The FTC and Privacy: We Don't Need No Stinking Data

Thomas M. Lenard and Paul H. Rubin

In March 2012, the Federal Trade Commission issued a report recommending a new privacy framework for businesses and policymakers.[1] The new framework includes "best practices" intended to better inform consumers about the collection and use of information about them, provide consumers with easier-to-understand choices, including a "Do-Not-Track" option, and incorporate "privacy by design" in the development of firms' products and services. The result of these best practices would be to limit how businesses collect, retain, and use customer data. The report also supports baseline privacy and data security legislation.

The Commission Report was preceded by a preliminary Staff Report that spelled out the rationale for a new privacy framework.[2] The Staff Report stated that "[a]lthough many . . . companies manage consumer information responsibly, some appear to treat it in an irresponsible or even reckless manner."[3] "[M]any companies . . . do not adequately address consumer privacy interests" and, therefore, the "[i]ndustry must do better."[4] However, neither the preliminary Staff Report nor the final Commission Report provide data to support these assertions or shed light on whether the recommended framework would improve consumer welfare relative to the status quo or to alternative proposals. Instead, the FTC, to a great degree, relies on statements at FTC roundtables, including those of well-known "privacy advocates," as evidence for their findings.[5]

Analysis That Should Precede Regulation

We begin with the premise that, before undertaking a major regulatory effort, regulators should determine, first, whether there is a market failure (if the market in question is working properly, then there is no reason to proceed further) and, second, whether there is a remedy available that will yield benefits greater than costs.

Market Failure? Market failures (distortions or inefficiencies due to improper pricing or inefficient definitions of property rights) often involve information problems, such as "lemons" problems (asymmetric information), free rider problems, and public goods problems. For example, if someone's identity is stolen, the victim probably will not know the source the thief used to obtain the information. This makes it difficult to impose costs on the source, and, as a result, reduces incen-

■

Thomas Lenard *is the President of the Technology Policy Institute.* ***Paul Rubin*** *is a Professor of Economics at Emory University and Senior Fellow with the Technology Policy Institute.* *The authors thank Eliska Repkova and Corwin Rhyan for assistance with earlier versions.*

[1] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change—Recommendations for Businesses and Policymakers* (Mar. 2012) [hereinafter Commission Report].

[2] Protecting Consumer Privacy in an Era of Rapid Change—A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report (Dec. 2010) [hereinafter Staff Report].

[3] *Id.* at i.

[4] *Id.*

[5] These include the Center for Democracy & Technology, The Electronic Frontier Foundation, Electronic Privacy Information Center, and the Consumer Federation of America. *See id.* nn. 53, 55, 56, 58, 59, 61, 66, 71, 75, 81, 82, 83, 84, 87, 89, 99.

tives for those who possess information to adequately protect it. However, there are countervailing forces. For example, with respect to identity fraud, consumers are liable for little, if any, of the direct losses. Rather, credit card companies, which are better able to ascertain the source of the security breach, assume responsibility for direct losses, helping to reduce any market failure.[6] Consumers are still subject to indirect costs, but the credit card companies have strong interests in encouraging the use of their products, and therefore strong interests in creating and maintaining consumer confidence through data security measures.

The Commission and Staff Reports do not provide a rigorous analysis of whether market failures exist with respect to privacy. The only systematic evidence on privacy practices referred to in the reports is out of date and likely does not represent practices today.

The most recent surveys of the privacy practices of commercial websites are more than a decade old, and the FTC did not conduct a current survey before issuing its reports.

