Berkeley Technology Law Journal

Volume 26 | Issue 3 Article 6

6-1-2011

Regulating Privacy by Design

Ira S. Rubinstein

Link to publisher version (DOI)
http://dx.doi.org/https://doi.org/10.15779/Z38368N

Berkeley

[technology law Journal]

VOLUME 26
NUMBER 3
2011

UNIVERSITY OF CALIFORNIA, BERKELEY
SCHOOL OF LAW
BOALT HALL

Production: Produced by members of the *Berkeley Technology Law Journal*. All editing and layout done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.
The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Berkeley Technology Law Journal
U.C. Berkeley School of Law
Student Center, Ste. 3
Berkeley, California 94720-7200
btlj@law.berkeley.edu
http://www.btlj.org

REGULATING PRIVACY BY DESIGN

Ira S. Rubinstein[†]

TABLE OF CONTENTS

---

† Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law. This Article was presented at the NYU Privacy Research Group, the Princeton's Center for Information Technology Policy, and the Privacy Law Scholars Conference and I am grateful for the comments of workshop participants. For detailed comments on an early draft, I am indebted to Kelly Caine, Peter Cullen, Erin Egan, Jacques Lawarrée, Ron Lee, Paul Schwartz, and Tal Zarsky. Thanks are also due to Solon Borcas, Travis Breaux, Anapum Datta, Cathy Dwyer, Kenneth Farrall, Foster Provost, and Adam Shostack for insights on various technology-related issues, and to Jeramie Scott for able research assistance. A grant from The Privacy Projects supported this work.

I. INTRODUCTION

Privacy officials in Europe and the United States are embracing privacy by design as never before. This is the idea that in designing information and communications technologies ("ICT"), building in privacy from the outset achieves better results than bolting it on at the end.[1] The European Union Data Protection Directive has always included provisions requiring data controllers to implement "technical and organizational measures" in the design and operation of ICT.[2] But this has proven insufficient and in their new call for privacy by design, the European Commission ("EC") hopes to see data protection principles taken into account at the outset of designing, producing, or acquiring ICT systems. In particular, they are encouraging both the use of Privacy Enhancing Technologies, or PETs, as well as default settings that favor privacy.[3]

1. *See* Ann Cavoukian, *Privacy by Design*, INFO. & PRIVACY COMM'R, 1 (2009), http://www.ipc.on.ca/images/Resources/privacybydesign.pdf (stating that she "first developed the term 'Privacy by Design' back in the '90s" and that " 'Build in privacy from the outset' has been [her] longstanding mantra, to 'avoid making costly mistakes later on, requiring expensive retrofits' "); *see also Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Agenda for Europe*, COM (2010) 245 final/2 (Aug. 26, 2010), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF [hereinafter EC, *A Digital Agenda for Europe*].

2. Council Directive 95/46 requires data controllers to "implement appropriate technical and organizational measures" for safeguarding personal data. In addition, Recital 46 calls for such measures to be taken, "both at the time of the design of the processing system and at the time of the processing itself." Directive 95/46/EC, 1995 O.J. (L 281) 31 (Nov. 23, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter EU Data Protection Directive].

3. *See* ART. 29 DATA PROTECTION WORKING PARTY, 02356/09/EN, WP 168, THE FUTURE OF PRIVACY (2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf; John J. Borking & Charles D. Raab, *Laws, PETs and Other Technologies for Privacy Protection*, 2001 J. INFO L. & TECH., no. 1, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/ (noting that PETs have a very specific meaning, namely, "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system"). This same definition is cited in *Commission Communication on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM (2007) 228 final (May 2, 2007). In 1995, in one of the earliest discussions of PETs, privacy commissioners from Ontario, Canada and the Netherlands collaborated on a paper describing the privacy concerns associated with the trail of identifying information created by electronic transactions and a number of techniques that would permit users to engage in

In the United States, a recent staff report of the Federal Trade Commission ("FTC") describes a Proposed Framework with three main components: privacy by design, simplified consumer choice, and increased transparency of data practices.[4] According to the Staff Report, companies engage in privacy by design when they promote consumer privacy throughout their organizations and at every stage of the development of their products and services.[5] More specifically, privacy by design has two main elements: first, incorporating substantive privacy protections into a firm's practices; and second, maintaining comprehensive data management procedures throughout the life cycle of their products and services.[6] The report also briefly mentions the use of PETs such as identity management, data tagging tools, transport encryption, and tools to "check and adjust default settings."[7] In short, regulators on both sides of the Atlantic agree on the need for a new legal framework to protect online privacy in the twenty-first century and that one of its major aspects should be privacy by design.

Although PETs and privacy by design resist precise definition and even overlap as to their usage, the two ideas are not identical. Their differences may be summed up as follows: PETs are applications or tools with discrete goals that address a single dimension of privacy, such as anonymity, confidentiality, or control over personal information. Frequently, PETs are added onto existing systems, sometimes as an afterthought by designers and sometimes by privacy-sensitive end-users.[8] In contrast, privacy by design is not a specific technology or product but a systematic approach to designing

transactions without revealing their identity. *See* 2 INFO. AND PRIVACY COMM'R (Ontario, Canada) & REGISTRATIEKAMER (Netherlands), PRIVACY-ENHANCING TECHNOLOGIES: THE PATH TO ANONYMITY (1995), *available at* http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf [hereinafter 1995 PETS REPORT] (proposing the use of "identity protectors" that "separate one's true identity from the details of one's transactions through the use of 'pseudo-identities' "). Although this 1995 report treats PETs primarily in these terms, the 2007 communication from the EC reflects a much broader view of PETs as encompassing not only identity protection but various encryption tools, cookie managers and other filtering devices, as well as data management protocols such as the Platform for Privacy Preferences ("P3P").

4. BUREAU OF CONSUMER PROTECTION, FED. TRADE COMM'N (FTC), PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter FTC STAFF REPORT].

5. *Id.* at 41.

6. *Id.* at 44–52.

7. *Id.* at 52 n.131.

8. Indeed, many PETs now take the form of so-called "browser add-ons." *See* Jim Brock, *Are Privacy Add-Ons Effective? Surprising Results from Our Testing*, PRIVACYCHOICE (Nov. 17, 2010), http://blog.privacychoice.org/2010/11/17/are-privacy-add-ons-effective-surprising-results-from-our-testing/ (comparing the effectiveness of a single type of privacy add-on that blocks efforts by data and marketing companies to track online activity).

any technology that embeds privacy into the underlying specifications or architecture.[9] Although PETs and privacy by design are distinguishable, these two phrases have no established usage and regulators and commentators often use them interchangeably.

Despite the endorsement of regulators, PETs have not achieved widespread acceptance in the marketplace, and relatively few firms have embraced privacy by design.[10] Confusion over a variety of key definitions contributes to this slow pace of adoption. For instance, it is not yet clear how the concept of "privacy by design" relates to certain technologies or organizational measures, nor what regulators really have in mind when they urge firms developing products to build in privacy.

Economics also plays an important role in determining the adoption rate of PETs and privacy design practices. On the consumer side, few PETs have proven popular and the demand for products and services with strong privacy safeguards seems quite limited. Reasons include consumers' lack of knowledge concerning the privacy risks associated with web surfing, search, social networks, e-commerce, and other daily internet activities and their limited understanding of how PETs or privacy by design might help reduce these risks. Further, cognitive and behavioral biases may prevent some individuals from acting in accordance with their stated preference for greater privacy. Other consumers just do not care very much about privacy.[11] On the business side, weak consumer demand discourages information technology ("IT") spending. Moreover, given the huge profits many firms derive from online advertising, they are reluctant to voluntarily implement PETs or design practices that would limit their ability to collect, analyze, or share valuable consumer data.[12]

Although the European Commission sponsored a study of the economic costs and benefits of PETs, and the United Kingdom is looking at how to improve the business case for investing in privacy by design, there is scant evidence that privacy technology pays for itself, much less confers a competitive advantage on firms that adopt it. Indeed, the economic or regulatory incentives for adopting privacy by design need more attention in Europe and are largely absent from the FTC report. In the meantime, the regulatory implications of privacy by design are murky at best, not only for firms that might adopt this approach but for free riders as well.

---

9. *See* Cavoukian, *supra* note 1, at 1 (noting that "[embedding privacy] may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems").

10. *See infra* Sections III.A, III.C.

11. *See infra* Section III.A.

12. *See infra* Section III.C.

This Article seeks to clarify the meaning of privacy by design and to suggest how privacy officials might develop appropriate regulatory incentives that offset the certain economic costs and somewhat uncertain privacy benefits of this new approach. Part II begins by developing a taxonomy of PETs, classifying them as substitutes or complements depending on how they interact with data protection or privacy laws. Substitute PETs aim for zero-collection of personal data[13] and, if successful, make legal protections less important or even superfluous. In contrast, complementary PETs fall into two subcategories: those which are privacy-friendly and those which are privacy-preserving. These are familiar terms within the privacy literature but they have no fixed meaning. As used here, "privacy-friendly" means literally a system or even a feature that welcomes individual control over personal data, mainly through enhanced notice, choice, and access, whereas "privacy-preserving" refers to a much smaller number of systems offering provable guarantees of privacy, mainly through cryptographic protocols or other sophisticated measures.

