiro and Varian's initial insights. Much of this work has been reported in the annual Workshop on the Economics of Information Security since 2002. For information on the workshops from 2002 to 2010, *see* http://weis2010.econinfosec.org/index.html. For a good general survey, *see* Ross Anderson & Tyler Moore, *Information Security: Where Computer Science, Economics and Psychology Meet*, 367 PHIL. TRANSACTIONS ROYAL SOC'Y A 2717, 2721–22 (2009).

23 *See* ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND INFORMATION SECURITY (2013); Richard Warner & Robert H. Sloan, *Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access*, 2012 UNIV. ILL. J. TECHNOL. LAW POLICY 45 (2012).

by exploiting human psychology."[24] Phishing is a good example. Phishing is the use of an electronic communication that masquerades as being from someone trustworthy in order to gain unauthorized access to information. For example, in a case study entitled, "Examining how a China-based threat actor stole vast amounts of PII," Mandiant notes that:

> Phishing attacks continue to be a theme year after year, and this case is no different. It began with a threat actor successfully enticing a user to follow a malicious link in a phishing email. The link downloaded a backdoor, providing the threat actor access to the victim's environment. Once the threat actor obtained a foothold, the reconnaissance activity was primarily centered on the identification of databases with the greatest volume of PII.[25]

Phishing is by no means the only way hackers masquerade themselves to exploit people's trust. Other examples include various other forms of social engineering[26] and Trojan horses.[27]

3. Vulnerabilities in Networks

The way to reduce human vulnerabilities is hardly a mystery. It is primarily a matter of adequate education and training.

There is no small set of vulnerabilities that accounts for all or most of the data breaches. Recent data breaches involve, among other things, misconfigured vendor access,[28] lack of encryption of data in motion,[29] lack of encryption of data at rest,[30] lack of basic use of firewalls,[31] and vulnerabilities in non-mass market infrastructure software. In the case of the Target

---

24 George V. Hulme & Joan Goodchild, *What is Social Engineering? How Criminals Take Advantage of Human Behavior*, CSO ONLINE (Aug. 3, 2017, 6:31 AM), https://www.csoonline.com/article/2124681/social-engineering/security-awareness-social-engineering-the-basics.html.

25 MANDIANT, *M-TRENDS 2016* 17 (2016), https://www.fireeye.com/current-threats/annual-threat-report/mtrends/rpt-2016-mtrends.html.

26 Social engineering is pretending to be someone else in order to gain access to a computer or network, or, more generally, to obtain any confidential information. Skip tracers (professionals specializing in locating people) have practiced social engineering for years, and so have debt collectors, bounty hunters, private investigators, and journalists. Phishing does this via email or malicious websites.

27 A Trojan Horse is malicious program masquerading as a safe and useful one.

28 A vulnerability involved in the Target breach, for example. *See* Brian Krebs, *Inside Target Corp., Days After 2013 Breach*, KREBS ON SECURITY (Sept. 21, 2015), https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/.

29 Target did not encrypt credit card numbers on their way out of the POS machine, instead of at the point of swipe. *Id.*

30 The 80 million records stolen from Anthem in 2015 were stored unencrypted and hence readable by the thieves. *See, e.g.*, Lance Whitney, *Anthem's Stolen Customer Data Not Encrypted*, CNET (Feb. 6, 2015, 10:06 AM), https://www.cnet.com/news/anthems-hacked-customer-data-was-not-encrypted/.

31 *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

breach, which was particularly well studied, we know that there was quite a significant number of vulnerabilities that together enabled a breach of that magnitude.[32] It seems likely that, for many of the massive data breaches, a combination of several different vulnerabilities enabled the breach.

Some network vulnerabilities are certainly software vulnerabilities since software (both mass market and non-mass market) is involved in running a network. Since human beings use networks, human vulnerabilities are also common. But not all network vulnerabilities are software or human ones. From now on, we will use "network vulnerabilities" to refer to non-software, non-human vulnerabilities in networks. These vulnerabilities are the ones whose remediation requires information that is not currently available.

To characterize network vulnerabilities, we offer a brief high-level sketch of how network security works. It works much like security at Chicago's United Center—the sports arena where the Bulls play basketball and the Blackhawks play hockey. If you oversaw security there, you would locate the doors and windows, put locks on all those doors and windows, lock the ones you do not need open, and post guards at the rest to check credentials like tickets, press passes, etc. You would also put guards inside to monitor behavior. Computer and network security is the same. You lock doors and windows,[33] post "credential-checking guards" by verifying authorization,[34] and deploy "behavior-monitoring guards," ranging from home computer antivirus programs to multimillion-dollar systems defending corporate networks.[35]

Likewise, competent network administrators know how to reduce network vulnerabilities.[36] Notice that we wrote "reduce," not "eliminate." In a large organization, both the routers and internal structure of the network can be quite complex, and the more complex the network, the more likely a misjudgment that creates a vulnerability. In addition, hackers "are well aware of the details of network . . . security mechanisms, and are developing increasingly sophisticated and effective methods for subverting them."[37] Thus, if businesses were meeting the risk management goal, we would ex-

---

32 MAJORITY STAFF REPORT FOR CHAIRMAN ROCKEFELLER, S. COMM. ON COMMERCE, SCIENCE, AND TRANSP., A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH (2014), https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf.

33 Examples include promptly applying patches, using reasonably up-to-date operating systems, and various uses of encryption.

34 Examples include passwords, more complex multi-factor identification, access control, firewalls, and both black and white listing.

35 Examples include intrusion detection and protection systems, some forms of malware detection, and various forms of traffic monitoring.

36 *See* STALLINGS, NETWORK SECURITY ESSENTIALS, *supra* note 7.

37 Archit Gupta et al., *An Empirical Study of Malware Evolution* 1, 1 (2009 First International Communication Systems And Networks Workshops, 2009).

pect to see a few network vulnerabilities. However, in practice, based on the past decade's record of breaches, there are *lots* of network vulnerabilities.

So why, in regard to network vulnerabilities, do businesses typically fail to meet the business risk management goal? One reason is that corporate culture has struggled to incorporate that goal in its business planning.[38] Lack of risk management expertise is another problem.[39] We assume businesses will eventually solve those problems. Doing so will not, however, eliminate a fundamental problem: the lack of information necessary for adequate risk assessment.

C. *The Lack of Information*

To adequately approximate the business risk management goal, a business has to calculate the expected losses from a data breach over some appropriate period of time. The expected cost of a data breach is the estimated actual cost of the breach if it occurs multiplied by the probability of its occurrence. If a business bases this calculation on accurate information about probabilities and costs, pursuing the business risk management goal is a profit maximizing strategy. The more inaccurate the information, the worse the business's strategy; it will either spend too much or too little.

Unfortunately, there is general agreement that businesses lack sufficiently accurate information about probabilities and costs. A recent World Economic Forum report paints an accurate, if disturbing, picture of the lack of relevant data:

> There are numerous cyber threats plaguing global organizations. Global data is expanding at exponential rates in terms of volume, velocity, variety and complexity. Commercial and personal data are increasingly migrating to global, interconnected technology platforms. The systems that depend upon this data increasingly manage key infrastructure. As access to data and systems increases via the rapidly evolving, interconnected digital ecosystem, the scale and types of risks from cyber threats expands proportionately.
>
> Unknowns concerning the scale and impact of cyber threats, as well as relative levels of vulnerability, threatens paralysis. Lacking accepted benchmarks, large organizations struggle to structure cyber resilience decisions and investments. Organizations lack common measures to quantify cyber threats, curtailing the ability to make clear strategic decisions concerning optimal access and investment levels.

---

38 *See, e.g.*, Marianne Davis, *Underinvesting in Cybersecurity: How Do You Know How Much Security Is Enough?*, SYMANTEC (Aug. 15, 2014), http://www.symantec.com/connect/blogs/underinvesting-cybersecurity-how-do-you-know-how-much-security-enough.

39 DOUGLAS W. HUBBARD ET AL., HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK 11–15 (2016).

> Due to this state of uncertainty, a pervasive concern over growing cyber risks curtails technical and economic development on a global scale. Lacking proper guidance, businesses are increasingly delaying the adoption of technological innovations due to inadequate understandings of required countermeasures. A tragedy of the commons scenario is emerging surrounding proliferating digital access in an unstable ecosystem, which lacks concerted controls and safeguards. A vicious circle results: uncertainty regarding proper levels of preparedness leads to forestalled investments in safeguards as interconnection expands exponentially.[40]

The report identifies two sources of uncertainty. The first is that the magnitude of the losses is not sufficiently well known: there are "[u]nknowns concerning the scale and impact of cyber threats." The second is that the probability of a loss is not sufficiently well known: there are "[u]nknowns concerning . . . relative levels of vulnerability." This puts a significant roadblock in the way of pursuing the business risk management goal.

The same point holds for *consumer* risk management, to which we now turn.

II. DEFENDING CONSUMERS

Risk management, whether business or consumer, requires reliable information—ideally, highly accurate information—about both the magnitude of the loss and the probability of its occurrence. For consumer risk management, the relevant magnitudes and probabilities are the magnitudes and probabilities of *consumer* losses. Neither is sufficiently well known. There have been far fewer studies of consumer losses, and, if it is problematic to accurately correlate the cost and probability of business losses with types of data breach, it is all the more difficult to do so in the case of consumer losses, where the relevant data is less available.

In the consumer context, the lack of information has consequences for the effectiveness of making businesses legally liable for consumer losses. Before turning to that issue, we briefly address the prior question of whether businesses should be liable for those losses.

---

40 WORLD ECON. FORUM, PARTNERING FOR CYBER RESILIENCE TOWARDS THE QUANTIFICATION OF CYBER THREATS 9 (2015), http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf. Others make the same points: "It has also long been known that we simply do not have good statistics on online crime, attacks and vulnerabilities. Companies are hesitant to discuss their weaknesses with competitors even though a coordinated view of attacks could allow faster mitigation to everyone's benefit. In the USA, this problem has been tackled by information-sharing associations, security-breach disclosure laws and vulnerability markets." Ross Anderson et al., *Security Economics and European Policy* 3 (2008), http://www.cl.cam.ac.uk/~rja14/Papers/enisa-short.pdf.