The most recent surveys of the privacy practices of commercial websites are more than a decade old, and the FTC did not conduct a current survey before issuing its reports. Given the changes in the online world, these data are no longer current, but they illustrate the type of data collection and analysis that should be a prerequisite to privacy policy recommendations. Notably, the period covered by the surveys saw a general improvement in the privacy practices of commercial websites. For example, the most recent (2001) survey found that relative to a 2000 FTC survey:[7]

- Websites were collecting less information.
- Fewer websites were using third-party cookies.
- Privacy notices were more prevalent, more prominent, and more complete.
- Consumers had more opportunities to choose how personally identifiable information (PII) was used.
- More sites were offering opt-in and fewer opt-out privacy options.
- More sites were offering a combination of fair information practice elements.
- Seal programs (in which trusted third parties guarantee security) were growing relatively slowly.

The Staff Report references the 2000 FTC survey, noting that "only about one-quarter of the privacy policies surveyed addressed the four fair information practice principles of notice, choice, access, and security."[8] However, the 2001 survey found that 80 percent of the most popular domains implemented notice, choice, and security—up from 63 percent in the 2000 survey—and 48 percent of a random sample (which included much smaller sites) implemented those three practices—up from 27 percent a year earlier.[9]

We are not aware of any studies indicating whether the period since 2001 saw further improve-

---

[6] *See* Thomas M. Lenard & Paul H. Rubin, *Much Ado About Notification*, REGULATION, Spring 2006, at 44–50.

[7] William F. Adkinson, Jr., Jeffrey A. Eisenach & Thomas M. Lenard, *Privacy Online: A Report on the Information Practices and Policies of Commercial Websites* (Mar. 2002) [hereinafter *Progress & Freedom Foundation Report*], *available at* http://www.pff.org/issues-pubs/books/020301privacyonlinereport.pdf; *see also* Fed. Trade Comm'n, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000) [hereinafter FTC 2000 Report], *available at* http://ftc.gov/reports/privacy2000/privacy2000text.pdf; Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission (June 1999), *available at* http://web.archive.org/web/20040204202945/http://www.msb.edu/faculty/culnanm/GIPPS/gipps1.PDF; Fed. Trade Comm'n, *Privacy Online: A Report to Congress* (June 1998) [hereinafter FTC 1998 Report], *available at* http://www.ftc.gov/reports/privcy3/index.htm.

[8] Staff Report, *supra* note 2, at 8.

[9] *Progress & Freedom Foundation Report*, *supra* note 7, at 24. The 2001 survey, while the same as the 2000 survey in all other respects, did not address access practices because of its "unique implementation issues." FTC 2000 Report, supra note 7, at 17.

ment in privacy practices or what commercial website practices are today. It is inappropriate for the FTC to call for a massive new regulatory scheme when the only available systematic surveys of the industry are both out of date and suggest significant improvement over time.

The Need for Cost-Benefit Analysis. Market failure is not enough to justify regulation. It is also necessary to show that the proposed regulation is desirable. That requires an assessment of the benefits and costs of the proposed remedies.

Many types of regulatory proposals are subject to this type of analysis under President Clinton's Executive Order 12866 and preceding executive orders. (The FTC, as an independent agency, is not subject to this order but has the option of following its principles.) The principles of E.O. 12866 were reaffirmed by President Obama:

> As stated in that Executive Order [12866] and to the extent permitted by law, each agency must, among other things: (1) propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs (recognizing that some benefits and costs are difficult to quantify) . . . (3) select, in choosing among alternative regulatory approaches, those approaches that maximize net benefits . . . .[10]

It seems clear that greater privacy protections will involve tradeoffs—costs to Internet businesses, as well as to consumers.

There is no such analysis in either of the FTC reports. Instead, the FTC's conclusions appear to be largely based on "the major themes and concepts developed through the roundtables."[11] However, "themes and concepts" developed from roundtables are an inadequate substitute for a careful evaluation of the benefits and costs of alternative privacy regimes (including the status quo) to determine which will best serve the interests of consumers. Because the FTC has presented no data on either benefits or costs, it is impossible to know whether any of the agency's recommendations would improve consumer welfare.