Part III explores the meaning of privacy by design in the specific context of the FTC's emerging concept of comprehensive information privacy programs ("CIPPs"). It also looks at how privacy by design practices relate to the use of PETs and at the activities of a few industry leaders, who rely on engineering approaches and related tools to implement privacy principles throughout the product development and the data management lifecycles. Building on this analysis, and using targeted advertising as a primary illustration against the backdrop of the FTC analysis, the Article then suggests that economic incentives are inadequate to ensure widespread adoption of PETs or significant investments in the design aspects of CIPPs.

Finally, Part IV considers how regulators might achieve better success in promoting the use of privacy by design by (1) identifying best practices, including prohibited practices, required practices, and recommended practices, which are compiled in the Appendix; and (2) situating these best practices within an innovative regulatory framework that (a) promotes experimentation with new technologies and engineering practices; (b) encourages regulatory agreements through stakeholder representation, face-to-face negotiations, and consensus-based decision making; and (c) supports flexible, incentive-driven safe harbor mechanisms as defined by newly proposed privacy legislation.

---

13. The EU Data Protection Directive defines "personal data" as "any information relating to an identified or identifiable natural person." EU Data Protection Directive, *supra* note 2, art. 2(a). In the United States, the cognate concept is personally identifiable information ("PII").

II. PETS AND PRIVACY BY DESIGN

The FTC's Proposed Framework states that companies should develop and implement CIPPs to ensure proper incorporation of the four substantive principles identified in the report (data security, reasonable collection limitations, sound retention practices, and data accuracy).[14] The two core elements of CIPPs are (1) assigning specific personnel the responsibility of privacy training, and (2) promoting accountability for privacy policies and assessing and mitigating privacy risks. These privacy assessments should occur before a product launches and periodically thereafter to address any changes in data risks or other circumstances. The size and scope of a CIPP should be determined based on the data at stake and the risks of processing such data, with companies that collect vast amounts of consumer data or sensitive data required to devote more resources than those collecting small amounts of non-sensitive data. Finally, the report mentions in passing that the FTC staff supports the use of PETs.[15]

The Staff Report's enticing description of privacy by design has great intuitive appeal. Why is this? The FTC's discussion suggests that privacy by design generally reduces errors and costs,[16] yet this discussion remains short on specifics and never quite explains what privacy by design amounts to. Do companies engage in privacy by design by making more and better use of PETs and, if so, what sorts of PETs are most effective and why? The report recommends, without discussion, the use of several kinds of PETs (identity management, data tagging tools, transport encryption, and tools to check and adjust default settings),[17] but it makes no effort to differentiate them according to relevant criteria. Alternatively, does privacy by design mean that companies should implement specific design practices or compliance measures? Without more detailed guidance, firms will not know what they are supposed to do (or not do), how much they should spend to achieve the desired outcomes, or to what extent this approach will enhance their standing

14. *See* FTC STAFF REPORT, *supra* note 4, at 50.

15. *See id.* at 44–52. For a more detailed FTC statement describing CIPPs in terms of five major elements, see *infra* notes 66–71 and accompanying text.

16. There is evidence that resolving security issues during the design phase is more efficient and less costly than having to deal with it later in the development process. *See* MARK GRAFF & KENNETH VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES 56 (2003) (citing evidence that the cost of a bug fix at design time is considerably less than the cost of fixing the same bug during implementation or testing, a disparity that only increases if a patch is required). It is beyond the scope of this Article to determine whether privacy design flaws are analogous to security bugs or if it is also cheaper to fix the former at an early as opposed to a later stage.

17. *See* FTC STAFF REPORT, *supra* note 4, at 52.

with regulators. The following discussion lays the groundwork for examining these issues by developing a new taxonomy of PETs, exploring the meaning of privacy by design, and comparing existing private sector approaches to the FTC's analysis in the Staff Report.

A. THE SUCCESSES AND FAILURES OF PETS

PETs have been around for about twenty-five years. Many PETs reflect major advances in cryptographic research, which have also enabled advanced privacy features such as anonymous payment systems, anonymous protection for real-time communications, authentication via anonymous credential schemes, and methods for anonymously retrieving online content.[18] Identity protectors and related PETs were first introduced as a regulatory strategy in the 1995 report on the "path to anonymity."[19] However, as Feigenbaum and her colleagues summed it up a little more than fifteen years later: "Despite the apparent profusion of such technologies, few are in widespread use. Furthermore, even if they were in widespread use, they would not necessarily eliminate" various deployment problems.[20]

Of course, not all PETs rely on anonymity protocols. The term encompasses a range of tools beyond anonymity including those that enhance notice and choice, help automate communication and/or enforcement of privacy policies, or ensure confidentiality via encryption. Arguably, anonymity tools are the most effective PETs precisely because they prevent identification or collection of personal data in the first place, irrespective of legal requirements. As a result, they are sometimes referred to as true or pure PETs.[21] In contrast, other privacy tools permit data collection and analysis but seek to assist knowledgeable and motivated consumers in

18. *See* Joan Feigenbaum et al., *Privacy Engineering for Digital Rights Management Systems*, 2320 LECTURE NOTES COMPUTER SCI., art. 6, 2002, *available at* http://cs-www.cs.yale.edu/homes/jf/FFSS.pdf.

19. *See* 1995 PETs REPORT, *supra* note 3.

20. These include overdependence on abstract models as opposed to "real-world" uses, insecure implementations, ease-of-use issues, and integration of PETs with legacy systems. *See* Feigenbaum et al., *supra* note 18, at 6–10; *see also* Ira Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 274–77 (2008) (discussing underutilization of anonymity tools due to apathy, consumer ignorance, and difficulty in finding, understanding, and configuring the relevant tools).

21. For an explicitly normative treatment of PETs, see, e.g., Roger Clarke, *Introducing PITs and PETs: Technologies Affecting Privacy*, 7 PRIVACY L. & POL'Y REP., no. 9, Feb. 2001, at 181, *available at* http://www.austlii.edu.au/au/journals/PLPR/2001/12.html (distinguishing PETs from so-called PITs (Privacy-Invasive Technologies), whose primary function is surveillance, and distinguishing "savage" PETs, which set out to deny identity and to provide untraceable anonymity, from "gentle" PETs, which include pseudonymity tools that balance the shielding of identity with accountability).

exercising greater control over what data they share and with whom they share it.

Although the Commission recommends the use of PETs, the Staff Report fails to discuss the different kinds and uses of PETs or their historical successes and failures. There is, in fact, a large literature on PETs including a number of proposed classifications. Most classifications of PETs take a functional approach (i.e., they distinguish PETs based on whether they ensure anonymity, confidentiality, transparency, and so on).[22] However, this is sometimes combined with other factors such as whether end-users deploy the PET on the client side or if firms deploy them on the server side. Other researchers classify PETs based on their underlying conception of privacy (e.g., control, autonomy, seclusion), but this has not proven very useful.[23]

This Article takes a different approach by classifying PETs in terms of how they relate to government regulation. The next Section suggests that *all* PETs fall into one of two very broad categories: substitute PETs (which take the place of privacy regulation by shielding identity and/or preventing the collection of personal data or personally identifiable information ("PII")) or complementary PETs (which support regulatory goals by using technical measures to achieve specific goals). The Article demonstrates that this categorization is far more likely to result in useful guidance to the private sector on their adoption of PETs.[24]

22. *See, e.g.*, COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 180–202 (2006); Lorrie Faith Cranor, *The Role of Privacy Enhancing Technologies*, *in* CONSIDERING CONSUMER PRIVACY: A RESOURCE FOR POLICYMAKERS AND PRACTITIONERS 80 (Paula J. Bruening ed., Mar. 2003), *available at* http://old.cdt.org/privacy/ccp/roleoftechnology1.pdf (full volume available at http://old.cdt.org/privacy/ccp/ccp.pdf); Ian Goldberg, *Privacy Enhancing Technologies for the Internet III: Ten Years Later*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 3 (A. Acquisti et al. eds., 2007); NAT'L RESEARCH COUNCIL, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 107–16 (2007).

23. *See, e.g.*, Herbert Burkert, *Privacy-Enhancing Technologies: Topology, Critique, Vision*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1998); L.J. Camp & C. Osorio, *Privacy-Enhancing Technologies for Internet Commerce*, *in* TRUST IN THE NETWORK ECONOMY (O. Petrovic et al. eds., 2003); Herman T. Tavani & James H. Moor, *Privacy Protection, Control of Information, and Privacy-Enhancing Technologies*, 31 COMPUTERS & SOC'Y 6 (2001).

24. For a similar distinction, see BENNETT & RAAB, *supra* note 22, at 153, 180 (noting that in Europe, PETs are often regarded as "a useful complement to existing regulatory and self-regulatory approaches" while in the United States they have sometimes been positioned as "an alternative to regulatory intervention").

B. A TAXONOMY OF PETS: SUBSTITUTES VS. COMPLEMENTS

Substitute PETs seek to protect privacy by blocking or minimizing the collection of personal data, thereby making legal protections superfluous. In contrast, complementary PETs permit the collection and use of such data as long as these activities are consistent with privacy laws and related statutory requirements.[25]

The main types of substitute PETs rely on anonymity to shield or reduce user identification and/or on client-centric architectures to prevent or minimize the collection of PII.[26] Their design is motivated by an underlying assumption that commercial IT systems are flawed, while legal rules and sanctions are in most (if not all) cases ineffective. These PETs shift the locus of protection from oversight of firm behavior to prevention or avoidance of the data collection and analysis requiring oversight in the first place. Most of the best known substitute PETs are discrete applications deployed by individual end-users to provide limited functionality (e.g., anonymous browsing or encrypted email).[27] Some substitute PETs also require ongoing maintenance, research, and support from non-profits and volunteers (e.g., the Tor anonymity network), but it is rare to see businesses deploy substitute PETs in their own products or services.