A. *The Landlord/Tenant Analogy*

There is a strong argument that businesses should bear a considerable part of the defensive burden. Consider an analogy with landlords and tenants. The "landlords" are the various kinds of businesses that store consumer data online.[41] Call them collectively *data holders*. "Tenants" divide into the data that resides with the data holder and the consumer subjects of that data. What makes the analogy apt is that unauthorized access to the data can harm the subjects. The argument is that just as landlords can be liable for harm to tenants from unauthorized access to the landlords' buildings, so data holders should be liable for harm caused to consumers by unauthorized access to the data they store. To see the argument, consider the landlord/tenant case, *Kline v. 1500 Massachusetts Avenue Apartment Corporation*.[42] Kline was assaulted in the common areas of the apartment building in which she lived.[43] She sued for negligence alleging that the building owner unreasonably failed to provide adequate security.[44] The court agreed:

> The landlord is no insurer of his tenants' safety, but he certainly is no bystander. And where, as here, the landlord has notice of repeated criminal assaults and robberies, has notice that these crimes occurred in the portion of the premises exclusively within his control, has every reason to expect like crimes to happen again, and has the exclusive power to take preventive action, it does not seem unfair to place upon the landlord a duty to take those steps which are within his power to minimize the predictable risk to his tenants.
>
> . . . .
>
> As between tenant and landlord, the landlord is the only one in the position to take the necessary acts of protection required. He is not an insurer, but he is obligated to minimize the risk to his tenants. Not only as between landlord and tenant is the landlord best equipped to guard against the predictable risk of intruders, but even as between landlord and the police power of government, the landlord is in the best position to take the necessary protective measures. Municipal police cannot patrol the entryways and the hallways, the garages and the basements of private multiple unit apartment dwellings. They are neither equipped, manned, nor empowered to do so. In the area of the predictable risk which materialized in this case, only the landlord could have taken measures which might have prevented the injuries suffered by appellant.[45]

The court held that the landlord was required to take reasonable steps to defend tenants in common areas from harm from unauthorized access to

---

41 Businesses range from resource- and expertise-rich corporations to mom-and-pop retailers. There is a pressing question of how small and medium sized businesses are to meet the risk management goals we suggest here.

42 Kline v. 1500 Massachusetts Ave. Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970).

43 *Id.* at 478.

44 *Id.* at 489.

45 *Id.* at 481, 484.

those areas.[46] Advances in technology have resulted in a new type of "landlord"—data holders. Like traditional landlords, they are typically in the best position to take steps to prevent the harm to data subjects that may follow a data breach.

So why not require data holders to take reasonable steps to prevent harm to the data subjects? We find that rationale to do so compelling, and, indeed, to an extent, the law already does so through common law negligence[47] and through various statutory requirements.[48] We will not discuss the exact form the reasonableness requirement should take. Our point is that unless the necessary risk management information is available, a reasonableness requirement will be ineffective.

B. *Lack of Data Means Lack of an Effective Legal Incentive*

To see why, consider an analogy. Suppose you are a teacher who would like students to write something to engage in adequate explanation and reflection. To achieve this goal, you tell them they must write a paper with enough pages to get a passing grade, but you do not tell them how many pages are enough. That would not only be unfair, it would also fail to create the right incentive for sufficient explanation and reflection. Some would write too little, expending less time and effort than they should, some would write too much, expending more time and effort than they should. Network defense is similar. Some businesses will invest too little in defense, some, too much.

Some may object that this argument looks only at the short-term consequences of imposing liability in the absence of relevant information about probabilities in costs. Why not impose liability to give businesses an incentive to develop ways to obtain the information they now lack? The classic torts case of *The T. J. Hooper*[49] is a good example, even though it involved providing an incentive to adopt technology that already existed, not providing an incentive to create information gathering practices that do not.

The tugboats the *Montrose* and the *T. J. Hooper* encountered a gale while towing barges up the Atlantic coast, and the tugs and the barges

---

46 *See id.* at 487.

47 At least in theory. The application of negligence is limited by the foreseeability requirement (*see, e.g.*, Guin v. Brazos Higher Education Service Corporation, Inc., No. Civ. 05-668 RHK/JSM, 2006 WL 288483, (D. Minn. Feb. 7, 2006) and the economic harm rule (*see, e.g.*, Banknorth, N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206 (M.D. Pa. 2006)).

48 *See, e.g.*, HIPAA Security Rule 45 C.F.R. § 164.308(A)(1), and the Gramm-Leach Bliley Safeguards Rule, 16 *C.F.R.* § 314.3. For an excellent discussion of the Federal Trade Commission's approach to security, *see* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

49 The TJ Hooper, 60 F.2d 737 (2d. Cir. 1932).

sank.[50] The tugs did not have shortwave radios.[51] Had they been so equipped, they would have received reports of the storm and put in at the Delaware breakwater to ride the storm out in safety.[52] Shortwave radios, however, were new technology, and the industry standard was for tugs *not* to have one.[53] The court nonetheless held that it was unreasonable not to equip the tug with a radio as a precaution against losses from storms.[54]

But notice that the risk management calculations are easy. It is obvious that the expected loss exceeds the cost of the radio. Owners know that the losses, when they do occur, can be huge, and they know that, while the occurrence of violent storms is difficult to predict, their occurrence from time to time is certain. So, tugboat owners should realize that they should buy a radio.

So why not impose liability for consumer losses from a data breach to give businesses an incentive to develop and implement effective information gathering practices? The incentive is unlikely to be effective. Contrasts with *The T. J. Hooper* show why. To begin with, tug boat owners could unilaterally buy shortwave radios, but businesses cannot unilaterally collect enough information. To figure the relevant probabilities and costs for a wide range of possible data breaches, a business needs information about the types of data breaches and associated losses that occur across a wide range of businesses. Determining probabilities and costs will require aggregating that information.

III. BETTER DEFENSE WITHOUT BETTER DATA?

Lack of sufficient information about relevant probabilities and costs does not mean it is impossible for businesses to improve their data security. We consider three possibilities: reliance on expert opinion, outsourcing, and compliance with data breach notification statutes. Each option, however, falls far short of approximating the business and consumer risk management goals.

---

50 *Id.* at 737.
51 *Id.*
52 *Id.*
53 *See id.* at 740.
54 *See id.*

A. *Expert Opinion*

Lacking sufficient information to accurately determine probabilities and costs,[55] businesses can turn to educated guesses—that is, to well-informed expert opinion. As one predictive analytics practitioner noted:

> Where very little data is available, it's not possible to use standard mathematics or statistical techniques, but what you can do is create models based on expert opinion. These won't be as good as a statistical model built on a much larger sample, but these types of models can often provide a reasonable level of predictive accuracy.[56]

Relying on expert opinion is reasonable given the current lack of information. But, relying merely on expert opinion is still not a reliable guide to meeting either risk management goal. Expert opinion may still over- or underestimate probabilities and costs, and in such cases a business will spend less or more than required to meet the goal.

B. *Outsourcing*

Outsourcing security recommends itself as at least a partial solution to the lack of information problem. One necessary step toward curing the lack of information is aggregating relevant information from a wide variety of businesses. Outsourcing security will help with that task by concentrating the information from several businesses in a single place. Outsourcing also makes good financial sense. As security and privacy expert Bruce Schneier noted:

> A company can get the security expertise it needs much more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring is vigilance: attacks can happen at any time of the day, any day of the year. While it is possible for companies to build detection and response services for their own networks, it's rarely cost-effective. Staffing for security expertise 24 hours a day, 365 days a year, requires five full-time employees—more when you include supervisors and backup personnel with specialized skills. Even if an organization could find the budget for all of these people, it would be very difficult to hire them in today's job market. Retaining them would be even harder. Security monitoring is inherently erratic: six weeks of boredom followed by eight hours of panic, then seven weeks of boredom followed by six hours of panic. Attacks against

---

55 In the case of the frequency interpretation of probability, a determination is accurate if closely approximates the actual frequency. For the belief interpretation, a determination is accurate to the extent it requires little or no revision in the light of future information.

56 STEVEN FINLAY, PREDICTIVE ANALYTICS, DATA MINING AND BIG DATA: MYTHS, MISCONCEPTIONS AND METHODS 232 (2014).

> a single organization don't happen often enough to keep a team of this caliber engaged and interested.[57]

Security outsourcing companies like AllClearID, BayDynamics, Healthguard Cyber Risk Management, and FireEye provide reasonable security options, especially for small and medium-sized businesses that may not be able to afford a significant investment in information security. Indeed, because basic outsourcing services are sufficiently inexpensive, they may be the twenty-first century equivalent of *The T. J. Hooper* shortwave radio. One may well see legal liability imposed for not using them.

Outsourcing is an attractive and important development; however, as currently practiced, it relies on models built using expert opinions, so it does not lead to an adequate approximation of either risk management goals. There are also privacy concerns. Businesses outsourcing security run their incoming data through the outsourcer. The outsourcer's access to the information raises privacy concerns, and some outsourcers do indeed analyze this data for advertising purposes.

C. *Data Breach Notification Laws*

Data breach notification laws may seem like an attractive option that both forces the disclosure of information about breaches without the privacy concerns of outsourcing and improves security, so its proponents claim. As Bruce Schneier notes:

> There are three reasons for breach notification laws. One, it's common politeness that when you lose something of someone else's, you tell him. The prevailing corporate attitude before the law—"They won't notice, and if they do notice they won't know it's us, so we are better off keeping quiet about the whole thing"—is just wrong. Two, it provides statistics to security researchers as to how pervasive the problem really is. And three, it forces companies to improve their security.[58]

We focus on the second and third reasons, beginning with the third. The laws certainly do lead businesses to increase security. The reason is that publicizing data breaches can impose significant costs on businesses,[59] and the threat of such losses has led businesses to increase online security.[60]

Does the increase yield a more effective pursuit of the goal of consumer risk management? We have found little relevant evidence, other than

---

57 Bruce Schneier, *The Case for Outsourcing Security*, SCHNEIER ON SECURITY (2002), https://www.schneier.com/essays/archives/2002/01/the_case_for_outsour.html.

58 Bruce Schneier, *State Data Breach Notification Laws: Have They Helped?* SCHNEIER ON SECURITY (2009), https://www.schneier.com/essays/archives/2009/01/state_data_breach_no.html.

59 *Cost of Data Breach Study*, *supra* note 2, at 19.

60 *Cost of Data Breach Study*, *supra* note 2, at 15.

a study focusing on identity theft. [61] There is some evidence that the laws reduce identity theft.[62] The identity theft study correlates the existence of data breach notification laws with reductions in identity theft.[63] One cannot simply infer, however, that an increase in security is responsible for the reduction. Reductions in identity theft may result from of a variety of factors other than increased security.[64] Furthermore, even if data breach laws do trigger increases in security that reduce identity theft, that still falls short of showing that those laws decrease overall consumer risk to the point where the consumer risk management goal is attained. The reason is that the harm from unauthorized access reaches far beyond identity theft. It includes harm from ransomware, denial of services attacks, botnets engaged in fraud and other illegal activities, and viruses.[65] The available evidence is thus inconclusive at best.

There is, moreover, a general reason to doubt that data breach notification requirements get us to the consumer risk management goal. It emerges from considering the costs of compliance with notification requirements. Those costs include: forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors, notification costs, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions, and lost business.[66] Data breach notification laws create an incentive to avoid *those* costs. It would be surprising if avoiding those *business* costs were strongly correlated with improved *consumer* risk management.