It seems clear that greater privacy protections will involve tradeoffs—costs to Internet businesses, as well as to consumers. The commercial use of online information produces a range of benefits, including advertising targeted to consumers' interests, advertising-supported services (such as email, search engines, and fraud detection), and a reduction in other threats, such as malware and phishing.[12] More privacy, in the current context, means less information available for the marketplace and therefore fewer of these benefits to consumers.[13] Even if the services are still offered, they will be of lower quality as providers will have less money and less data to use in providing services.

Several studies support this intuition. On the cost side, a recent study by Goldfarb and Tucker found that the European Privacy Directive, which limits the use of information, reduced the effectiveness of online advertising by about 65 percent.[14] This suggests that privacy protections make advertising less useful to consumers and less valuable to advertisers. Advertisers will pay less for less-effective ads, which decreases the resources available to support online content. The authors found the effect to be particularly pronounced for more general (less product-specific) websites, such as newspapers.

---

[10] Exec. Order 13563, Improving Regulation and Regulatory Review (Jan. 17, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/01/18/improving-regulation-and-regulatory-review-executive-order.

[11] Staff Report, *supra* note 2, at iv.

[12] The benefits of information are laid out in detail in Thomas M. Lenard & Paul H. Rubin, *In Defense of Data: Information and the Costs of Privacy*, 2 POLICY & INTERNET 149 (2010), http://www.psocommons.org/policyandinternet/vol2/iss1/art7/.

[13] The Staff Report mentions some of the benefits produced by consumer data but does not evaluate the tradeoffs inherent in greater privacy protections. *See, e.g.*, Staff Report, *supra* note 2, at 21, 33–35.

[14] Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Online Advertising*, 57 MANAGEMENT SCI. 57 (2011).

These results are reinforced by a study by Howard Beales, which shows the rates for behaviorally targeted advertising to be more than twice the rates for untargeted ads.[15] Again, this result stems from the greater value that consumers receive from ads targeted to their interest, which ultimately increases the revenue available to support content. The FTC has made no effort to determine the impact of its regulations on such content, or on the degree to which its regulations will prevent consumers from even having the option for such content.

Although only a few empirical studies of the costs of privacy regulation exist, even less information is available on benefits. The FTC takes a broad view of the benefits of privacy. The agency rejects an approach limited to physical or economic injury because

> the actual range of privacy-related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information "out there." Consumers may feel harmed when their personal information—particularly sensitive health or financial information—is collected, used, or shared without their knowledge or consent or in a manner that is contrary to their expectations. For instance, the Commission's online behavioral advertising work has highlighted consumers' discomfort with the tracking of their online searches and browsing activities, which they believe to be private.[16]

Neither FTC report contains any data on any harm, however defined. Demonstrating, and to the extent feasible quantifying, harm is important because it can be the starting point for assessing benefits, which are the reduced harms associated with increased privacy protection.

Neither report demonstrates that its proposals would reduce the amount of any existing consumer harm. For example, assume that consumers' discomfort with their information being "out there" is a major element of harm. The Staff Report provides no evidence or explanation as to how or whether its proposed framework would make consumers feel significantly more comfortable. Without a dramatic change in the Internet ecosystem, a substantial amount of information would remain "out there." What, if anything, is the incremental benefit provided by the FTC's proposed regulations? We do not know.

Another way to assess the benefits of additional online privacy is by using market-generated information to measure how much consumers are willing to pay for more privacy. Economists usually prefer basing consumers' willingness to pay on observed market behavior because how people behave when confronted with actual market choices better reflects their real preferences than do responses to survey questionnaires or behavior observed in experiments. The widespread use of free, advertising-supported services, such as email and online news subscriptions, suggests that people routinely give up some information about themselves in return for access to content, more useful advertising, and other services, although the transaction is indirect. That is, consumers often are willing to exchange less privacy for the resulting benefits. The FTC has not done a similar balancing.