In practice, many substitute PETs are more theoretical than practical. Few are widely deployed,[28] for the reasons discussed above, and the firms that have sought to create a business around such tools have failed, which in turn discourages further investment.[29] This is hardly surprising. Profit-motivated internet firms collect and analyze personal data for multiple purposes—serving targeted ads, personalizing their services, and charging

25. Most U.S. privacy laws focus on the collection and use of PII, while EU privacy law turns on the related concept of personal data. Under both regimes, the collection and use of information other than PII or personal data is unregulated.

26. *See* S. Spiekermann & L. Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 67 (2009).

27. This is at least partly the result of the inhibitory effect of a regulatory environment driven by concerns over money laundering and other financial crimes, which have undermined government (and hence private-sector) support for anonymous payment systems and other forms of anonymity.

28. For a discussion of the most popular and useful substitute PETs, see Ethan Zuckerman, *How To Blog Anonymously*, *in* HANDBOOK FOR BLOGGERS AND CYBER-DISSIDENTS (Reporters Without Borders ed., 2005), *available at* http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf.

29. *See* Goldberg, *supra* note 22, at 12. Nevertheless, firms persist in trying to distinguish themselves on the basis of privacy. For recent examples of search engines that seek to maximize user privacy, see IXQUICK, http://www.ixquick.com (last visited Nov. 6, 2011); DUCKDUCKGO, http://www.duckduckgo.com (last visited Nov. 6, 2011).

prices that extract as much surplus as possible from any sale (which economists refer to as price discrimination).[30] As a result, they are reluctant to adopt substitute PETs voluntarily, which further erodes any market in such tools.

In sharp contrast, complementary PETs are designed to implement statutory privacy principles or related legal requirements. Thus, businesses are eager to deploy them both to ensure regulatory compliance and/or to give customers a positive impression of their commitment to privacy (here understood in terms of control over personal data). Developers of complementary PETs take it for granted that firms will collect data for various useful (and profitable) purposes. Their goal in developing complementary PETs is not to block or minimize such collection, but to reduce the risk of consumer harms by ensuring that data is collected and processed in compliance with regulatory requirements based on Fair Information Practice Principles ("FIPPs"). Complementary PETs can focus on the front-end user experience (e.g., informed consent mechanisms, access tools, and preference managers), or address privacy issues that arise with back-end infrastructure and data sharing networks (e.g., IBM's Tivoli Privacy Manager, which helps enterprises manage user identities, access rights, and privacy policies across an entire e-business infrastructure, and HP's proposed Policy Compliance Checking System).[31]

Complementary PETs fall into two subcategories: *privacy-friendly* and *privacy-preserving* PETs. Privacy-friendly PETs seek to give people more control over their personal data through improved notice and consent mechanisms, browser management tools, digital dashboards, and so on. In contrast, privacy-preserving PETs in many cases resemble substitute PETs. They rely on sophisticated cryptographic protocols that may lead to

30. *See* LONDON ECON., STUDY ON THE ECONOMIC BENEFITS OF PRIVACY-ENHANCING TECHNOLOGIES (PETS) 46–49 (2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf [hereinafter LONDON ECON. STUDY] (also noting the use of personal data as a "productive resource" and "tradable commodity"). Some economists argue that price discrimination is the principle motivation for businesses to collect personal data and that privacy erosion is driven to a large extent by the incentives to price discriminate. *See* Andrew Odlyzko, *Privacy, Economics, and Price Discrimination on the Internet*, *in* ICEC2003: PROCEEDINGS OF THE FIFTH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE (N. Sadeh ed., 2003), *available at* http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf.

31. On the front-end/back-end distinction, see LONDON ECON. STUDY, *supra* note 30, at 13 (noting that Yoram Hacohen, Head of the Information and Technology Authority of Israel, draws a similar distinction between "technologies that are used before any personal data is used ('pre-usage') and technologies that safeguard privacy while personal data is being processed"), and *infra* Section II.C.1.

deployable solutions with strong privacy guarantees but that also satisfy legal requirements. This combination of features permits companies and government agencies to engage in activities that might otherwise be viewed as privacy invasive while preserving privacy in a rigorous manner. Good examples include privacy-preserving data mining[32] and privacy-preserving targeted advertising.[33]

Why are these distinctions important?[34] The answer relates to the incentives for developing and using PETs. Bluntly, the market incentives for substitute PETs are feeble. On the other hand, a much stronger business case exists for complementary PETs because they both support existing compliance obligations and tend to enhance a firm's reputation as a trustworthy company that cares about privacy. Of course, businesses will adopt complementary PETs only if they determine that the direct and opportunity costs of doing so are low enough to justify the investment. Thus, firms are less likely to adopt privacy-preserving PETs because they are both harder to implement and less flexible than privacy-friendly PETs. These observations suggest that regulatory incentives may still be necessary to overcome the reluctance of private firms to increase their investments in PETs, especially in the face of limited consumer demand, competing business needs, and a weak economy.

The distinction between substitute and complementary PETs and the incentives for adopting them are well-illustrated by PETs designed to control the receipt of targeted advertising.[35] This Section concludes with brief

32. *See* Rakesh Agrawal & Ramakrishnan Srikant, *Privacy-Preserving Data Mining*, 29 SIGMOD REC. 439 (2000).

33. *See* VINCENT TOUBIANA ET AL., ADNOSTIC: PRIVACY PRESERVING TARGETED ADVERTISING (2010), *available at* http://crypto.stanford.edu/adnostic/adnostic.pdf.

34. For the sake of completeness, we may also distinguish a third category of PETs consisting in certain hybrid privacy solutions that may exhibit characteristics of privacy by design and utilize one or more kinds of PETs. Examples of such hybrid solutions may be found in Daniel J. Weitzner et al., *Information Accountability*, 51 COMM. ACM 82 (2008) (describing an accountability framework that combines strict legal rules on the permissible uses of data with a technical architecture that supports policy-aware transaction logs, a policy-language framework, and policy-reasoning tools); PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH. (PCAST), REALIZING THE FULL POTENTIAL OF HEALTH INFORMATION TECHNOLOGY TO IMPROVE HEALTHCARE FOR AMERICANS: THE PATH FORWARD 46 (2010), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-health-it-report.pdf (recommending a new health IT architecture that offers much stronger privacy and security protections than existing systems by using a universal exchange language and "tagged" data elements, i.e., each unit of data is accompanied by a mandatory "metadata tag" that describes the attributes, provenance, and required privacy and security protections of the data).

35. *See* FTC, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 9 n.21 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavad

descriptions of the PETs in targeted advertising sorted into the categories of PETs distinguished above:

> **1. Substitute PETs:** Various anonymity tools are available that prevent tracking and targeted advertising by enabling consumers to surf the web anonymously. For example, anonymous proxy servers permit users to surf the web without revealing their IP addresses. The Tor Browsing bundle offers similar functionality using a much stronger cryptographic protocol. Consistent with their business models, however, none of the major search or network advertising firms support the use of such tools in their web services, either by building in such functionality or educating users about where to find and how to use these PETs. It seems unlikely that the FTC could devise attractive enough incentives to overcome the opportunity costs associated with substitute PETs short of threatening highly restrictive regulations for those failing to adopt them.
>
> **2. Complementary Privacy-Friendly PETs:** On the other hand, many of the most popular commercial internet and network advertising firms strongly support tools that enable users to control their online advertising by editing their inferred interest and demographic categories or opting-out of behavioral targeting with respect to participating firms. Examples include ad preference managers, standalone and browser-based cookie managers, additional browser controls that allow users to delete cookies (including Flash cookies), "private browsing" features (which delete cookies each time the user closes the browser or turns off private browsing, effectively hiding his history), new icons that link to additional information and choices about behavioral advertising, and new, browser-based "do not track" tools from all three of the major browser vendors. These PETs are attractive to companies for obvious reasons: they enhance notice and choice in a privacy-friendly manner without disrupting the advertising business model.
>
> **3. Complementary Privacy-Preserving PETs:** Finally, a group of privacy researchers at Stanford and New York University recently developed a privacy-preserving approach to targeted advertising, which they call Adnostic.[36] This proposed system would allow ad networks to engage in behavioral profiling and ad targeting but without having a server track consumers. Rather, all of the tracking and profiling necessary for serving targeted ads takes place on the client side, i.e., in the user's own browser.

report.pdf (defining targeted advertising as "the collection of information about a consumer's online activities in order to deliver advertising targeted to the individual consumer's interests"); *see also* FTC STAFF REPORT, *supra* note 4, at 63–69 (discussing the "do not track" option).

36. TOUBIANA ET AL., *supra* note 33.

> When a site wants to serve an interest-based ad, the user's browser chooses the most relevant ad from a portfolio of ads offered by the ad network service but the browser doesn't reveal this information to the ad service or to any third-party. Adnostic is a promising technology because it offers much greater privacy protections than privacy-friendly PETs while preserving much of the advertising business model.[37] On the other hand, Adnostic imposes new costs and complexity on the online advertising industry and arguably undermines the ability of different ad services to compete based on which of them has the best ad matching algorithms. Adnostic has not found any takers as of this writing and seems unlikely to do so absent much stronger regulatory incentives.