Indeed, there is some reason to think such a correlation is unlikely. The reason is that the laws define the type of event a business must report.[67] They thus create an incentive to reduce *reportable* data breaches. They do not create an incentive to improve security in regard to problems that do not manifest themselves as reportable data breaches. As professor David Thaw

---

61 David Thaw's work is an important exception. *See* David Thaw, *Data Breach (Regulatory) Effects*, 2015 CARDOZO L. REV. DE NOVO 163 (2015) (arguing that "an affirmative presumption of notification is superior from a cybersecurity perspective. Such a presumption avoids disincentivizing thorough cybersecurity investigations, which are one of the most important tools in protecting consumers against future data breaches and securing existing information systems.")

62 *Id.* at 161.

63 *Id.*

64 Richard J. Sullivan & Jesse Leigh Maniff, *Data Breach Notification Laws*, FED. RESERVE BANK OF KANSAS CITY, https://www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2016/1q16sullivanmaniff.pdf.

65 DETICA, *supra* note 4, at 2.

66 *Cost of Data Brach Study*, *supra* note 2, at 3.

67 CENT.S FOR MEDICARE & MEDICAID SERV.S, *CMS Information Security and Privacy Overview*, https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/ (last modified Apr. 27, 2018).

notes, specific statutory regulations like data breach notifications laws can drive

> perhaps-otherwise-sufficient security budgets toward specific compliance objectives, such as encryption. This, in turn, reduces the available resources for other security activities and forces CISOs to focus on meeting minimum compliance objectives rather than prioritizing the greatest threats they feel their organization face[s]. With an abundance of low-hanging fruit available to regulators–even if likely through malfeasance, not misfeasance–the bar is set extremely low. Thus, regulators are faced with an "industry standard" set perhaps below their optimal level. As long as low-hanging fruit remains available to regulators, CISOs will not be able to justify requests for new resources on the grounds that peer organizations with comparable policies have been subject to enforcement action. Nor will they be able to justify requests based on the regulations themselves, as "reasonable" lacks an operational definition any higher than the low hanging fruit provided by cases [involving obvious and egregious security weaknesses] such as *B.J.'s Wholesale Club, T.J. Maxx Cos.,* and *Twitter*. And so the cycle continues. [68]

Similar worries arise for the role of data breach notification laws in forcing businesses to divulge information about data breaches. They certainly do that. But the information businesses provide is only information about reportable data breaches. Data breach notification laws do not create an incentive to report information about data breaches generally.

IV. MANDATORY ANONYMOUS REPORTING

To estimate the probability of a data breach, we need information about the occurrence of data breaches across a wide range of businesses. The costs of a data breach divide into the costs to businesses and the costs to consumers. To aggregate information about the occurrence of data breaches and their costs to *businesses*, we suggest obtaining that information through *mandatory* collection in a central depository and through the sharing of an *anonymous* summary of the data to all of the mandatory reporters. The data would allow the depository to provide high quality data to the business world about the actual prevalence and cost of breaches in practice today.[69] Mandatory sharing has at least two advantages over voluntary sharing. If sharing is voluntary, businesses will weigh the benefits of

---

68 David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. UNIV. L. REV. 287, 368-69 (2014).

69 Some worry that the data may have limited predictive value. See Annmarie Geddes Baribeau, *Cyber Insurance: The Actuarial Conundrum*, INSUR. COMMUN. 33, 37-38 (2015) (providing, "[W]hile actuaries do need as much historical data as they can get, past data is not always indicative of future events or their costs. 'The challenge is much greater than not having enough historical data . . . Because cyber risk is both growing and rapidly evolving, information about the past may be of limited predictive value.'"). To some extent, the risk that one's data is not representative is inherent in all risk management. Where cyber risk changes rapidly, companies would be well advised to base their predictions on a smaller, more recent sample rather than a larger, but necessarily less recent sample.

information sharing with the risks and costs of doing so, and they may decide that the benefits are insufficient. In particular, at the beginning of a voluntary program, the initially small pool of information means limited benefits, so businesses may be unwilling to participate until enough others do. It may be possible to overcome these problems, but we put them aside. Our concern is to defend mandatory sharing as an acceptable option.

There are at least three existing models in the broad ballpark of what we have in mind. One is the 2015 Cybersecurity Information Sharing Act (CISA), which is voluntary, but covers quite similar information.[70] The second is the mandatory reporting of certain electrical outages to the Department of Energy (DOE).[71] Finally, there is the required, completely confidential reporting of network outages to the FCC under the Network Outage Reporting System (NORS).[72] Each of these three is informative, but not one is a perfect match. CISA is voluntary.[73] The DOE reporting covers a much smaller number of incidents than any estimates of the current number of computer security incidents; for example, the public summary of electrical outage events from January through July 2017 shows only 91 total reported events.[74] The data from NORS does not become public nor, as far as we know, is it ever shared with the cable, satellite, telephone, etc. companies that provide the data to the FCC; the FCC says, "Given the sensitive nature of this data to both national security and commercial competitiveness, the outage data is presumed to be confidential."[75]

To aggregate information about the *consumer* cost of data breaches, we do *not* propose any sort of mandatory reporting by consumers to the government. It would raise significant privacy issues to require consumers to report the type of data involved in a breach, the storage location of the data, and the type and extent of the losses sustained. We propose instead government-initiated or government-funded research, which focuses on consumers who consent to provide their information. The approach is far from unproblematic, but we put those issues aside. We focus primarily on mandatory reporting by businesses.

---

70 CYBER SECURITY INFORMATION SHARING ACT OF 2015, 6 U.S.C. § 148.

71 15 U.S.C. § 772 mandates the sharing of the information. *See* Emily Fisher, Joseph H. Eto & Kristina Hamachi LaCommare, *Understanding Bulk Power Reliability: The Importance of Good Data and a Critical Review of Existing Sources* 2159–2168 (2012 45th HI Int'l Conf. on Sys. Sci., 2012), http://ieeexplore.ieee.org/abstract/document/6149274/.

72 FED. COMMC'NS. COMM'N., *Network Outage Reporting System (NORS)*, https://www.fcc.gov/network-outage-reporting-system-nors (last viewed Dec. 4, 2018).

73 CYBER SECURITY INFORMATION SHARING ACT, 6 U.S.C. § 148.

74 DEPARTMENT OF ENERGY, *Electric Disturbance Events (OE-417) Annual Summaries*, https://www.oe.netl.doe.gov/OE417_annual_summary.aspx (last visited Dec. 4, 2018).

75 FED. COMMC'NS. COMM'N., *supra* note 72.

A. *Sketch of Our Proposal for Reporting*

We propose a reporting regime for computer security incidents for organizations that are closest to the DOE electrical outage reporting, or more specifically, to the first part of the DOE's mandatory two-part reporting form, OE-417.[76] That form has two parts, Schedules 1 and 2; the first part is highly structured, consisting of checkboxes, and constrained, very short answer questions, such as "estimate number of customers affected," and fits on two pages.[77] Schedule 1 is made public.[78] Schedule 2, which asks for a narrative description, is not made public.[79]

Similarly, we envision a mandatory report that would consist of checkboxes and very short answer questions asking for the size, type, and estimated costs of a breach, along with several attributes about the organization attacked and its defenses. As mentioned, the DOE makes the Schedule 1 information from every reported electrical outage incident public.[80] We would do the same, but redact the name of the organization and any geographic information. We would also round numerical reports, making them at least modestly more difficult to associate with particular incidents. The goal is not to anonymize all reports, but rather to attempt to anonymize many of the reports of smaller incidents.[81] Because the major incidents are often widely reported news events and may also be subject to mandatory public disclosure, there is no point in trying to anonymize them.

B. *Benefits of the Proposed Reporting*

The information gathered and reported, together with an estimate of the number of organizations required to report, will give both researchers and organizations themselves the data needed to make reasonably accurate estimates of the probability of a security incident, and more specifically, the probability of a security incident of a specific cost. This is precisely the information that we have argued is needed but is currently missing. It

---

76 U.S. DEP'T OF ENERGY, OE-417 ELECTRIC EMERGENCY AND DISTURBANCE REPORT, https://www.oe.netl.doe.gov/docs/OE417_Form_05312021.pdf (last visited Dec. 3, 2018).

77 *Id.*

78 *Id.*

79 *Id.*

80 *Id.*

81 We write "attempt to anonymize" rather than "anonymize" because of the frequent successes of computer scientists in deanonymizing supposedly anonymized datasets over the past decade or two. *See, e.g.*, A. Narayanan & V. Shmatikov, *De-anonymizing Social Networks* 173–187 (PROC. OF IEEE SYMP. ON SECURITY AND PRIVACY 2009); Arvind Narayanan & Vitally Shmatikov, *Robust De-anonymization of Large Sparse Datasets* 111–125 (PROC. OF IEEE SYMP. ON SECURITY AND PRIVACY 2008); Paul Ohm, *Broken Promises of Privacy:Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

makes sense for the federal government to collect this data nationwide, but that is not absolutely necessary. If just a handful of states, or even one large enough state with enough business activity were to gather and report this information, then that would probably suffice. Estimates of breach probabilities based on, say, only California or only Texas would not be quite as accurate as those based on the nation as a whole, but they should still be quite good.

The collection we have in mind should be able to be done at quite a low cost for both the reporting companies and for whatever government agency collects and publishes it. There is no reason a report shouldn't fit on a two-page form, just like Schedule 1 of OE-417.

C. *Privacy Concerns?*

Prior to its passage, privacy advocates "asked Congress to kill or reform the Cybersecurity Information Sharing Act, a bill that they [said hid] new government surveillance mechanisms in the guise of security protections."[82] The issue was that the shared information in CISA could include detailed information about various consumers' data or online behavior if it was relevant to a breach. It is difficult to see how our proposal, for short reporting of the size and nature of a breach and an organization's defenses, could become a surveillance system in the guise of security protection. We envision businesses reporting only the size, type, and approximate cost to the business of a breach along with several relevant attributes of the business and its defenses. With a little information on which organizations are required to report, this would allow businesses and other organizations to calculate expected business losses. It is difficult to see how sharing and disclosing such information threatens privacy.

V. CONCLUSION

Business and consumer information sharing can provide the data necessary to adequately approximate the business and consumer risk management goals. This would improve defenses against data breaches by reducing network vulnerabilities. It would do so on two conditions. First, businesses incorporate the risk management goals into their business planning.[83] Second, businesses have sufficient information about data breach losses, and they face liability to some appropriate extent for failing to meet the

---

82 Michael Reynolds, *CISA Security Bill Passes Senate with Privacy Flaws Unfixed*, WIRED (Oct. 27, 2015, 5:30 PM), https://www.wired.com/2015/10/cisa-cybersecurity-information-sharing-act-passes-senate-vote-with-privacy-flaws/.

83 *See generally supra* notes 14–15 and accompanying text.

consumer risk management goal. Even then, information sharing remains a partial solution to the problem of improving data breach defenses. One must also reduce software and human vulnerabilities. Information sharing is nonetheless an essential step in the right direction.