Application of Standard Regulatory Principles to the FTC's Proposed Privacy Framework

The FTC's proposed framework is intended to correct perceived shortcomings in the "notice-and-choice" and "harm-based" models of consumer injury. The Commission Report claims the notice-and-choice model is unsatisfactory because consumers do not understand how their data are

---

[15] Howard Beales, *The Value of Behavioral Targeting*, *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, at 3.

[16] Staff Report, *supra* note 2, at 20–21.

being used or the posted privacy notices.[17] Likewise, it claims that the harm-based approach is unsatisfactory because, as indicated above, it focuses on an overly narrow range of harms. To correct these deficiencies, the FTC recommends that companies adopt privacy by design, offer simplified choices to consumers about their data practices (including a Do-Not-Track option for browsers), make their data practices more transparent to consumers, provide consumers with reasonable access to their data, and obtain affirmative consent for retroactive changes to data policies.[18] The Commission and Staff Reports provide virtually no analysis of the benefits or costs of any of these proposals.

Privacy by Design. Privacy by design includes providing "reasonable" security for consumer data; "limit[ing] data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law;" retaining data only as long as necessary to fulfill the purpose for which it was originally collected; and safely disposing of data no longer being used, while ensuring the accuracy of data, particularly if the data could cause significant harm to consumers.[19] In addition, companies should have comprehensive data-management procedures, including training employees on privacy issues and conducting regular privacy reviews for products and services. As discussed above, the Commission and Staff Reports contain no analysis of how companies currently address privacy within their organizations or the extent to which companies already take such steps (without the additional burden of regulatory monitoring). Many companies already have Chief Privacy Officers and devote significant resources to privacy and data security, but the Commission does not appear to have data on these metrics.

The Commission Report notes that the Commission has brought thirty-six cases against companies that failed to provide reasonable security.[20] In addition, the Commission has entered into settlements with Google and Facebook, after accusing the companies of deceptive practices.[21] The Commission Report does not explain why the Commission's current enforcement authority, together with other substantial incentives that companies already have to protect data, is insufficient. Building greater privacy protections into operations and products and services and assigning additional personnel to privacy issues entails costs that companies would likely pass through to consumers. There is no analysis of what the costs or the benefits of this "privacy by design" would be. Do consumers want companies to incur these costs or would they instead prefer to pay lower prices?

Simplified Choice. The Commission Report proposes requiring companies to offer choice for practices that are not "commonly accepted." Whether a practice is commonly accepted would depend on "the extent to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law."[22] Commonly accepted practices would include product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and most first-party marketing.[23] The Commission Report does not analyze the implications or the costs and benefits of making it more difficult to use data for all the remaining "not commonly accepted" practices.

---

[17] Commission Report, *supra* note 1, at 2.

[18] *Id.* at i, iv, and 57.

[19] *Id.* at 27–29.

[20] *Id.* at 24.

[21] *Id.* at 31.

Do Not Track. The Staff Report endorsed a Do-Not-Track mechanism that would allow consumers to opt out of collecting behavioral data for most purposes but, at the same time, asked commenters a series of questions on how a mechanism should be designed and what its impact would be, including:[24]

- What are the potential costs and benefits of offering a standardized uniform choice mechanism to control online behavioral advertising?
- How many consumers would likely choose to avoid receiving targeted advertising?
- How many consumers, on an absolute and percentage basis, have used the opt-out tools currently provided?
- What is the likely impact if large numbers of consumers elect to opt out? How would it affect online publishers and advertisers, and how would it affect consumers?

Due to the popularity of the telemarketing Do-Not-Call List, a Do-Not-Track mechanism may sound like a good idea. But the similarities between the two end at the names.