These main characteristics of the three categories of PETs are summarized in Table 1:

Table 1: Main Characteristics of PETs

Type of PET	Purpose	Examples	Incentives To Adopt
Substitute PET	Prevent tracking and profiling	Anonymous proxy servers; Tor Browsing Bundle	Weak due to high opportunity costs
Complementary: Privacy-Friendly	User control of online advertising	Ad-preference and cookie managers; advertising icons; "do not track" tools	Strong: PETs enhance user controls with minimal disruption of advertising business model
Complementary: Privacy-Preserving	Allow tracking and profiling without revealing user's preferences to third parties	Adnostic	Weak: Even though it supports the business model, Adnostic adds complexity and shifts control from advertisers to users

C. ANALYZING PRIVACY BY DESIGN

Privacy by design is an amorphous concept. At the very least, it means implementing FIPPs in the design and operation of products and services that collect, or in any way process, personal data. One way of accomplishing this is by using existing PETs or creating new ones in response to emerging privacy concerns. Alternatively, privacy by design may refer to the adoption of processes, systems, procedures, and policies—any of which may also have

37. *See also* ANN CAVOUKIAN, REDESIGNING IP GEOLOCATION: *PRIVACY BY DESIGN* AND ONLINE TARGETED ADVERTISING (2010), *available at* http://www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf (discussing Bering Media's "doubleblind" privacy architecture).

a technological dimension—and which may be referred to collectively as privacy safeguards. EU privacy officials have long embraced PETs[38] but have begun to embrace a more expansive approach to privacy by design that emphasizes sound design practices as well.[39] In the United States, the FTC gives short shrift to PETs[40] and instead highlights a broad set of safeguards including certain design practices. The following discussion attempts to put some meat on these bones by analyzing the Staff Report in greater detail.

The Staff Report suggests that privacy by design consists of an integrated set of development and management processes and practices.[41] As with PETs, it is necessary to differentiate front-end software development activities from back-end data management practices. Front-end activities are a design process for customer-facing products and services (i.e., those with which customers interact by downloading software, using a web service, and/or sharing personal data or creating user content). Back-end practices consist of data management processes that ensure that information systems (for both internal use and for sharing data with affiliates, partners, and suppliers) comply with privacy laws, company policies (including published privacy policies), and customers' own privacy preferences. Although distinctive, the two lifecycles overlap in that most products and services designed for the Internet combine a front-end component with back-end data handling.[42]

The software development lifecycle seeks to ensure that in designing products and services, software developers take account of both customer privacy expectations and the relevant threat model that needs to be guarded against. This approach empowers users to control their personal data (for example, by improving their understanding of what information will be collected from them, how it will be used and what choices they have as to its

38. *See supra* note 3.

39. *See* EC, *A Digital Agenda for Europe*, *supra* note 1, at 17 n.21 (explaining that the principle of "privacy by design" means "that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal").

40. For example, the FTC staff report on consumer privacy discusses privacy-friendly choice mechanisms for online behavioral advertising (including "do not track") but otherwise barely mentions any substitution or privacy-preserving PETs. FTC STAFF REPORT, *supra* note 4.

41. *Id.* at 41.

42. Cavoukian avoids distinguishing front-end software development activities from back-end data management practices and instead takes a more holistic approach. *See* Cavoukian, *supra* note 1, at 4 (noting that "the PbD concept can be applied at many levels, from specific technologies, to organizational practices, extending to entire information ecosystems and architectures").

transfer, storage, and use). At the same time, it seeks to minimize the risks of privacy incidents (such as surreptitious or unanticipated data collection, unauthorized data use, transfer or exposure, and security breaches). The data management lifecycle, on the other hand, focuses more on how firms should engineer and manage information systems with privacy in mind as firm employees access, use, disclose, and eventually delete customer data.

This front-end/back-end distinction is generally consistent with the chief concerns discussed in subsections V(B)(1) and (2) of the Staff Report. The former advises companies on "incorporating substantive privacy protections into their practices,"[43] while the latter recommends that companies maintain "comprehensive data management procedures."[44] Yet there are notable shortcomings in the Commission's analysis. For instance, there is a lack of detail describing software design guidelines and data management practices. Overall, the Staff Report lacks the more robust discussion of best practices and other actionable steps that companies require to deploy privacy by design effectively. The next two Sections elaborate upon these concerns.

1. Privacy by Design in the Private Sector: Front-End and Back-End Approaches

Several of the older and more well-established multinational IT companies have developed guidelines, policies, tools, and systems for building privacy into software development and data management. For example, Microsoft's Security Development Lifecycle ("SDL") for software development is the best-known example of how privacy can be built into the design process.[45] The SDL aims to integrate privacy and security principles into each of the five stages of the software development lifecycle (requirements, design, implementation, verification, and release).[46] Privacy impact ratings are given to each project and these ratings determine the

43. FTC STAFF REPORT, *supra* note 4, at 44.

44. *Id.* at 49.

45. *See* Steve Lipner & Michael Howard, Microsoft Corp., *The Trustworthy Computing Security Development Lifecycle*, MDSN (Mar. 2005), http://msdn.microsoft.com/en-us/library/ms995349.aspx. Microsoft claims—with some independent support—that when compared to software that has not been subject to the SDL, software that has undergone SDL processes has a significantly reduced rate of external discovery of security vulnerabilities. *See SDL Helps Build More Secure Software*, MICROSOFT, http://www.microsoft.com/security/sdl/learn/measurable.aspx (last visited Nov. 6, 2011). The Department of Homeland Security's Software Assurance program adopts a similar approach, which it refers to as "Build Security In." *See* Nat'l Cyber Sec. Div., Dep't of Homeland Sec. (DHS), *Build Security in Home*, https://buildsecurityin.us-cert.gov/bsi/home.html (last visited Nov. 6, 2011).

46. *See* MICROSOFT CORP., SIMPLIFIED IMPLEMENTATION OF THE MICROSOFT SDL 3, http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=12379 (last updated Nov. 4, 2010).

design specifications needed for compliance.[47] The SDL guidelines are supplemented by Microsoft's "Privacy Guidelines for Developing Software and Services," a fifty-one-page document that lays out basic concepts and definitions based on FIPPs and related U.S. privacy laws; discusses different types of privacy controls and special considerations raised by shared computers, third parties, and other situations; and then enumerates nine specific software product and web site development scenarios.[48] For each scenario, the guidelines identify required and recommended practices relevant to notice and consent, security and data integrity, customer access, use of cookies, and additional controls or requirements.[49]

On the data management side, IBM's Tivoli Privacy Manager is a comprehensive enterprise privacy management system that supports a variety of privacy functionalities.[50] HP is also developing a comprehensive approach to managing the information lifecycle—storage, retrieval, usage, prioritization, update, transformation, and deletion—as well as identity management tasks such as the collection, storage, and processing of identity and profiling information, authentication and authorization, "provisioning" of digital identities (i.e., account registration and related tasks), and user management of personal data and identities. According to researchers in HP's Trusted Systems Lab, this requires both a model of privacy obligations (based on the rights of data subjects, any permission they have granted over the use of their personal data, and various statutory obligations associated

47. *Id.* at 10.

48. *See* MICROSOFT CORP., PRIVACY GUIDELINES FOR DEVELOPING SOFTWARE PRODUCTS AND SERVICES (ver. 3.1, Sept. 2008), http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&DisplayLang=en (describing nine scenarios at length). Although these guidelines mainly treat privacy design issues for front-end products and services, they also address back-end services such as "Server Deployment." This implies that "front-end" and "back-end" are not exclusive categories so much as primary areas of focus. One of the very few comparably detailed sets of privacy guidelines is the European Privacy Seal ("EuroPriSe") for IT products and services, which has developed a fifty-nine-page document with four sets of detailed criteria that firms must satisfy to demonstrate compliance with the EU Data Privacy Directive. *See* EUROPRISE, EUROPRISE CRITERIA (2010), *available at* https://www.european-privacy-seal.eu/criteria/EuroPriSe%20Criteria%20201011.pdf.

49. *See generally* MICROSOFT CORP., *supra* note 48.

50. *See* Paul Ashley & David Moore, *Enforcing Privacy Within an Enterprise Using IBM Tivoli Privacy Manager for E-business*, IBM DEVELOPERWORKS (2002), http://www.ibm.com/developerworks/tivoli/library/t-privacy/index.html (describing functions such as tracking different versions of privacy policies; storing consent of the individual to the privacy policy when PII data is collected; auditing of all submissions and accesses to PII; and authorization of submissions and accesses to PII).

with FIPPs) and a framework for managing these obligations.[51] The resulting "obligation management system" enables enterprises to configure information lifecycle and identity management solutions to deal with the preferences and constraints dictated by privacy obligations and ideally to do so in an automated and integrated fashion.[52]

Although product development and data management emphasize different aspects of privacy by design, the goal of both approaches is roughly the same: to build in privacy protections using a combination of technological and organizational measures that ensure compliance with applicable rules. Over the past decade, computer scientists have begun to develop formal methods for extracting descriptions of rules from the policies and regulations that govern stakeholder actions,[53] formal languages for representing such rules,[54] and methods for enforcing such rules via software systems that perform run-time monitoring and post hoc audits to ensure that disclosure and use of personal information respects these rules.[55] As Breaux and Anton note in a paper using the HIPAA Privacy Rule as a model: "Actions that are permitted by regulations are called rights, whereas actions that are required are called obligations. From stakeholder rights and obligations, we can infer system requirements that implement these rules to comply with regulations."[56] The idea of using formal languages to align

51. *See* MARCO CASASSA MONT, HP LABS., ON PRIVACY-AWARE INFORMATION LIFECYCLE MANAGEMENT IN ENTERPRISES: SETTING THE CONTEXT 5–8 (2006), http://www.hpl.hp.com/techreports/2006/HPL-2006-109.pdf.