BALANCING THE BENEFITS AND COSTS OF HEALTH DATA COLLECTED BY EMPLOYER-SPONSORED WELLNESS PROGRAMS

Dale B. Thompson[*]

INTRODUCTION

The collection of data is not the neutral act of a scientist, but rather it represents a conscious policy choice, with associated benefits and costs. This article examines data collected in a particular context: health data for use in an employer-sponsored "wellness" program. Wellness programs have the potential to lead employees to take self-directed actions that greatly reduce future expenditures on health care. On the other hand, the potential abuse of health data collected by these programs can lead to invasions of privacy and discrimination.

This article carefully examines the benefits and costs of collecting health data for employee wellness programs. It then explores different mechanisms for balancing these benefits and costs, including market-based solutions combining competition with information disclosure, and regulatory systems done at federal and state levels. It concludes that, because of the fundamental role of uncertainty in health care, the best way to balance these benefits and costs will be through a combination of informed consumer choice and baseline regulatory protections set by a competing mix of states.

The rest of this article is as follows: Section I provides a foundational introduction to health data and wellness programs, and Section II conducts a literature review of the legal issues of health data, the effectiveness of and legal issues raised by wellness programs, and analytical frameworks for regulation. Section III analyzes the benefits and costs of health data in wellness programs, and draws inferences based on this analysis. Section IV examines regulatory options, including federal-only approaches, information and marketplace approaches, and approaches based on Optimal Federalism. This section concludes with its recommended policy approach.

---

[*] Professor & Faculty Director of the Undergraduate Business Program, Opus College of Business, University of St. Thomas; J.D. Stanford Law School, Ph.D. Stanford University (Economics), B.A. Williams College (Economics). This research has also been supported by a grant from the Opus College of Business, University of St. Thomas. The author would like to thank participants at the 2017 Symposium on the Law & Economics of Privacy and Data Security, and at the 2017 Academy of Legal Studies in Business Annual Conference for helpful comments and suggestions.

I. BACKGROUND

This section provides a foundation to our analysis by providing background on wellness programs, health data used in these programs, and the regulatory structure underlying the collection, use, and distribution of health data by wellness programs.

A. *Wellness Programs*

In the past ten years, employers have increased their use of wellness programs. One estimate from 2017 is that of firms with at least 200 employees that offer health benefits, 85 percent utilize a wellness program.[1] This is up from the 81 percent in 2015.[2] These programs can be done internally, or with an outside vendor. With outside vendors, wellness plans are a $6 billion per year industry in the United States.[3]

Wellness programs almost always include two components: efforts to address obesity and programs to stop smoking.[4] These two components frequently lead to chronic health conditions[5] that significantly increase health care expenditures and increase absenteeism at work. Wellness programs also identify other health concerns such as stress, other chronic conditions, and nutrition.[6]

The goals of wellness programs depend on their structure. Some are designed to improve employees' performance of certain health-improving activities, such as attendance at fitness centers.[7] Others aim to improve actual health outcomes, such as improving health measurements concerning

---

[1] KAISER FAMILY FOUNDATION & HEALTH RESEARCH AND EDUCATIONAL TRUST, EMPLOYER HEALTH BENEFITS: 2016 ANNUAL SURVEY 194 (2017), http://files.kff.org/attachment/Report-Employer-Health-Benefits-Annual-Survey-2017.

[2] KAISER FAMILY FOUNDATION & HEALTH RESEARCH AND EDUCATIONAL TRUST, EMPLOYER HEALTH BENEFITS 2015 ANNUAL SURVEY 197, 205 (2015), http://files.kff.org/attachment/report-2015-employer-health-benefits-survey.

[3] Sharon Begley, *'Workplace Wellness' Fails Bottom Line, Waistlines - RAND*, REUTERS (May 24, 2013, 6:41 PM), http://www.reuters.com/article/us-wellness-idUSBRE94N0XX20130524.

[4] Ifeoma Ajunwa, *Workplace Wellness Programs Could Be Putting Your Health Data at Risk*, HARV. BUS. REV. (Jan. 19, 2017), https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk.

[5] Roland Sturm, *The Effects of Obesity, Smoking, and Drinking on Medical Problems and Costs*, 21 HEALTH AFF. 245 (2002).

[6] Sidney Slover, *The Future of Wellness is Here: Managing Chronic Disease via Interactive Health and Wellness Education*, CORP. WELLNESS MAG. (last visited Dec. 1, 2018), https://www.corporatewellnessmagazine.com/focused/the-future-of-wellness-is-here-managing-chronic-disease-via-interactive-health-and-wellness-education /.

[7] SOC'Y FOR HUM. RESOURCE MGMT., *How to Establish and Design a Wellness Program* (Feb. 27, 2018), https://www.shrm.org/resourcesandtools/tools-and-samples/how-to-guides/pages/howtoestablishanddesignawellnessprogram.aspx.

cholesterol, blood pressure, blood glucose, and alcohol consumption.[8] Some focus on reducing expenditures on health care, leading to "return on investment" (ROI).[9] Recent research has emphasized assessing the "full value" from wellness programs, including "improved quality of life; a more engaged and motivated workforce; increased worker retention and attraction; improved safety performance; improved manufacturing reliability; and a healthier company culture."[10] This research has led many wellness companies to "redefin[e] their business models to promote a culture of health" and to emphasize "value on investment."[11]

Wellness programs use a variety of techniques to achieve these objectives. One technique is basic education: make employees aware of their current health status, and give them information and coaching on how to improve their health.[12] Employers can then provide a number of offerings, including gym memberships, weight-loss programs, and programs to stop smoking.[13] Employers can offer wellness coaches to help employees identify achievable goals, and then keep them on the path to achieving those goals.[14] Employers can go further and provide economic incentives for participation and outcomes in the form of discounts on health insurance costs (carrots) or financial penalties (sticks).[15]

One important aspect of any wellness program is the degree at which the program fits with the corporate culture.[16] Dee Edington, an eminent scholar of wellness programs,[17] and Jennifer Pitts note, "[t]o support healthy employees, we need … an approach that [will] encourage organizations to

---

8 Julia Appleby, *Benefits of Workplace Wellness Programs Questioned* (Oct. 3, 2015, 3:04 PM), https://www.usatoday.com/story/news/2015/10/03/kaiser-workplace-wellness-programs-overtesting/73109946/.

9 SOC'Y FOR HUM. RESOURCE MGMT., *supra* note 7.

10 Ron Goetzel et al., *Do Workplace Health Promotion (Wellness) Programs Work*, 56 J. OCCUPATIONAL & ENVTL. MED. 927, 929 (2014).

11 Jean Abraham & Katie M. White, *Tracking the Changing Landscape of Corporate Wellness Companies*, 36 HEALTH AFF. 222, 222 (2017).

12 Slover, *supra* note 6.

13 Ajunwa, *supra* note 4.

14 Slover, *supra* note 6.

15 *See* Fred S. Switzer III et al., *Carrots, Not Sticks: Adverse Impact and Wellness Programs*, 59 J. OCCUPATIONAL & ENVTL. MED. 250 (2017); Reed Abelson, *Employee Wellness Programs Use Carrots and, Increasingly, Sticks*, N.Y. TIMES (Jan. 25, 2016) https://www.nytimes.com/2016/01/25/business/employee-wellness-programs-use-carrots-and-increasingly-sticks.html.

16 Hector De La Torre & Ron Goetzel, *How to Design a Corporate Wellness Plan That Actually Works,* HARV. BUS. REV. (Mar. 31, 2016), https://hbr.org/2016/03/how-to-design-a-corporate-wellness-plan-that-actually-works.

17 Dr. Edington has been called the "godfather of health-risk assessment." Michael Friedman, *Dee Edington and the Power of Positive Organizational Health*, PSYCHOL. TODAY (Feb. 4, 2016), https://www.psychologytoday.com/blog/brick-brick/201602/dee-edington-and-the-power-positive-organizational-health.

modify their health-related environments, cultures, and climates. At the end of the day, no matter how good an organization's wellness program, employees cannot realize their fullest potential health in an unhealthy workplace."[18] Others have pointed to the need for "leadership commitment and support,"[19] and an integrated approach to wellness that connects health with "every aspect of business practice, from company policies to everyday work activities."[20] In addition to executive support, employees themselves need to be directly connected to the development and operation of a wellness program; "[b]oosting engagement in wellness can only be achieved when workers own the program, understand how they and the company benefit, and are given a meaningful voice in its ongoing operation."[21]

B. *Health Data on Wellness Programs*

Another key aspect of any wellness program is how it collects, uses, and distributes health data. Health data plays essential roles for wellness programs. Health data is used initially to identify what health risks individual employees face. It is also used to establish baseline levels of health for determining program objectives for individual employees. For wellness programs with outcome objectives, health data is used to determine whether an individual employee has achieved program objectives.

Health data can take many forms. Perhaps the most popular way to collect health data is through a "Health Risk Assessment" (HRA).[22] Many times, the HRA is the starting point for a wellness program; an HRA asks employees about their stress levels, "medical history, health status, and lifestyle."[23] Many wellness programs also offer "biometric screenings," which are "health examinations that measure[] an employee's risk factors for certain medical issues such as cholesterol, blood pressure, stress, and nutrition."[24] Wellness programs are sometimes offered through a health

---

18 Dee W. Edington & Jennifer S. Pitts, *Shared Values – Shared Results: Positive Organization Health as a Win-Win Philosophy* xvii-xviii (2015).

19 De La Torre & Goetzel, *supra* note 16.

20 *Id.*

21 *Id.*

22 Ron Z. Goetzel, et al., *A Framework for Patient-Centered Health Risk Assessments* 20, CENTER FOR DISEASE CONTROL AND PREVENTION (2011), https://www.cdc.gov/policy/hst/HRA/FrameworkForHRA.pdf.

23 KAISER FAMILY FOUNDATION & HEALTH RESEARCH AND EDUCATIONAL TRUST, *supra* note 2.

24 *Id.* at 197.

plan.[25] In those instances, the health plan has access to health claims information, and will incorporate that data into its program.[26]

In addition to these traditional sources of health data, wellness plans have begun collecting health data from a variety of new sources. A recent white paper by Optum notes that, "Since 2014, there has been a significant increase in the use of online competitions, activity tracking devices, social networks, mobile apps and mobile messaging to help engage employees [in wellness programs]."[27] Wearable devices, such as Fitbits, can collect a wide range of health data, including steps taken, heart rate, sleep patterns, and body temperature.[28] Social media has been described as a "gold mine" for healthcare data,[29] and can provide information about an employee's fitness patterns and food choices.[30] Genetic testing is also becoming more common in wellness programs.[31] Genetic testing can identify particular genes that are linked to traits such as "obesity, appetite, and compulsive behavior."[32] Just as we have many forms of this health data, we also have a multitude of laws related to this data. We now turn to these laws.

C. *Regulatory Framework*

The common law and an array of statutory laws provide the current regulatory framework for the collection, use, and distribution of health data in the context of wellness programs.[33] These regulatory systems relate to

---

25 DEP'T OF LABOR, *HIPAA and the Affordable Care Act Wellness Program Requirements* 27 (last visited Dec. 1, 2018), https://www.dol.gov/sites/default/files/ebsa/about-ebsa/our-activities/resource-center/publications/caghipaaandaca.pdf.