These are questions the FTC staff itself should have researched before endorsing the Do-Not-Track mechanism. Despite the lack of research, the Commission Report also endorsed a Do-Not-Track mechanism.[25] Partly as a result of the FTC's recommendations, the World Wide Web Consortium (W3C) is developing an industrywide Do-Not-Track standard and the three major browser providers—Google, Microsoft, and Mozilla—have announced that their products will include Do-Not-Track mechanisms.[26]

Due to the popularity of the telemarketing Do-Not-Call List, a Do-Not-Track mechanism may sound like a good idea. But the similarities between the two end at the names. For example, people sign up for the Do-Not-Call List to reduce unwanted marketing solicitations. A Do-Not-Track mechanism would not do that. Consumers would not necessarily receive fewer ads. (Indeed, for that reason, it might be difficult for them to know if the mechanism was actually working.) They would just receive ads that are less well-targeted to their interests. (Several free tools already let consumers block all online ads on the Internet.)

Some people may use a Do-Not-Track mechanism because they like knowing they are not being tracked. As the discussion above indicates, although this value is not easily quantifiable, the FTC staff should have considered what is known about consumers' valuation of privacy and should perhaps sponsor additional research in the area.[27]

These potential benefits need to be weighed against the costs, assuming a Do-Not-Track mechanism is technically feasible.[28] First, what are the direct costs of implementation? Second, what are the indirect costs in terms of the quantity and quality of services and content on the Internet? Many of these costs would be borne not only by Do-Not-Track participants but by other Internet users as well. A Do-Not-Track mechanism (depending on how many people used it) would reduce the value of the Internet as an advertising medium and therefore would reduce the

---

[22] *Id.* at 38–39.

[23] *Id.*

[24] Staff Report, *supra* note 2, at A-4.

[25] Commission Report, *supra* note 1, at 53.

[26] *See* Commission Report, *supra* note 1, at 54; Sebastian Anthony, *Do Not Track: Analysis of Google, Microsoft and Mozilla's Solutions*, SWITCHED.COM, Jan. 26, 2011, *available at* http://downloadsquad.switched.com/2011/01/26/do-not-track-analysis-of-google-microsoft-and-mozillas-solutions/.

[27] This point is also made in Commissioner William Kovacic's concurring statement. *See* Staff Report, *supra* note 2, at D-1.

[28] *See* Staff Report, *supra* note 2, at E-6 (concurring statement of Commissioner W. Thomas Rosch).

revenues available to support Internet content. Finally, consumers who use a Do-Not-Track mechanism will receive ads that are less well-targeted and therefore less useful. The cost of this would depend on the value these consumers place on relevant advertising.

Increased Transparency. The Staff Report and the Commission Report call for increased transparency,[29] noting that many consumers do not understand how their data are collected and used and that privacy notices are complex. This is undoubtedly true, because the use of data online is quite complicated. Accordingly, the framework proposes steps to make data practices more transparent to consumers. It recommends that privacy notices should be clearer, simpler to understand, and more transparent.

Transparency and simplicity are worthwhile goals but are unlikely to be costless. Simplifying privacy notices might not just affect the notices. Because the FTC penalizes firms if they do not adhere strictly to announced policies, simplifying notices could affect the ways companies use data, which would be constrained to conform to the notice standards. Thus, implementing transparency and simplicity requirements could reduce benefits to consumers and impose costs on businesses. Whether this is an important issue or not is unclear, but it should be analyzed.

Access. Previous FTC reports have acknowledged the complexity of providing consumers with the ability to examine data about themselves and potentially to challenge their accuracy. The FTC 2000 Report stated that "the Commission believes that Access presents unique implementation issues . . . including what categories of data must be made available; the costs and benefits of providing access; and how to ensure adequate authentication . . . ."[30] Yet, neither the Staff Report nor the Commission Report addressed whether access is valuable to consumers, how it would actually be implemented, and its potential to reduce the security of personal information.