52. *Id.* at 7.

53. *See* Travis D. Breaux & Annie I. Anton, *Analyzing Regulatory Rules for Privacy and Security Requirements*, 34 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 5 (2008).

54. *See* A. Barth et al., *Privacy and Contextual Integrity: Framework and Applications*, *in* PROCEEDINGS OF 2006 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 184 (2006), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1624011 (describing a language for representation of rules based on Helen Nissenbaum's theory of contextual integrity and showing how to represent a collection of rules from several federal statutes using this language).

55. *See* D. GARG ET AL., A LOGICAL METHOD FOR POLICY ENFORCEMENT OVER EVOLVING AUDIT LOGS (Carnegie Mellon Univ., Technical Report No. CMU-CyLab-11-002, rev. May 6, 2011), *available at* http://arxiv.org/PS_cache/arxiv/pdf/1102/1102.2521v3.pdf. One challenge in automated enforcement of rules that appear in privacy regulations is that they sometimes include subjective concepts (e.g., related to beliefs of individuals). Such policies cannot be automatically enforced in their entirety, but recent results demonstrate that software systems can in fact support a best-effort enforcement regime by checking all parts of the rules that do not contain subjective concepts and outputting the rest for inspection by human auditors. I am grateful to Anapum Datta for this reference.

56. Breaux & Anton, *supra* note 53 (explaining that the 55-page HIPAA Privacy Rule yielded 300 stakeholder access rules, which in turn were comprised of 1,894 constraints); *see also* TRAVIS D. BREAUX & DAVID G. GORDON, REGULATORY REQUIREMENTS AS OPEN

privacy requirements of software systems with legal regulations no doubt exceeds anything that the FTC has in mind when it recommends that companies incorporate substantive privacy protections into their practices. On the other hand, requirements engineering, formal languages, and related tools and techniques are precisely what software developers need in order to transform privacy by design from a vague admonition (that it is better to build in privacy than to bolt it on later) into a planned and structured design process.

2. Privacy by Design in the Staff Report and FTC Enforcement Actions

In comparison to these front-end and back-end commercial approaches, which are both rich in detail and very comprehensive, or to the emerging discipline of requirements engineering, the discussion of privacy development guidelines in Section V(B)(1) seems incomplete. To begin with, it considers only four substantive privacy protections that firms should incorporate into their practices (security, collection limits, retention practices, and accuracy) but fails to explain why all eight FIPPs are not applicable.[57] Certainly, two of these other principles—purpose specification and use limitation—are highly relevant to building privacy protections into products and services. An equally serious omission of this section (but not of later sections of the report) is the failure to discuss common use scenarios or the rules that should govern them, the severity of threat associated with each of them, and the safeguards needed to address these threats consistent with customer expectations and legal requirements.[58] In Section V(B)(2), the report's guidance consists of two recommendations. First, that firms implement CIPPs, and second, that they assess risks (in a manner akin to

SYSTEMS: STRUCTURES, PATTERNS AND METRICS FOR THE DESIGN OF FORMAL REQUIREMENTS SPECIFICATIONS (Carnegie Mellon Univ., Technical Report No. CMU-ISR-11-100, 2010), http://reports-archive.adm.cs.cmu.edu/anon/isr2011/CMU-ISR-11-100.pdf (describing a formal requirements specification language that allows developers to turn regulations into computational requirements that they can "design and debug" using formal structures, patterns, and metrics, and validating the approach using state data breach notification laws).

57. *See, e.g.*, Hugo Teufel III, Privacy Policy Guidance Memorandum, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, DEP'T HOMELAND SECURITY (Dec. 29, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (identifying eight principles including purpose specification and use limitation).

58. In fact, sections V(C) and (D) of the FTC staff report on consumer privacy examine a number of scenarios involving choice, notice, access, and material changes. FTC STAFF REPORT, *supra* note 4, at 58–77. Unfortunately, the report does not incorporate this analysis into the discussion of privacy by design.

Privacy Impact Assessments ("PIAs")) "where appropriate." But these insights are not sufficiently developed to provide much useful guidance.

For example, the report neglects to define when risk assessments are appropriate. This is surprising considering that section 208(b)(1)(A) of the E-Government Act of 2002[59] offers relevant guidelines, requiring federal agencies to perform a privacy assessment prior to developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.[60] Although the Staff Report offers a few illustrations of privacy reviews (notably in its discussion of peer-to-peer file sharing) and some prescriptive guidance, it does not go far enough in providing detailed rules or requirements for privacy assessments to help companies determine when to conduct them or whether they have done so in a meaningful way. Of course, PIAs are the most widely used tool for privacy risk assessments, especially in the public sector.[61] Interestingly, the privacy Green Paper recently published by the Department of Commerce ("DOC") also encourages firms to use PIAs to enhance transparency, increase consumer awareness, and identify alternative approaches that would help to reduce relevant privacy risks.[62] But the Staff

59. Pub. L. No. 107-347, § 208(b)(1)(A), 116 Stat. 2899, 2921–22 (2002) (codified at 44 U.S.C. § 3501 (2006)).

60. *See* Joshua B. Bolten, *M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OFF. MGMT. & BUDGET (Sept. 26, 2003), http://www.whitehouse.gov/omb/memoranda_m03-22 (further specifying when PIAs are required).

61. *See* Roger Clarke, *Privacy Impact Assessment: Its Origins and Development*, 25 COMP. L. & SECURITY 123, 129 (2009). Clarke defines a PIA as "a systemic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts." *See* Roger Clarke, *An Evaluation of Privacy Impact Assessment Guidance Documents*, 1 INT'L DATA PRIVACY L., no. 2, at 111 (2011), *available at* http://idpl.oxfordjournals.org/content/1/2/111.full.pdf. Clarke criticizes the Section 208 PIA process as mainly "checklist-based and almost entirely devoid of any content of significance to privacy protection, beyond the narrowly circumscribed legal requirements." *Id.* at 117.

62. INTERNET POL'Y TASK FORCE (IPTF), U.S. DEP'T OF COMMERCE (DOC), COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 34–36 (2010), *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf [hereinafter DOC GREEN PAPER]. The discussion cites a recent EC recommendation encouraging the RFID industry and relevant stakeholders to develop a framework to assess the privacy risks of using RFID applications, subject to endorsement by the Article 29 Working Party. *See Industry Proposal: Privacy and Data Protection Impact Assessment Framework for RFID Applications*, EUROPE'S INFO. SOC'Y (2010) (draft), *available at* http://ec.europa.eu/information_society/policy/rfid/documents/d31031industrypia.pdf. This 25-page proposed framework would require RFID operators to report the types of data that RFID tags and applications collect and process, including any personal or sensitive data; whether this information gives rise to particular privacy risks, such as tracking

Report discussion of privacy assessments is too brief to infer whether it concurs with the DOC's reasoning or would embrace the European model in which industry-wide PIAs must be reviewed and approved by privacy officials.

In sum, the Staff Report is best read as a first cut at agency guidance regarding privacy by design, with Sections V(B)(1) and (2) offering preliminary guidelines on how firms might integrate privacy safeguards into their development and data management practices. Other sources of guidance in the Staff Report include the discussion of "commonly accepted practices" in providing notice and choice[63] and how to increase transparency in data practices,[64] both of which suggest recommended practices in privacy by design.

Also instructive are some half-dozen "spyware" and "adware" enforcement actions suggesting prohibited design practices or required disclosure practices. In the prohibited category, the FTC has brought several cases involving the alleged practices of (1) installing software without a user's consent by exploiting security vulnerabilities; (2) bundling software with malware; and (3) installing root kit software. In the required category, several additional cases concern allegations of failing to clearly and conspicuously disclose (4) the bundling of free software with malware; (5) all the features of a program (such as content protection or "phone home" features); (6) the types of data that certain tracking software will monitor, record, or transmit; and (7) the means by which consumers may uninstall any adware or similar programs that monitor internet use and display frequent, targeted pop-up ads. These enforcement cases help flesh out the discussion in the Staff Report and constitute a down payment on privacy design guidelines in the form of prohibited, required, and recommended practices.[65]

---

an individual's movements; and to address the privacy and security features designed to minimize these risks, and whether the applications are ready for deployment (i.e., provide for suitable controls, practices, and accountability) or if a corrective action plan needs to be developed followed by a new PIA. Industry won the endorsement of the Working Party after revising its proposed framework in response to criticism. *See* Art. 29 Data Protection Working Party, 00327/11/EN, WP 180, *Opinion 9/2011 on the Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications* 3–4 (Feb. 11, 2011), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf.

63. *See* FTC STAFF REPORT, *supra* note 4, at 53–65.

64. *Id.* at 69–77.

65. The Appendix, *infra*, identifies the relevant cases and additional discussion in the FTC Staff Report and organizes them into a list of prohibited, required, or recommended privacy design practices.