26 Dinah Wisenberg Brin, *Wellness Programs Raise Privacy Concerns Over Health Data*, SOC'Y FOR HUM. RESOURCE MGMT. (Apr. 6, 2016), https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/wellness-programs-raise-privacy-concerns-over-health-data.aspx

27 Seth Serxner, Rohit Kichlu & Erin Ratelis, *Employee Health: Are You Leading or Lagging?*, OPTUM 5 (2017), https://cdn-aem.optum.com/content/dam/optum3/optum/en/resources/white-papers/WIW_final_WP_8th_annual_320.pdf.

28 *See generally* FITBIT, *Why Fitbit* (last visited Sept. 7, 2018), https://www.fitbit.com/whyfitbit.

29 April Dembosky, *Social Media a Healthcare Data Gold Mine*, FIN. TIMES (Dec. 11, 2012), https://www.ft.com/content/2fe7e98a-4334-11e2-aa8f-00144feabdc0.

30 *See generally* CRIMSON HEXAGON, *The Health of the Nation: Farmers Markets, FitBits and Other Wellness Trends in the US* (2016), http://pages.crimsonhexagon.com/rs/284-XQB-702/images/CHX-N17-026_US%20Trends%20Report_HealthWellness_v8.pdf.

31 Rebecca Greenfield, *How Testing Workers' Genes Could Make Office Wellness Programs Work*, CHI. TRIB., (Feb. 8, 2016, 10:55 AM), http://www.chicagotribune.com/business/ct-office-wellness-programs-20160208-story.html.

32 Gregory Steinberg, *Reducing Metabolic Syndrome Risk Using a Personalized Wellness Program*, 57 J. OCCUPATIONAL. & ENVTL. MED. 1269, 1271 (2015). For a critique of this study, *see* Al Lewis, *Genetic Testing: The New Frontier of Wellness Madness*, HEALTH CARE BLOG (Dec. 16, 2015), http://thehealthcareblog.com/blog/2015/12/16/genetic-testing-the-new-frontier-of-wellness-madness/.

33 For another summary of these, *see* Kristin M. Madison, *The Risks of Using Workplace Wellness Programs to Foster a Culture of Health*, 35 HEALTH AFF. 2068 (2016).

possible violations of privacy, discrimination, and the delivery of health care.

Privacy protections include both common and statutory laws. Tort law includes a basic right of protection from publication of private information. The Restatement (Second) of Torts § 652D states that:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
>
> (a) would be highly offensive to a reasonable person, and
>
> (b) is not of legitimate concern to the public.[34]

Statutes protecting privacy include the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[35] and the Genetic Information Nondiscrimination Act of 2008 (GINA).[36] Under HIPAA, when health plans are the providers of the wellness programs, the health information they collect is subject to the same restrictions as for health care providers in other contexts.[37] HIPAA limits the disclosure of protected health information (PHI) by "covered entities."[38] Covered entities include health plans, health care providers, and their business associates.[39] Employers who are not directly operating a health plan are not covered by HIPAA.[40] Consequently, while a health-plan provided wellness program is covered, employer-provided wellness programs and programs from non-health-plan external wellness vendors are not covered.[41]

GINA prohibits the use of genetic data by health plans, health insurers, and employers in making significant decisions about health insurance and employment.[42] GINA also makes it unlawful in general "for an employer to request, require, or purchase genetic information with respect to an employee or a family member of the employee."[43] Employers can request that an

---

34 RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW. INST., 1977).

35 U.S. DEP'T OF HEALTH & HUM. SERV.S, *Guidance Regarding Methods for De-Identification of Protected Helath Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* (last visited Dec. 1, 2018), https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected.

36 NAT'L HUM. GEOME RES. INST., *The Genetic Information Nondiscrimination Act of 2008* (last visited Dec. 2, 2018), https://www.genome.gov/27568492/the-genetic-information-nondiscrimination-act-of-2008/.

37 U.S. DEP'T OF HEALTH & HUM. SERV.S, *supra* note 35.

38 U.S. DEP'T OF HEALTH & HUM. SERV.S, *supra* note 35.

39 U.S. DEP'T OF HEALTH & HUM. SERV.S, *supra* note 35.

40 U.S. DEP'T OF HEALTH & HUM. SERV.S, *supra* note 35.

41 U.S. DEP'T OF HEALTH & HUM. SERV.S, *supra* note 35.

42 NAT'L HUM. GEOME RES. INST., *supra* note 36.

43 42 U.S.C. § 2000ff–1(b).

employee voluntarily give his or her own genetic information as part of a wellness program, as long as the employer only receives de-identified information.[44] The Equal Employment Opportunity Commission (EEOC) is in charge of implementing and enforcing GINA.[45]

Concerning discrimination, Title VII of the Civil Rights Act of 1964 (Title VII)[46] and the Americans with Disabilities Act of 1990 (ADA)[47] apply, along with HIPAA. Title VII prohibits discrimination based on certain protected categories.[48] The ADA prohibits discrimination based on protected status.[49] It also prohibits employers from asking for a medical exam (including giving medical history), except for "voluntary medical examinations, including voluntary medical histories, which are part of an employee health program."[50]

In addition to privacy protections, HIPAA prohibits health plans from denying health insurance coverage or charging differently based on certain health factors.[51] However, HIPAA did provide an exception for wellness programs, and under this exception, employers could provide wellness incentives up to "20 percent of the cost of coverage."[52] Under the Patient Protection and Affordable Care Act (ACA), this exception was extended to 30 percent of the cost of coverage (and 50 percent for anti-smoking programs).[53]

Another relevant statute is the Employee Retirement Income Security Act of 1974 (ERISA).[54] States wishing to regulate health data in wellness programs will be limited by ERISA's preemption principles. Federal preemption under ERISA is complex, with a three-part analysis. This begins by determining whether a state law "relates to" employee benefit plans.[55] However, ERISA also has a "savings clause" that permits state laws that regulate insurance.[56] Nonetheless, ERISA specifically states that self-insured employee benefit plans shall not "be deemed" an insurance company.[57] At the end of this analysis, the conclusion is that state regula-

---

44 42 U.S.C. § 2000ff–1(b)(2) (2008).

45 NAT'L HUM. GEOME RES. INST., *supra* note 36.

46 EQUAL EMP. OPPORTUNITY COMMISSION, *Title VII of the Civil Rights Act of 1964* (last visited Dec. 2, 2018), https://www.eeoc.gov/laws/statutes/titlevii.cfm.

47 DEP'T OF LAB., *Americans with Disabilities Act* (last viewed Dec. 2, 2018), https://www.dol.gov/general/topic/disability/ada.

48 EQUAL EMP. OPPORTUNITY COMMISSION, *supra* note 46

49 DEP'T OF LAB., *supra* note 47

50 Americans with Disabilities Act of 1990 42 U.S.C. § 12112(d)(4) (2008).

51 U.S. DEP'T OF HEALTH & HUM. SERV.S, *supra* note 35.

52 Nondiscrimination and Wellness Programs in Health Coverage in the Group Market, 71 Fed. Reg. 75013, 75018 (Dec. 13, 2006), https://www.dol.gov/ebsa/regs/fedreg/final/2006009557.htm.

53 DEP'T OF LABOR, *supra* note 25.

54 29 U.S.C. § 1001 (2008).

55 29 U.S.C. § 1144(a) (2008).

56 29 U.S.C. § 1144(b)(2)(A) (2008).

57 29 U.S.C. § 1144 (b)(2)(B) (2008).

tions can only address wellness programs by employers who do not self-insure. This remains a sizable part of the market, with one estimate suggesting this would reach 70 million employees of a total of 123 million employees covered by an employer-sponsored health plan.[58]

Some other issues arise in this web of statutes. Under the ADA, employers cannot request medical exams, unless they are "voluntary."[59] The exception to GINA's prohibition on collecting genetic information also only applies if the employee "voluntarily" provides his or her own genetic information.[60] However, the ACA allows employers to provide a financial incentive for wellness program participation up to 30 percent of the cost of individual coverage.[61] But is someone operating under the threat of a 30 percent penalty doing so voluntarily? The EEOC has issued rules finding that wellness programs can offer incentives of up to 30 percent of self-only coverage for inducing employees to undergo a medical examination, or for inducing an employee's spouse to provide genetic information.[62] Participation under these incentives is still considered "voluntary."[63] One court has pushed this interpretation to the point where a choice with a financial penalty of 100 percent was still considered "voluntary," finding that "even a strong incentive is still no more than an incentive; it is not compulsion."[64]

In this context, a recent bill, H.R. 1313,[65] proposed in the U.S. House of Representatives aims to extend these exceptions. H.R. 1313 finds that employer-provided wellness plans with financial penalties of no more than 30 percent of coverage (though that would be doubled for genetic information from employee and spouse) would be in compliance with both the

---

58 NAT'L ACAD. FOR ST. HEALTH POL'Y, *ERISA Preemption Primer* 3-4 (2009), https://nashp.org/wp-content/uploads/sites/default/files/ERISA_Primer.pdf.

59 EQUAL EMP. OPPORTUNITY COMMISSION, *Enforcement Guidance: Disability-Related Inquiries and Medical Examinations of Employees Under the Americans with Disabilities Act* (last updated Mar. 24, 2005), https://www.eeoc.gov/policy/docs/guidance-inquiries.html.

60 42 U.S.C. § 2000ff–1(b)(2).

61 DEP'T OF LABOR, *supra* note 25.

62 EQUAL EMP. OPPORTUNITY COMMISSION, *EEOC Issues Final Rules on Employer Wellness Programs* (May 16, 2016), https://www.eeoc.gov/eeoc/newsroom/release/5-16-16.cfm.

63 *Id.*

64 Equal Emp't Opportunity Comm'n v. Orion Energy Systems, Inc., No. 14-CV-1019 (E.D. Wisc. Sept. 19, 2016. The author would argue that this wellness program is an example of "'unmistakably clear' coercion." *See* Dale B. Thompson, *"Unmistakably Clear" Coercion: Finding a Balance between Judicial Review of the Spending Power and Optimal Federalism*, 50 SAN DIEGO L. REV. 589 (2013).

65 Preserving Employee Wellness Programs Act, H.R. 1313, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/1313.

ADA and GINA.[66] Voluntariness would be irrelevant. This bill has led to vigorous criticism,[67] and raised great concerns about genetic information.[68]

II. LITERATURE REVIEW

To fully appreciate the context of health care data and wellness programs, this article will briefly review the extensive literature on the legal issues of health data, and the effectiveness of and legal issues raised by wellness programs. This article will also look briefly at regulatory issues such as benefit-cost analysis and federalism.