Affirmative Consent for Retroactive Changes to Data Policies. The Staff Report and the Commission Report encourage firms to seek affirmative consent before revising their data policies to allow for greater use of previously collected data. Requiring that consumers have the opportunity to consent to "new uses" of data may have the unintended consequence of inducing firms to adopt overly vague data policies that are consistent with a very broad set of uses because of the strong tendency of consumers to stay with the default.[31] To allow the use of data in innovative and beneficial ways, less specific data policies would offer more flexibility to companies but would at the same time diminish the usefulness of the privacy policies to consumers. An example of how FTC action might lead to less transparency comes from the recent fine levied against Google for violating an agreement to not misrepresent its privacy policies.[32] In this instance, which involved Google's +1 feature and tracking cookies, had Google initially been less specific, it might have avoided the historic fine of $22.5 million.

Additionally, the requirement of consent for "new uses" discourages the development of new or lower-cost products or services based on existing information. The recent Department of Commerce Green Paper recognizes this concern. While proposing that companies should incorporate "purpose specifications" and "use limitations" in their notices and privacy practices, the Green Paper notes that "[t]he current privacy policy framework has created an environment in

---

[29] Commission Report, *supra* note 1, at 60.

[30] FTC 2000 Report, *supra* note 7, at 17.

[31] Lenard & Rubin, *supra* note 12, at 174.

[32] Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), http://www.ftc.gov/opa/2012/08/google.shtm.

which 'creative re-use of existing information' has led to innovations."[33] The Green Paper provides a useful hypothetical that illustrates the potential tradeoff:

> [S]uppose that company executives have grown concerned with security threats against its network equipment and customers' computers. The Chief Executive Officer (CEO) approves a proposal to provide . . . Internet usage records . . . to in-house researchers, so that they can analyze network traffic and develop security countermeasures. This use of personal information has the clear potential to bring privacy and security benefits to the ISP and its customers. The proposed use, however, would also be contrary to the ISP's specified purposes for collecting the information in the first place.[34]

The privacy debate is taking place in an empirical vacuum. The FTC has developed policy recommendations without the benefit of systematic data on current privacy practices of firms or consumers, or systematic analysis of the benefits or costs of alternative privacy regimes.

There are likely to be new commercial uses (unrelated to security) that also might benefit consumers. It is important to carefully weigh the privacy benefits against the costs of not being able to use data for new uses. Obviously, new uses are not going to be known at the time a privacy rule or practice is being implemented. Innovations forgone are, by their nature, difficult to identify or measure.

Conclusion

The privacy debate is taking place in an empirical vacuum. The FTC has developed policy recommendations without the benefit of systematic data on current privacy practices of firms or consumers, or systematic analysis of the benefits or costs of alternative privacy regimes. Some of the neglected issues include:

- Collecting current data on the privacy and data-management practices of major websites. The most recent data referenced in the Staff Report are from 2000.
- Producing systematic evidence showing whether current practices are harming consumers. Although the Staff Report rejects a harm-based approach, the proposed framework will only produce benefits to the extent it alleviates identified harms.
- Reviewing what is known about how consumers value privacy and undertaking additional studies as a basis for estimating the benefits of a new privacy framework.
- Estimating the costs of the proposed framework and alternatives, including direct pecuniary costs to firms from devoting more resources to privacy and the indirect costs of having less information available. The Staff Report does not acknowledge that its proposal would entail any costs.
- Producing sufficient evidence of a reasonable expectation that the benefits of the proposal are greater than the costs. Otherwise, the proposal should not be adopted.

Although the staff acknowledged the need to assess the costs and benefits of its most prominent proposal, a Do-Not-Track mechanism, the Commission endorsed the proposal without the benefit of an assessment.

Because the Commission and Staff Reports provide virtually no new data or analysis, they are seriously deficient as a foundation for new policy recommendations. They also violate the spirit, if not the letter, of President Obama's recent executive order on regulation, which stresses the need to evaluate both benefits and costs. Without such analysis, there is no way of knowing whether a particular regulatory action will improve or reduce consumer welfare. ●

---

[33] U.S. Dep't of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* 38 (Dec. 2010), *available at* http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf.

[34] *Id.* at 39.