Admittedly, none of this adds up to a complete version of what the FTC means by privacy by design, or—to use the broader notion—by CIPPs. But the Commission provides two hints of what future enforcement actions may bring. The first hint is discernible in the FTC's letter to Google closing the Street View investigation.[66] Despite its stated concerns regarding the adequacy of Google's internal review processes, the Commission chose to end this inquiry based on assurances that (1) Google neither had nor would use the Wi-Fi payload data and intended to delete it, and (2) that it would adopt certain practices "including appointing a director of privacy for engineering and product management; adding core privacy training for key employees; and incorporating a formal privacy review process into the design phases of new initiatives."[67] In addition, the Commission recommended that Google "develop and implement reasonable procedures" such as "collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored."[68] This closing letter clearly anticipates several themes in the Staff Report discussion of privacy by design. The second hint consists in the obvious similarities between CIPPs, as described in the Staff Report, and comprehensive information security programs ("CISPs"), as defined in the Safeguards Rule[69] and numerous FTC enforcement actions.[70] A recent consent agreement resolving allegations that Google engaged in deceptive trade practices when it launched its "Buzz" social networking service confirms that the Commission modeled CIPPs on CISPs, both as to their overall conception and specific elements.[71]

66. *See* Letter from David C. Vladeck, Director, Bureau of Consumer Protection, to Albert Gidari, Esq., Counsel for Google (Oct. 27, 2010), *available at* http://www.ftc.gov/os/closings/101027googleletter.pdf (closing Google inquiry). The Google Street View service displays panoramic images of many cities taken from cars equipped with specially adapted digital cameras and antennas. In April 2010, Google revealed that these cars had been inadvertently collecting data from Wi-Fi networks. *See* Kevin J. O'Brien, *New Questions over Google's Street View in Germany*, N.Y. TIMES, Apr. 29, 2010.

67. Letter from David C. Vladeck to Albert Gidari, *supra* note 66.

68. *Id.*

69. The Safeguards Rule, 16 C.F.R. pt. 314 (2010), implements the security and confidentiality requirements of the Gramm-Leach-Bliley Act ("GLBA"), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6809 (2006)).

70. For a list of relevant cases, see FTC STAFF REPORT, *supra* note 4, at 10–11. For a recent example of an enforcement action defining a CISP, see Agreement Containing Consent Order, *In re* Twitter, Inc., File No. 0923093 (Fed. Trade Comm'n (FTC) June 24, 2010), *available at* http://www.ftc.gov/os/caselist/0923093/100624twitteragree.pdf.

71. *See* Agreement Containing Consent Order, *In re* Google, File. No. 102 3136 (FTC Mar. 30, 2011), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzz

Although both CISPs and CIPPs incorporate a mix of personnel and accountability measures, risk assessments (including consideration of product design), design and implementation processes, and ongoing evaluations, there are important respects in which the two programs differ. For example, privacy risk assessments are still in their infancy and have far fewer technical resources to draw upon than security risk assessments, which often take the form of threat modeling and rely on highly developed and well-established secure coding practices and testing tools.[72] Similarly, the FTC consent orders establishing CISPs and CIPPs require companies to submit periodic assessments from qualified professionals certifying that their programs operate effectively based on generally accepted procedures and standards. While in the security world such benchmarks exist, in the privacy world they do not, although this is changing.[73] Lastly, it is worth noting that while the

agreeorder.pdf. FTC consent orders resulting from data security incidents usually require the violating company to implement a comprehensive, written CISP that is (1) reasonably designed to protect the security, privacy, confidentiality, and integrity of personal information; and (2) contains administrative, technical, and physical safeguards appropriate to a company's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information. *See In re Twitter*, Consent Order, *supra* note 70, at 3. Similarly, the Google consent order requires the company to implement a comprehensive, written CIPP that is (1) reasonably designed to address privacy risks and protect the privacy and confidentiality of personal information; and (2) contain privacy controls and procedures appropriate to the company's size and complexity. *See In re Google*, Consent Order, *supra*, at 4–6. Additionally, the five major constituents of each type of program are all but identical. The first element in both programs is "the designation of a responsible employee to coordinate and be accountable for" the program. The second element in both, "the identification of reasonably foreseeable, material risks," is similarly structured although each focuses on somewhat different dangers and requires assessments of different factors. The third element, the design and implementation of reasonable "safeguards" (CISPs) or "privacy controls and procedures" (CIPPs), and the "regular testing or monitoring of the effectiveness" of such safeguards or controls, is also the same in both. The fourth element in both programs calls for reasonable care in selecting and retaining service providers. The fifth element in both uses nearly identical language to require "the evaluation and adjustment" of the relevant program based on the results of the required "testing and monitoring . . . , any material changes to respondent's operations or business arrangements, or any other" relevant circumstances. *See In re Twitter*, Consent Order, *supra* note 70; *In re Google*, Consent Order, *supra*.

72. For a description of relevant tools and techniques, see generally MARK GRAFF & KENNETH VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES (2003); MICHAEL HOWARD & DAVID LEBLANC, WRITING SECURE CODE (2003); GARY MCGRAW, SOFTWARE SECURITY: BUILDING SECURITY IN (2006).

73. ISO/IEC 27002 is a widely acknowledged and well-established, certifiable information security standard published by the International Organization for Standardization ("ISO"). Although Subcommittee 27 ("SC 27"), IT Security Techniques, of the ISO's Joint Technical Committee 1 is working on several projects, including a "Privacy Framework," "Privacy Reference Architecture," and "Proposal on a Privacy Capability Assessment Model," international privacy standards remain at a very preliminary stage. *See IT*

Staff Report's discussion of CIPPs largely anticipates the obligations set forth in the Google settlement, the report endorses "privacy by design" while the consent decree avoids this language entirely, even though several of the prescribed elements of CIPPs include design aspects. It remains to be seen whether this omission is deliberate or signals a shift in how the FTC refers to and/or conceives of these requirements.

III. MARKET INCENTIVES

This Part addresses the question of whether the privacy market provides sufficient incentives for firms to invest in the elements of CIPPs (including privacy design and technology aspects) at a socially optimal level or if government intervention is needed to ensure appropriate investment. Many of the privacy regulators who endorse privacy by design seem confident that businesses will recognize the advantages of such investments and act accordingly. Thus, the U.K. Information Commissioner's Office ("ICO") insists that privacy by design will yield a "privacy dividend"[74] echoing Ann Cavoukian's earlier claim of a "privacy payoff" for firms that respect privacy and earn customer trust,[75] and her more recent assertion that "Full Functionality—*Positive-Sum*, not Zero-Sum" is a foundational principle of what she refers to as PbD.[76] But there are reasons to question their optimism.

To begin with, the orthodox economic view predicts that under perfect information, market forces will produce an efficient level of data collection and analysis. As a corollary, rational firms will invest in CIPPs in response to consumer demand for protection against the risks associated with data collection, unauthorized secondary use, processing errors, and improper access.[77] However, this view assumes that consumers understand how to recognize and protect themselves against both tangible harms, such as

Security Techniques, INT'L ORG. FOR STANDARDIZATION, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&development=on (last visited Nov. 6, 2011).

74. *See* U.K. INFO. COMM'R'S OFFICE, THE PRIVACY DIVIDEND: THE BUSINESS CASE FOR INVESTING IN PROACTIVE PRIVACY PROTECTION 3 (2010).

75. *See* ANN CAVOUKIAN & TYLER J. HAMILTON, THE PRIVACY PAYOFF: HOW SUCCESSFUL BUSINESSES BUILD CUSTOMER TRUST 36 (2002).

76. *See* Ann Cavoukian, Info. & Privacy Comm'r (Ontario, Canada), *Privacy by Design: The 7 Foundation Principles* 2 (revised Jan. 2011) (2009), *available at* http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf. ("*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner . . . .").

77. *See* H. Jeff Smith & Sandra J. Milberg, *Information Privacy: Measuring Individuals' Concerns About Organizational Practices,* 20 MIS Q. 167 (1996) (identifying these four specific privacy dimensions, which represent the cognitive state of consumers towards corporate use of information).

identity theft or price discrimination, and intangible harms, which are harder to define in economic terms since they involve what Daniel Solove refers to as "digital dossiers" and the sense of "unease, vulnerability, and powerlessness" associated with them.[78] In fact, few consumers understand these risks and even fewer are familiar with PETs (or take the trouble to use them) or can easily identify firms with sound privacy programs.[79] Moreover, the weight of scholarly opinion suggests that this lack of awareness reflects information asymmetries and that this and related market failures are difficult to correct absent regulatory intervention.[80]

Second, firms contemplating how much to invest in privacy programs run up against several problems. In theory, establishing a CIPP, designing privacy into products and services, and/or deploying PETs should lower the risk of misuse or abuse of personal data, thereby reducing the probability and costs of any privacy breaches. Using a cost-benefit approach, firms would decide how much to invest by estimating and comparing the anticipated value of the benefits of avoiding such losses against the expected costs of privacy (and related security) safeguards. But the necessary data for these estimates is lacking and without it many firms instead lapse into a reactive mode, delaying needed investments until a privacy incident occurs or government regulation forces their hand.[81] Moreover, because firms profit from targeted advertising, personalization, and price discrimination, they are strongly motivated to collect and analyze as much customer data as possible with the fewest possible restrictions. Thus, certain PETs or privacy design decisions may impose opportunity costs that firms are reluctant to pay. Third, other reasons to make such investments—such as avoiding damage to

78. DANIEL J. SOLOVE, THE DIGITAL PERSON 149 (2004). More generally, Solove argues that privacy encompasses a range of problems that can create many different types of individual and societal harms, including financial losses, reputational harms, emotional and psychological harms, and relationship harms, to name a few. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 174–79 (2008). *See also* Ryan Calo, The Boundaries of Privacy Harm (July 2010) (unpublished manuscript), *available at* http://works.bepress.com/m_ryan_calo/2 (arguing that privacy harms fall into two overarching categories: subjective harm (the unwanted perceptions of observation by others resulting in mental states such as anxiety, embarrassment, or fear) and objective harm (the "unanticipated or coerced use of information concerning a person against that person" such as "identity theft, the leaking of classified information that reveals an undercover agent, and the use of a drunk-driving suspect's blood as evidence against him")).