A. *Health Data*

There is a large and growing body of literature on the legal issues of health data, going back at least twenty years. This literature delves deeply into privacy and discrimination through the use of health data.[69] Significant scholars of this literature include Nicolas Terry,[70] Frank Pasquale,[71] and Sharona Hoffman and Andy Podgurski.[72] This literature has been extended recently by Janine Hiller, who examines "whether massive data collection about personal health and individual social status, both within the health-care system and outside of it, will serve the goal of addressing historical discrimination in health care, or whether data analytics will lead to the loss

---

66 *See generally id.*

67 *See, e.g.,* Nicholas Bagley, *Preserving wellness programs by infringing on privacy*, INCIDENTAL ECONOMIST (Mar. 13, 2017), http://theincidentaleconomist.com/wordpress/preserving-wellness-programs-by-infringing-on-privacy/.

68 *See* Cole Holderman, *H.R. 1313 – New Bill to Threaten Genetic Nondiscrimination*, HOPES (Mar. 13, 2017), https://web.stanford.edu/group/hopes/cgi-bin/hopes_test/h-r-1313-new-bill-to-threaten-genetic-nondiscrimination/ (stating "What's more concerning is that employers would then have direct access to bulk genetic data from any wellness programs . . . opening the door wide for employers to discriminate based on genetics.").

69 *See* Michael L. Tudor, *Protecting Privacy of Medical Records of Employees and Job Applicants in the Digital Era Under the Americans With Disabilities Act*, 40 N. KY. L. REV. 635 (2013).

70 *See, e.g.,* Nicolas P. Terry, *Will the Internet of Things Transform Healthcare?*, 19 VAND. J. ENT. & TECH. L. 327 (2016); Nicolas P. Terry, *Protecting Patient Privacy in the Age of Big Data*, 81 UMKC L. REV. 385 (2012).

71 *See, e.g.,* Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682 (2013); Frank Pasquale and Tara Adams Ragone, *Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing*, 17 STAN. TECH. L. REV. 595 (2014).

72 *See, e.g.,* Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for Regulation and Oversight of Electronic Health Record Systems*, 22 HARV. J. LAW & TECH. 103 (2008); Sharona Hoffman and Andy Podgurski, *The Use and Misuse of Biomedical Data: Is Bigger Really Better?*, 39 AM. J.L. MED. 497 (2013).

of individual privacy, unequal treatment of individuals, and the perpetuation of health inequality."[73]

Another large part of this literature addresses the "Internet of Things." One possible element of a wellness program is a "wearable," and the Internet of Things includes wearable devices like Fitbits.[74] Some have argued for new regulations for the Internet of Things.[75] Others predict that regulations would be a straight-jacket on future development of these technologies, and instead recommend the use of education and information; they suggest that beyond these regulatory concerns, these technologies could possibly lead to a "revolution" in ethical business cultures.[76]

One aspect of health care and health data that should not be forgotten is uncertainty. More than fifty years ago, Kenneth Arrow started a new field in economics with his landmark article, "Uncertainty and the Welfare Economics of Medical Care."[77] Arrow pointed to the fundamental role of uncertainty across the field of health care, concluding that "the special structural characteristics of the medical-care market are largely attempts to overcome the lack of optimality due to the nonmarketability of the bearing of suitable risks and the imperfect marketability of information."[78]

B. *Wellness Programs*

The literature has found a wide range of success for wellness programs. One meta-study in 2010 found positive financial impacts (positive Return-on-Investment, or ROI).[79] A study of a program at Johnson & Johnson found a "strong return on investment."[80]

---

73 Janine S. Hiller, *Healthy Predictions? Questions for Data Analytics in Health Care*, 53 AM. BUS. L. J. 251, 251-52 (2016).

74 *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 88-89 (2014).

75 *See id.* at 85 (finding that "four inherent aspects of sensor-based technologies . . . create very real discrimination, privacy, security, and consent problems[]" and "[t]his article . . . propose[s] concrete first steps for a regulatory approach to the Internet of Things."); Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y, L. & ETHICS. 1 (2016) (offering "two detailed and workable solutions for remedying the current lack of protection of employee health data that will realign employer use with reasonable expectations of health and fitness privacy.").

76 Timothy L. Fort, Anjanette H. Raymond & Scott J. Shackelford, *The Angel on Your Shoulder: Prompting Employees to Do the Right Thing Through the Use of Wearables*, 14 N.W. J. TECH. & INTELL. PROP. 139, 139 (2016).

77 Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963).

78 *Id.* at 947.

79 *See* Katherine Baicker, David Cutler, & Zirui Song, *Workplace Wellness Programs Can Generate Savings*, 29 HEALTH AFF. (2010) (providing a meta-analysis of costs and financial savings from wellness programs found reductions in medical costs of $3.27 and reductions in absenteeism costs by

However, a "congressionally mandated report"[81] was conducted by the RAND Corporation and examined programs from seven employers with over 600,000 employees.[82] This report found that the ROI from wellness programs derived completely from disease management programs, while lifestyle management programs had negative ROI.[83] Overall, including both disease and lifestyle management, per member per month savings from an average wellness program were $2.38 in the first year, and $3.46 in fifth year, "but the changes [we]re not statistically significant."[84] A long-term–over seven years–study of PepsiCo's "Healthy Living" program found similar results, with "disease management but not lifestyle management . . . associated with lower costs."[85] Another study of BJC HealthCare's wellness program found that "although the program did cut some hospitalizations, it did not save money for the employer in the short term."[86]

Consequently, recent literature has moved away from ROI as the metric for examining wellness programs, and more towards total value for the organization: "A broader view considered by leading employers is moving beyond ROI to the full value of the investment in improving the health of a population."[87] The role of corporate culture has also been emphasized: "Successful programs are delivered through customized, integrated, comprehensive solutions that are strongly linked to an organization's business strategy and firmly championed by senior leadership and managers throughout the organization."[88] An important part of these integrated solutions is the use of coaching to encourage employees to make healthier deci-

---

$2.73, i.e. $6 total, for every dollar spent on wellness programs). *But see* Shannon Mullen, *Can Your Boss Fine You for not Disclosing Your Weight?*, MARKETPLACE.ORG (July 22, 2013, 9:48 AM), https://www.marketplace.org/2013/07/22/health-care/can-your-boss-fine-you-not-disclosing-your-weight (noting that "Harvard health economics professor Katherine Baicker says it's too early to tell whether wellness programs pay off.").

80 Rachel M. Henke, et al., *Recent Experience in Health Promotion at Johnson & Johnson: Lower Health Spending, Strong Return On Investment*, 30 HEALTH AFF. 490 (2011).

81 Dan Munro, *RAND Corporation (Briefly) Publishes Sobering Report on Workplace Wellness Programs*, FORBES (May 28, 2013), https://www.forbes.com/sites/danmunro/2013/05/28/rand-corporation-briefly-publishes-sobering-report-on-workplace-wellness-programs/#47803bbe6075.

82 RAND CORP., *Do Workplace Wellness Programs Save Employers Money?* (2013), http://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9744/RAND_RB9744.pdf.

83 *Id.*

84 Soeren Mattke, et al., *Workplace Wellness Programs Study: Final Report* 55-56, RAND CORP. (2013), https://aspe.hhs.gov/system/files/pdf/76661/rpt_wellness.pdf.

85 John P. Caloyeras, et al., *Managing Manifest Diseases, but not Health Risks, Saved PepsiCo Money Over Seven Years*, 33 HEALTH AFF. 124, 128 (2014).

86 Gautam Gowrisankaran et al., *A Hospital System's Wellness Program Linked to Health Plan Enrollment Cut Hospitalizations but not Overall Costs*, 32 HEALTH AFF. 477, 477 (2013).

87 Goetzel et al., *supra* note 5, at 929.

88 *Biometric Health Screening for Employers*, 55 J. OCCUPATIONAL. & ENVTL. MED. 1244, 1244 (2013).

sions.[89] Considered in this light, wellness programs can show greater benefits if executed properly and in the right conditions.[90]

Meanwhile, many other scholars and advocates have raised concerns about the effects of wellness programs on privacy and discrimination. [91] One article pointed to the interconnection of cost savings from wellness programs and discrimination:

> [W]e found little evidence that such programs can easily save costs through health improvement without being discriminatory. Our evidence suggests that savings to employers may come from cost shifting, with the most vulnerable employees—those from lower socioeconomic strata with the most health risks—probably bearing greater costs, that in effect subsidize their healthier colleagues.[92]

A recent article found discriminatory problems with wellness programs with penalties as incentives: "the results of this study indicate that disincentive-based programs pose a high risk of differentially selecting protected groups into program categories. This is especially true for members of multiple protected classes."[93] It is important to note that this study did not find the same effect for positive incentives, i.e. "carrots."[94]

Privacy advocates raise serious concerns with the impacts of these programs on individual privacy. [95] Some of these concerns result from confusion over the applicability of federal laws: "Individuals often erroneously think that the HIPAA rules protect the privacy of any health information, and they may let their privacy guard down as a result."[96] Meanwhile, wellness vendors may utilize other sources of information: "[T]he business proposition of wellness vendors often depends on collecting, combining, and analyzing data from many sources, ranging from health claims to detailed geo-location data to records of grocery purchases."[97] With imperfect protection of data privacy, "the result is that personally identifiable information that starts out as part of a wellness program may become input to American marketers, database companies, and other data profilers."[98]

---

89 Interview with Sara Ratner, Senior Vice President for Compliance & Corporate Systems, RedBrick Health, Minneapolis, MN (June 2, 2017) (notes on file with author).

90 *See* Goetzel et al., *supra* note 10, at 933.

91 *See generally* Jill R. Horwitz, Brenna D. Kelly, & John E. DiNardo, *Wellness Incentives in the Workplace: Cost Savings through Cost Shifting to Unhealthy Workers*, 32 HEALTH AFF. 468 (2013).

92 *Id.* at 468.

93 Switzer et al., *supra* note 15, at 250.

94 *See generally* Switzer et al., *supra* note 15.

95 *See generally* Pam Dixon, *Comments of World Privacy Forum to Equal Employment Opportunity Commission Regarding Title II of the Genetic Information Nondiscrimination Act of 2008, Revisions to the Wellness Program Exception*, WORLD PRIVACY F. (January 20, 2016), http://www.worldprivacyforum.org/wp-content/uploads/2016/01/WPF_CommentsEEOC_GINA_fs.pdf.

96 *Id.* at 3.

97 *Id.*

98 *Id.*

Another article points to the inherent conflict between the need for wellness to be a part of corporate culture, with the possible detrimental effects of wellness programs on discrimination and privacy: "Enthusiasm about the financial and health gains that wellness programs might yield coexists with concerns about health costs shouldered by employees, the possibility of employment discrimination, and the potential for employers' invasion of employees' privacy."[99] Also, "programs might help some employees, but not others, and they could harm morale or create or exacerbate a sense of exclusion among employees not able to take full advantage of program offerings."[100]

And yet another article suggests an "ethical framework" to "reconcile employer and employee interests while maintaining efficacy."[101] To do so, employers must "adopt … innovative approaches to wellness that encourage employee input and oversight, rather than merely plac[e] the responsibility for healthful behavior solely on the employee."[102]

C. *Regulation Including Benefit-Cost Analysis and Federalism*

Finally, we will take a brief look at the literature related to regulation of health care data and wellness programs. Before implementing a particular regulation, we might want to conduct a benefit-cost analysis of that regulation. Benefit-cost analysis is an oversight tool for assessing the tradeoffs embodied in a regulation. In using it, an analyst frequently compares the benefits and costs of a regulation directly, by measuring them in a common manner, such as assigning a dollar value to them. Executive orders from Presidents Ronald Reagan[103] and Bill Clinton[104] required the use of benefit-cost analysis in the regulatory process. After criticisms of benefit-cost analysis,[105] a report on reforming the practice of benefit-cost analysis was published by Resources for the Future.[106] Among its recommendations

---

99 Madison, *supra* note 33, at 2068.

100 *Id.* at 2072.

101 Ifeoma Ajunwa, Kate Crawford & Joel S. Ford, *Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs*, 44 J.L. MED. & ETHICS 474, 479 (2016).

102 *Id.*

103 Exec. Order No. 12,291, 46 Fed. Reg. 13193 (1981).

104 Exec. Order No. 12,866, 59 Red. Reg. 51735 (1994).

105 *See, e.g.,* Duncan Kennedy, *Cost-Benefit Analysis of Entitlement Problems: A Critique*, 33 STAN. L. REV. 387 (1981); Dale B. Thompson, *Beyond Benefit-Cost Analysis: Institutional Transaction Costs and the Regulation of Water Quality*, 39 NAT. RESOURCES J. 517 (1999); Amartya Sen, *The Discipline of Cost-Benefit Analysis*, 29 J. LEGAL STUD. 931 (2000); Frank Ackerman & Lisa Heinzerling, *Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection*, 150 U. PA. L. REV. 1553 (2002).

106 RESOURCES FOR THE FUTURE, REFORMING REGULATORY IMPACT ANALYSIS (Winston Harrington, Lisa Heinzerling, & Richard D. Morgenstern, eds., 2009).

were "include in RIAs [Regulatory Impact Analysis] detailed descriptions of expected consequences as physical or natural units, without monetization or discounting,"[107] and "consider interactions between the distribution of regulatory costs and benefits."[108]

There were some early uses of benefit-cost analysis for examining online privacy[109] and "healthcare quality" programs,[110] earlier versions of wellness programs. More recently, Adam Thierer presented a benefit-cost analysis "framework" for "digital privacy."[111] While this article was addressed to digital privacy in general, it has significant relevance for health data and wellness programs.

Thierer points out that the harms associated with digital privacy violations are based on "emotional appeals and highly subjective assertions."[112] These harms (the prevention of which would be a benefit of a regulation) include claims that "targeted online advertising or data collection is 'creepy.'"[113] Furthermore, in instances like these, he claims that "regulatory advocates . . . worry that people may not be acting in their own best self-interest when it comes to online . . . digital privacy choices."[114] As a result, it seems that "the benefits of regulation are [treated as] virtually boundless and that the costs should generally be ignored in order to essentially save consumers from their own choices."[115] He does however note that as to "health information, . . . privacy violations can pose a more direct and quantifiable threat to personal well-being."[116]

Meanwhile, Thierer also disputes that regulations of online privacy can provide benefits by "enhancing consumer trust."[117] The rapid expansion of online activity and responses from consumer surveys "call into question the assertion that expanded privacy regulation is needed to achieve greater consumer online trust or enhance online commerce."[118] On the other hand, Thierer argues for closer investigation into valuation of digital privacy: "Analyzing those costs and the consumers' willingness to pay for privacy should be an essential part of any BCA [Benefit-Cost Analysis] in this

---

107 *Id.* at 225.

108 *Id.* at 232.

109 Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85 (2002).

110 Sean Nicholson, et al., *How to Present the Business Case for Healthcare Quality to Employers*, 4 APPLIED HEALTH ECON. & HEALTH POL'Y 209 (2005).

111 Adam Thierer, *A Framework for Benefit-Cost Analysis in Digital Privacy Debates*, 20 GEO. MASON L. REV. 1055, 1056 (2013).

112 *Id.* at 1067.

113 *Id.*

114 *Id.*

115 *Id.* at 1068.

116 *Id.* at 1070.

117 *Id.* at 1071.

118 *Id.* at 1072.

arena."[119] However, the value of privacy may be considered a "non-use value" because privacy is valued primarily when it is lost, and there are many difficulties in properly determining nonuse values.[120] Thierer also cites possible costs of regulations that could dampen activities that "cross-subsidize and sustain content and culture and ensure more and better services are made available to consumers."[121]

Consequently, "because th[e]se benefits and costs remain so remarkably subjective and contentious," Thierer argues that we should manage online privacy via "less restrictive solutions."[122] We should use education, information, and consumer choice, "before resorting to potentially costly and cumbersome legal and regulatory regimes that could disrupt the digital economy and the efficient provision of services that consumers desire."[123]

Another area of concern for regulation is federalism. Federalism is the idea that the universe of regulatory powers should be divided between federal, state, and local authorities.[124] Federalism in health care has recently returned to the conversation. Nicholas Bagley writes:

> Missing from [the] debate [over replacing Obamacare], however, is a theoretically grounded and empirically informed understanding of how best to allocate power between the federal government and the states . . . . Instead, federal action is necessary to overcome the states' fiscal limitations: their inability to deficit-spend and the constraints that federal law places on their taxing authority.[125]

Fortunately, such a theory exists, in Optimal Federalism.[126] This theory, previously applied to environmental policies, health care, and immigration policies is "an analytical technique for determining the appropriate level of government for carrying out different functions of a public policy."[127]

---

119 *Id.* at 1078.

120 *See*, *e.g.*, Dale B. Thompson, *Valuing the Environment: Courts' Struggles with Natural Resource Damages*, 32 ENVTL. L. 57 (2002) (discussing the difficulty of applying valuation methods such as contingent valuation to assess nonuse values, in a court setting).

121 Thierer, *supra* note 111, at 1086.

122 *Id.* at 1056.

123 *Id.*

124 ENCYCLOPEDIA BRITTANICA, *Federalism* (last viewed Dec. 2, 2018) https://www.britannica.com/topic/federalism.

125 Nicholas Bagley, *Federalism and the End of Obamacare*, 127 YALE L.J. FORUM 1 (Feb. 14, 2017).

126 *See* Dale B. Thompson, *Optimal Federalism across Institutions: Theory and Applications from Environmental Policies and Health Care*, 40 LOY. U. CHI. L.J. 437 (2009); Dale B. Thompson, *Immigration Policy through the Lens of Optimal Federalism*, 2 WM. & MARY POL'Y REV. 236 (2011); Dale B. Thompson, *"Unmistakably Clear" Coercion: Finding a Balance between Judicial Review of the Spending Power and Optimal Federalism*, 50 SAN DIEGO L. REV. 589 (2013) [hereinafter *Unmistakably Clear*].

127 *Unmistakably Clear*, *supra* note 126, at 591.

III. BENEFITS & COSTS OF ACQUIRING, USING, AND DISTRIBUTING HEALTH DATA IN OR BY WELLNESS PROGRAMS

This article now turns to analyzing the benefits and costs associated with collecting, using, and distributing health data in conjunction with an employer-sponsored wellness program. In doing benefit-cost analysis, we typically take a given regulation and then ask what its associated benefits and costs are. The benefits of a regulation include those that arise from the prevention of the harmful acts at which the regulation is directed, and the costs include opportunity costs of the activities that are foregone in order to comply with the regulation. However, for this analysis we are going to "flip" the benefits and costs: we will be looking at the benefits of the targeted activity, along with the costs that are imposed by those activities. This is because the purpose of this analysis is not to assess the benefits and costs of a given regulation, but rather to determine whether some sort of intervention—including regulation—is necessary, from the standpoint of social welfare. In essence, we are comparing the benefits and costs of the activity versus the "universe" of possible interventions and regulations.

We begin with the benefits from health data collected by employers or vendors for wellness programs. Table 1 in the Appendix displays the significant benefits, across the collection, use, and distribution of health data. By collecting health data, employers can create a consistent database of health information across the population of their employees. This database can be used to identify the health conditions that are the most significant overall threat to the workforce, enabling the employer to develop programs that target those conditions. This database can also be used to estimate health care expenditures and absenteeism.

Meanwhile, there are some benefits that arise from the disclosure of this health data to external parties. Third parties are interested in health data collected for a wellness program and the sale this kind of data is frequently sold.[128] These disclosures will entail social costs, but they do also have some benefits. The magnitude of these benefits can be estimated by the revenues generated by the sale of this data.

Table 2 lists the costs imposed by the collection, use, and distribution of health data. Collection of data involves direct and indirect costs. The direct costs are the costs of administering the surveys and tests, and of operating the wellness program. As mentioned above, the most common instrument is a health risk assessment (HRA); HRAs will collect information about "seat belt use, fruit and vegetable consumption, physical activity, stress, alcohol use, and current and past health conditions."[129] They also

---

128 *See* Ajunwa, Crawford & Ford, *supra* note 101, at 478 (noting that "investigations have confirmed that wellness vendors do frequently sell the data entrusted to them by employee participants").

129 Madison, *supra* note 33, at 2071.

may include "questions about cancer."[130] Tests may include biometric screening and genetic tests.

As also mentioned above, this data collection can lead to ethical issues about businesses collecting this wide array of information. Individuals may also be concerned about invasions of privacy. Privacy concerns include the "possibility of harm to distant persons, some not even born, that can result from certain kinds of DNA research;"[131] "risks . . . related to the information revealed about subjects' genetic inheritance[:] . . . anxiety, distress, and other psychological harms to subjects who learn that they carry genes that may predispose them to serious medical problems;"[132] the idea that employee health data is "lucrative data . . . to pharmaceutical companies interested in developing drugs or to data brokers to be used in creating various types of lists, including one reflecting credit risk;"[133] and "painful facts about family relationships (such as non-paternity)."[134]

The costs of discrimination can appear as a "disability-related stigma."[135] Employees may also be concerned that the purpose of wellness programs is to "root out 'costly' [higher health care cost] employees, who could then be targeted for termination."[136] Both privacy and discrimination concerns lead to social costs from the collection of data, and the possible distribution of that data, in the context of wellness programs.

Meanwhile, there are also costs associated with the use of data by wellness programs. As seen when Penn State University tried to impose a financial penalty for not completing HRAs or participating in screenings, wellness programs offering "sticks" can frequently lead to significant dissatisfaction in overall management.[137] This dissatisfaction can inhibit normal operation of businesses using these sticks as part of their wellness program, and thus lead to social costs.