79. *See* LONDON ECON. STUDY, *supra* note 30, at 32–45.

80. *See, e.g.*, SOLOVE, THE DIGITAL PERSON, *supra* note 78, at 76–92; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1265–68 (1998); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076–84 (2004).

81. *See infra* Section III.C.

reputation and associated lost sales or customers—are not as compelling as they might seem.

As expected, industry defends its current practices quite vigorously, arguing that targeted ads provide consumers with useful information and underwrite free web content and services, and that advertisers use such information "anonymously."[82] Privacy advocates, on the other hand, strongly object to this rationale, calling attention instead to the potential harms associated with industry practices (such as the costs to consumers of price discrimination) and the advent of a dossier society.[83] In what follows, the goal is not to resolve these longstanding disputes or decide whether consumers would be better off if online advertisers were not only self-regulated but regulated by new privacy laws. Rather, the goal is to examine privacy investments in economic terms and decide if the market is or is not working.

A. WHY IS THERE WEAK DEMAND FOR CONSUMER PETS?

There is very little market data on the consumer demand for PETs, in part because they are not tracked as a separate product category. Anecdotal evidence exists regarding both substitute PETs and privacy-friendly PETs, and while inconclusive, it suggests that most PETs reach fewer than a million users.[84] The recent FTC Staff Report provided similar statistics on downloads or usage of popular ad-blocking tools.[85]

Are these numbers indicative of growing consumer demand for privacy tools to which companies should rationally respond by offering more PETs

82. *See* THOMAS M. LENARD & PAUL H. RUBIN, IN DEFENSE OF DATA: INFORMATION AND THE COSTS OF PRIVACY 2–3 (2009), *available at* http://www.techpolicyinstitute.org/files/in%20defense%20of%20data.pdf.

83. *See* Press Release, Ctr. for Digital Democracy (CDD), CDD and U.S. PIRG Call on FTC To Develop Stronger Online Privacy Framework (Feb. 18, 2011), http://www.democraticmedia.org/cdd-and-us-pirg-call-ftc-develop-stronger-online-privacy-framework.

84. *See* John Alan Farmer, *The Specter of Crypto-anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725, 754 (2003) (noting that an anonymity-protecting, peer-to-peer network had been downloaded over 1.2 million times since its launch in 1999); Steven Cherry, *Virtually Private*, IEEE SPECTRUM ONLINE (Dec. 1, 2006), *available at* http://spectrum.ieee.org/dec06/4744 (noting that an anonymous remailer had about 700,000 users in 1996); Kim Zetter, *Rogue Nodes Turn Tor Anonymizer into Eavesdropper's Paradise*, WIRED (Sep. 10, 2007), http://www.wired.com/politics/security/news/2007/09/embassy_hacks?currentPage=all (noting that "Tor has hundreds of thousands of users around the world").

85. *See* FTC STAFF REPORT, *supra* note 4, at 28. Mozilla.org estimates that AdBlock Plus has over 12 million "active daily users," which is much higher than anything in the FTC report. *See AdBlock Plus Statistics*, MOZILLA, https://addons.mozilla.org/en-US/statistics/addon/1865 (last visited Nov. 6, 2011).

or—alternatively—by building in privacy? Clearly, they are very small compared, for example, to popular anti-virus and related security products, which claim to have as many as 133 million users,[86] and miniscule compared to the nearly two billion worldwide Internet users.[87] The only contradictory data comes from a privacy official at Facebook, who recently indicated that almost thirty-five percent of the company's 350 million users customized their privacy settings when Facebook released new privacy controls in December of 2009.[88] This data may reflect user dissatisfaction with unpopular changes in Facebook's privacy controls; if not, it is an interesting development requiring further examination.

The most common explanation for the (apparently) weak demand for PETs is that due to information asymmetries, most individuals do not understand the risks to which they are exposed through sharing personal data.[89] Other commentators have noted the existence of a "privacy paradox" in that consumers both routinely state that they value their privacy highly yet behave as if their personal data has very little value.[90] Well-known examples of such behavior include consumers giving away personal data in exchange

86. *Internet Usage Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm. (last visited Nov. 6, 2011).

87. *Internet Usage in Europe*, INTERNET WORLD STATS, http://www.internetworldstats.com/stats4.htm. (last visited Nov. 6, 2011).

88. *See* FTC STAFF REPORT, *supra* note 4, at 28 n.68. For evidence that users will adjust their sharing behavior on social networks when user interfaces are augmented with visual or numerical displays of the size of the audience, see Kelly Caine et al., *Audience Visualization Influences Disclosures in Online Social Networks*, *in* PROCEEDINGS OF THE 2011 ANNUAL CONFERENCE EXTENDED ABSTRACTS ON HUMAN FACTORS IN COMPUTING SYSTEMS (ACM ed., 2011), *available at* http://dl.acm.org/citation.cfm?id=1979825&bnc=1.

89. *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES 363, 366–68 (Alessandro Acquisti et al. eds., 2007); *id.* at 364 ("Data subjects often know less than data holders about the magnitude of data collection and use of (un)willingly or (un)knowingly shared or collected personal data; they also know little about associated consequences.").

90. *See, e.g.*, Luc Wathieu & Allan Friedman, *An Empirical Approach to Understanding Privacy Valuation* (Harvard Bus. Sch., Working Paper No. 07-075, 2007), *available at* http://www.hbs.edu/research/pdf/07-075.pdf. In *U.S. West, Inc. v. Federal Communications Commission*, 182 F.3d 1224, 1234 (10th Cir. 1999), the court struck down on First Amendment grounds FCC regulations requiring customer opt-in approval prior to a telecommunications firm using their information for marketing purposes. In concluding that the FCC had failed to establish the protection of customer privacy as a "substantial interest," the court observed that it was insufficient to merely speculate that there are a substantial number of individuals who feel strongly about their privacy while at the same time assuming that they would not bother to opt-out even if given the chance. *Cf.* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 29–36 (2005) (arguing that a cost-benefit approach to valuing privacy inevitably favors the side seeking more data collection and sharing).

for loyalty cards, discounts, and other conveniences such as access to free content and services.[91] Privacy expert Alan Westin cites variable privacy sensitivities.[92] More recently, behavioral economists have developed explanations based on bounded rationality[93] and behavioral biases such as immediate gratification or optimism bias.[94]

Perhaps the most intuitively satisfying explanation of why people seem unwilling to look after their own privacy needs—whether through self-help or by demanding better privacy tools—comes from computer researchers Adam Shostack and Paul Syverson. They suggest that when people know they have a privacy problem (such as being on display to neighbors), they will pay for effective and understandable solutions (curtains and fences). But new situations like the Internet are harder to understand, a point they illustrate by reference to cookies:

> It is not trivial to understand what an http cookie is, as this requires some understanding of the idea of a protocol, a server, and statefulness. Understanding the interaction of cookies with traceability and linkability is even more complicated, as it requires understanding of web page construction, cookie regeneration, and non-cookie tracking mechanisms.[95]

---

91. *See* Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFO. SYS. RES. 254, 255–56 (2011) (citing several relevant studies).

92. *See Opinion Surveys: What Consumers Have To Say About Information Privacy: Hearing Before the House Commerce Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 107th Cong. 15–16 (2001) (testimony of Alan K. Westin, Professor, Public Law & Gov't Entities, Columbia Univ.; President, Privacy and Am. Bus.) (describing overall consumer privacy preferences as divided into three basic segments: *Privacy Fundamentalists* (25%), who reject offers of benefits, want only opt-in, and seek legislative privacy rules; *Privacy Unconcerned* (now down to 12% from 20% three years ago), who are comfortable giving their information for almost any consumer value; and . . . *Privacy Pragmatists* (63% or 125 million strong) [who] ask what the benefit is to them, what privacy risks arise, what protections are offered, and whether they trust the company or industry to apply those safeguards and to respect their individual choice").

93. *See* Acquisti & Grossklags, *supra* note 89, at 369–70 (noting that humans have limited ability to "process and act optimally on large amounts of data" and instead rely on simplified mental models).

94. *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 21, 22 (ACM ed., 2004) (highlighting "various forms of psychological inconsistencies (self-control problems, hyperbolic discounting, present-biases, etc.) that clash with the fully rational view of the economic agent").

95. Adam Shostack & Paul Syverson, *What Price Privacy? (and Why Identity Theft Is About Neither Identity Nor Theft)*, *in* ECONOMICS OF INFORMATION SECURITY 7 (L. Jean Camp & Stephen Lewis eds., 2004).