A few key lessons derive from this analysis of benefits and costs of health data in wellness programs. Thierer pointed out that both the benefits and the costs from regulation of digital privacy were "remarkably subjective and contentious."[138] Similarly, the benefits from collecting data depend significantly upon the effectiveness of the wellness program in improving

---

130 *Id.*

131 Ronald M. Green & A. Mathew Thomas, *DNA: Five Distinguishing Features for Policy Analysis*, 11 HARV. J.L & TECH. 572 (1998).

132 *Id.*

133 *Id.* at 478.

134 *Id.* at 573.

135 Madison, *supra* note 33, at 2070.

136 Ajunwa, Crawford & Ford, *supra* note 101, at 478.

137 Dennis Scanlon & Dennis Shea, *Assessing the Evidence for Penn State University's "Take Care of Your Health" Benefits Program* 1-2, INCIDENTAL ECONOMIST (Sept. 20, 2013), http://theincidentaleconomist.com/wordpress/wp-content/uploads/2013/09/Scanlon-Shea-Assessing-the-Evidence-for-Penn-State-University_Sept_20_2013_correction.pdf.

138 Thierer, *supra* note 111, at 1056.

the health of workers, and in improving workers' perceptions of their company. Prior literature suggests that many wellness programs will not be effective, and that their effectiveness frequently depends upon factors beyond the programs themselves. Consequently, it will be difficult to provide a consistent estimate for these benefits. Similarly, just as noted by Thierer, the values of the impacts of potential privacy and discrimination violations are by their nature quite subjective, and their estimation will be contentious and depend significantly on underlying assumptions. This analysis is consistent with Arrow's 1963 article on the predominant role of uncertainty in health care.[139]

Another lesson is the significance of the level of employees' trust in their employers in determining both the benefits and costs from health data in wellness programs. The existing literature suggests that to have an effective wellness program, the corporate culture itself needs to embody a spirit of wellness. Furthermore, at the individual employee level, an effective wellness program requires an employee who is willing and motivated to make changes. Again, the literature suggests that that employee's willingness and motivation for change depends significantly upon his or her trust in the employer. The effectiveness of wellness programs, and the values of the benefits from health data, thus depend critically upon trust in employers.

Likewise, the costs of health data also depend upon trust in employers. How would the costs of privacy and discrimination be determined? An employee would calculate the expected value of breaches of privacy and discrimination. One component of expected value is the expected probability of an event. An employee who trusted a current employer would assign a lower probability of a breach happening than the same employee would assign to a different employer who was not trusted. As a result, the expected value of these privacy and discrimination breaches would have an inverse relationship with the level of trust in the employer.

When you put these two benefit and cost effects together, we see that net social value of health data in wellness programs is strongly related to employees' trust in their employers. Consequently, in a situation of low trust, i.e. where the benefits from health data in wellness programs can be extremely low but where their costs can be extremely high, it is quite likely that social welfare can be negatively impacted by the management of health data in wellness programs.

One more lesson to note is that most of these benefits and costs are contained within the total environment of the employers and their employees. However, one item in particular—the benefit of distributing health data beyond wellness programs—has impacts beyond employers and em-

---

139 *See generally* Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AMER. ECON. REV. 941 (1963).

ployees. This is the case where the health data might be used for other applications, such as marketing to employees. While employees may get some benefit from this marketing, a large part of the benefit from this data distribution will accrue to either the party selling the data, or to the party buying that data. Just as Thierer noted, market structure in the delivery of wellness programs has significant impacts, because health data may be acquired through a wellness program run by a wellness vendor who is external to the employer-employee universe.[140] Consequently, in many instances, the benefits from distributing health data beyond wellness programs may be captured completely by parties external to the employer-employee universe.

It is important to remember that this item, the benefit from distributing health data beyond wellness programs, is becoming more significant in the overall scope of wellness programs. This is because new technologies such as wearables and fitness apps collect even more information that would have significant values outside of the context of a wellness program, and in some cases are collected directly by external firms. As these new technologies become an even larger part of wellness programs,[141] the role of externalities becomes even more significant for health data and wellness programs.

IV. WHAT SHOULD WE DO?

Thus, our analysis of the benefits and costs of the collection, use, and distribution of health data show that uncertainty plays a major role in both benefits and costs, that this data can cause net social harm particularly in situations of low trust in employers, and that there are also significant externalities associated with health data in wellness programs. These findings remind us that the collection of data is not the neutral act of a scientist, but is rather a conscious policy choice, with associated benefits and costs. So how should public policy makers address health data in wellness programs?

One approach would be to enact federal legislation that puts regulatory responsibility for implementation and enforcement in the hands of federal agencies such as the Federal Trade Commission (FTC) or the EEOC. An article in the California Law Review[142] proposes a portfolio of federal legislative options for addressing concerns about worker surveillance in the context of "productivity apps and worker wellness programs [including] . . . (1) a comprehensive omnibus federal information privacy law, . . . (2) a narrower, sector-specific Employee Privacy Protection Act (EPPA), . . . and

---

140 *Id.* at 1087.

141 *See* Serxner, Kichlu, & Ratelis, *supra* note 27.

142 Ifeoma Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 735 (2017).

(3) an even narrower sector and sensitivity-specific Employee Health Information Privacy Act (EHIPA)."[143] Another recent article suggests amending the ADA to prohibit discrimination based on a health-data-based prediction of future health problems.[144]

Another approach would be to focus on education and information, and then let individual choice in the marketplace be the guide. As noted above, Thierer argues that for digital privacy "we should look to employ less restrictive solutions . . . before resorting to potentially costly and cumbersome legal and regulatory regimes that could disrupt the digital economy and the efficient provision of services that consumers desire."[145] These less restrictive solutions include "Education and Awareness-Building,"[146] "Transparency/Disclosure Solutions,"[147] "User Empowerment and Self-Help Solutions,"[148] "Self-Regulation and Codes of Conduct,"[149] and "Contracting Opportunities."[150] The rationale for these approaches lies in Thierer's and Fred Cate's assertion that "individual responsibility, not regulation, is the principal and most effective form of privacy protection in most settings."[151]

The idea here is that of the efficiency of perfectly competitive markets. When consumers have perfect information, their choice among a set of market competitors both reveals their preferences and leads to efficient outcomes. Individuals know their own preferences–which may be unknown and otherwise unobservable to an external regulator–and hence can make the best choice among a range of options. As a result, an educated and informed individual choice among market competitors, who have transparently self-regulated, is the one that seems to lead to the best outcome for society.

However, this article suggests that both of these approaches are incomplete in the context of health data in wellness programs. Federal legislation can create important inalienable[152] baselines for privacy and discrimination protections. But this article argues that state legislatures and state and local regulatory authorities should play significant roles in setting and enforcing policies related to health data in wellness programs. While there

---

143 *Id.* at 736.

144 Sharona Hoffman, *Big Data and the Americans with Disabilities Act*, 68 HASTINGS L.J. 777 (2017).

145 Thierer, *supra* note 111, at 1056.

146 *Id.* at 1091.

147 *Id.* at 1094.

148 *Id.* at 1095.

149 *Id.* at 1098.

150 *Id.* at 1100.

151 *Id.* at 1092.

152 *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

are current limits to state regulation of wellness programs,[153] states do have opportunities to develop new standards, and new federal legislation could extend the reach of state authority. Federal legislation that does not preempt[154] additional protections under state and local law can thereby enable an optimal federalism approach incorporating participation by state and local governments.

Meanwhile, individual choice should be an essential component to any approach to health data in wellness programs. Well-informed individuals are the best evaluators of the proper balancing of their own personal benefits and costs. The context of the employer-employee relationship also points to the need for using individual choice to enable heterogeneous employees to find the employer whose policies match their own preferences.

However, the fundamental problem of uncertainty in health care means that individuals can never be completely informed and educated prior to making their choices about health data in wellness programs. An individual might agree to genetic testing without fully appreciating the possible maladies that such testing might reveal.[155] Furthermore, the presence of externalities in the distribution of health data outside of the context of wellness programs means that individual choices may not be socially optimal ones.

Instead of using market choices alone to reveal preferences, this article argues that a combination of market choices in the context of differential regulatory regimes is necessary to fully elucidate optimal social approaches to health data in wellness programs. Just because benefits and costs are uncertain does not mean that we should foreclose regulatory options. Instead, an optimal federalism approach incorporating different levels of protection allows us to perform natural experiments to identify the socially optimal balancing of benefits and costs.

In an optimal federalism approach, different states would have different levels of protections. We can then examine the performance of these regulatory regimes to determine which generate the best outcomes in terms of health care results, company performance, and protections of privacy and discrimination interests. Heterogeneity of preferences for privacy and discrimination protections will probably lead to multiple optimal equilibria. However, it is only through the operation of an optimal federalism approach that these can be identified.

---

153 *See* discussion of ERISA *supra* Section I.c.

154 H.R. 1313, *see supra* Section I.c. If enacted, it could possibly preempt more stringent regulation of health data in wellness programs by state or local governments.

155 Behavioral economics provides many lessons on the limits of the rationality of individual decision-making. *See*, *e.g.*, Daniel Kahneman & Amos Tversky, *Prospect Theory: An Analysis of Decision under Risk*, 47 ECONOMETRICA 263 (1979); Christine Jolls, Cass R. Sunstein, & Richard Thaler, *A Behavioral Approach to Law and Economics*, 50 STAN. L. REV. 1471 (1998).

Consequently, what we should do is a combination of non-preemptive federal legislation on health data in wellness programs to provide baseline protections, education and information to promote appropriate individual choice, and differential state and local regulatory regimes based on optimal federalism to identify the regulatory approaches that best balance the benefits and costs of health data in wellness programs. Wellness programs, particularly with the advancements of new technologies such as wearables, provide opportunities to reduce health care costs and improve worker productivity and satisfaction. The potency of the employer-employee relationship also suggests that wellness programs may provide an excellent context for balancing the benefits and costs of the use of health data. Achievement of these objectives while protecting privacy and discrimination interests requires the use of both informed individual choice and optimal federalism.

APPENDIX

TABLE 1: Benefits of Health Data Collected by Employers / Wellness Vendors

Collection	Use		Disclosure
Create Consistent Database of Employees~	Direct		Revenues from external parties for alternative uses of data
		Lower Health Care Claims*~ [this is your typical Return-on-Investment for wellness programs]	
		Lower Absenteeism*~	
		Higher Productivity*~	
		Increased Retention*~	
	Indirect		
		Improvement in Health*~	
		Satisfaction in Health*~	
		Satisfaction in Workplace*~	

* Indicates magnitude depends on level of trust in employer by employees.
~ Indicates estimation is speculative, dependent upon a multitude of independent factors, or difficult to quantify.

TABLE 2: Costs of Health Data Collected by Employers / Wellness Vendors

Collection		Use		Disclosure
Direct		Direct		Privacy Issues*~
	Cost of Collecting Information		Costs of Operating Program	Concern for Discrimination*~
Indirect		Indirect		
	Ethical issues~		Sticks:*~ May lead to distrust of management	
	Privacy Issues*~			
	Concern for Dis-			