Unfortunately, it is all too easy to extend this analysis of the threat of cookies to other technologies consumers encounter in their everyday use of the Internet. In many cases, consumers lack awareness of tracking technologies or do not understand how the technology works when, for example, they visit a website that hosts "beacons" (invisible pixels that allow advertisers to track users as they surf the web), register for an online account, click on a banner ad, install a toolbar, use an ad-funded photo storage service, or use a mobile phone to locate a nearby store.[96] When they blog or share ideas, photos, or videos about themselves or their friends and relatives on a social network, they may have a better understanding about what they are doing while failing to fully appreciate the privacy implications of their actions. All of these cases require more insight and foresight about internet technology than most consumers have. Nor are there any "consumer reports" for privacy products and services that might assist them in evaluating the worth of a product or service.[97] This lack of an effective signaling mechanism to indicate "good" privacy practices has led one group of economists to conclude that online privacy suffers from adverse selection.[98]

B. WHY ARE FIRMS RELUCTANT TO INVEST IN PRIVACY BY DESIGN?

In deciding whether to invest in privacy by design, firms engage in a complex cost-benefit trade-off involving the direct, indirect, and opportunity costs of such investments; the effectiveness of various technologies and other privacy safeguards in reducing risks and associated losses; the demand for such technologies and safeguards; the competitive advantage gained by deploying them; and the opportunity costs associated with any technologies that may limit or prevent processing of personal data. The previous Section suggested that consumer demand is weak. This Section explores how firms go about budgeting for privacy expenditures in the face of weak consumer demand. An important caveat applies to this line of inquiry: most of the

96. For a discussion of the privacy (and security) implications of most of these activities, see GREG CONTI, GOOGLING SECURITY: HOW MUCH DOES GOOGLE KNOW ABOUT YOU? (2008).

97. Privacy seal programs seek to fill this role but have done so with only limited success.

98. *See* Tony Vila et al., *Why We Can't Be Bothered To Read Privacy Policies: Models of Privacy Economics as a Lemons Market*, *in* PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE 403, 404–05 (ACM ed., 2003), *available at* http://dl.acm.org/citation.cfm?id=948057 (suggesting this lemons market might be fixed by privacy signals that differentiate "good" sites and concluding that an efficient and reliable marketplace requires either privacy regulation or governments assuming the cost of testing signals; another possible solution is price discrimination).

relevant analysis and data originates in the literature on information security investments. This is unavoidable given the scarcity of reliable data on the costs of privacy.[99] For the sake of analysis, however, we will assume that firms approach both investments in roughly the same manner.[100]

This Section also examines a factor largely neglected when regulators make the business case for privacy by design—namely, the reasons that regulators think that businesses will benefit from adopting this approach. The missing factor is the opportunity costs businesses would incur if privacy design practices limit the scope of commercial exploitation of personal data.[101]

Economists who have analyzed how much firms should invest in information security generally agree on three points. The first is that cost-benefit analysis is a sound basis for decision making. Under this approach, firms must estimate both the costs and expected benefits of security activities, which in turn requires estimates of the potential losses from security breaches[102] and the probability of such breaches occurring. The second is that firms are more likely to utilize cost-benefit analysis if there is reliable data to inform the analysis. Here, however, that data on potential losses and their probability is hard to come by. The third is that in the absence of such data, many firms rely on alternatives to cost-benefit approaches such as incremental budget adjustments (i.e., adjusting the prior year's budget up or down based on possibly extraneous factors) or a more reactive approach (i.e., increasing investments in response to a breach event that makes security a must-do project).[103]

---

99. *See* LONDON ECON. STUDY, *supra* note 30, at 59.

100. This assumption may be justified given that at large corporations, chief privacy officers ("CPOs") and chief security officers ("CSOs") work closely and cooperatively and frequently sit in the same organization, or have similar reporting structures. Moreover, surveys of CPOs and CSOs suggest that in many cases, security issues may drive a CPO's objectives, while privacy issues may drive a CSO's. *See generally* ERNST & YOUNG, ACHIEVING SUCCESS IN A GLOBALIZED WORLD: IS YOUR WAY SECURE? (2006); IAPP/PONEMON, BENCHMARK PRIVACY: AN EXECUTIVE SUMMARY STUDY (2010). On the other hand, if weak security has clear economic costs and inadequate privacy does not, then perhaps firms will approach the relevant investment decisions in a different manner.

101. *But see* LONDON ECON. STUDY, *supra* note 30 (taking into account this factor).

102. These losses include direct losses, such as fraud, identity theft or interference with intellectual property rights; consequential losses, such as fines, penalties, and investigatory and remedial costs; and reputational damage, which may result in lost customers, sales, or profits.

103. *See, e.g.*, Lawrence Gordon & Martin Loeb, *Budgeting Process for Information Security Expenditures*, 49 COMM. ACM 121 (2006); Brent R. Rowe & Michael P. Gallaher, Private Sector Cyber Security Investment Strategies: An Empirical Analysis (Mar. 2006) (unpublished manuscript), *available at* http://weis2006.econinfosec.org/docs/18.pdf.

Assume for the sake of argument that these observations apply to privacy investment decisions as well. As noted, there is almost no data on the "benefits of privacy," i.e., any reliable estimates of the potential loss from a privacy incident or the probability that such incidents would occur. As for data on the "costs of privacy," the two available studies report very different results: the first suggests that large organizations spend from $500,000 to $22 million annually on overall privacy investments and that spending on privacy technology accounts for less than ten percent of the total budget (as compared to twenty-three percent and twenty-four percent devoted to a privacy office (staff and related overhead) and training programs, respectively).[104] The second study pegs this range at $500,000 to $2.5 million per year.[105] It is not clear if these figures are high or low when compared with the average security expenditures of a Fortune 500 firm.[106]

In the absence of data that would enable firms to use a cost-benefit approach in evaluating privacy investments, firms may decide not to invest in privacy by design due to opportunity costs, i.e., the costs attributed to technologies or other safeguards that may interfere with their current methods of collecting and analyzing customer data including such common practices as profiling and targeting. Indeed, opportunity costs might be thought of as the uninvited guests at the privacy by design pep rally. Standard economic doctrine teaches that firms will only care about privacy if that helps them increase their profits by attracting new customers.[107] There is some

104. *See* IBM & PONEMON INST., THE COSTS OF PRIVACY STUDY 13–14 (2004) (studying 44 large corporations, mostly Fortune 500 companies with between 5,000 and 75,000 employees).

105. *Cf.* IAPP/PONEMON, supra note 100 (finding that more than 70% of companies with over $10 billion in revenue reported privacy budgets between $500,000 and $2.5 million).

106. According to a recent survey that included data on total estimated information security budgets (including the cost of hardware, software, IT salaries, and consultants), 23% of respondents spent less than $100,000; 18% spent $100,000–$500,000; 18% spent $500,000–$2,000,000; and 10% spent $2,000,000–$10,000,000 (and the rest didn't know). *See* INFORMATIONWEEK, 2011 STRATEGIC SECURITY SURVEY: CEOS TAKE NOTICE 51 (2011), *available at* http://analytics.informationweek.com/abstract/21/6854/Security/research-2011-strategic-security-survey.html. Unfortunately, this data is not comparable to the privacy studies noted above because it is based on the responses of 1,084 business technology and security professionals at companies with more than 100 employees and does not segregate its findings by company size.

107. *See* LONDON ECON. STUDY, *supra* note 30, at 32–45; R. Böhme & S. Koble, On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market: Will Privacy Remain a Luxury Good? (2007) (unpublished manuscript), *available at* http://www.inf.tu-dresden.de/~rb21/publications/BK2007_PET_Viability_WEIS.pdf; Joan Feigenbaum et al., Economic Barriers to the Deployment of Existing Privacy Technologies 2

experimental evidence of consumers' willingness to pay a privacy premium to online merchants with superior privacy practices even though they offer goods at higher prices.[108] Economists, including Alessandro Acquisti, have also speculated on whether privacy-enhanced identity management systems ("IDMs") may be used to enable consumers to interact pseudonymously with merchants while nevertheless allowing businesses to collect, analyze, and profitably exploit de-identified or aggregate data.[109] These are intriguing ideas, but Acquisti offers no evidence of commercial adoption despite the fact that the relevant technology has been available for many years.[110]

On the other hand, firms profit from collecting and analyzing customer data and are more likely than not to reject any privacy safeguards that would deprive them of this highly valuable information.[111] This data collection and analysis for online advertising purposes is big business.[112] According to

(2003) (unpublished manuscript), *available at* http://www.homeport.org/~adam/econbar-wes02.pdf.

108. *See* Serge Egelman et al., Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators 1 (2009) (unpublished manuscript), *available at* http://www.guanotronic.com/~serge/papers/chi09a.pdf (follow-up study demonstrating that consumers are willing to pay more for a higher level of privacy when privacy indicators are presented alongside of search results); Tsai et al., *supra* note 91, at 255 (lab study demonstrating that consumers are willing to pay more to shop at websites that have better privacy policies).

109. *See* Alessandro Acquisti, *Privacy and Security of Personal Information: Economic Incentives and Technological Solutions*, *in* ECONOMICS OF INFORMATION SECURITY, *supra* note 95, at 7; Alessandro Acquisti, *Identity Management, Privacy, and Price Discrimination*, 6 IEEE SECURITY & PRIVACY 18 (2008); Böhme & Koble, *supra* note 107.

110. *See* Jan Camenisch et al., Position Paper, Credential-Based Access Control Extensions to XACML 4 (W3C Workshop on Access Control Application Scenarios, 2009), *available at* http://www.w3.org/2009/policy-ws/papers/Neven.pdf.

111. *See* Catherine E. Tucker, *The Economics Value of Online Customer Data* (WPISP & WPIE, Background Paper #1, Dec. 1, 2010), *available at* http://www.oecd.org/dataoecd/8/53/46968839.pdf (noting that online merchants and ad-funded Web businesses benefit from creating customer profiles based on clickstream data, cookies and Web bugs that track activities across the Web, demographic and behavioral data collected by specialized firms, data harvested from user-generated content on social networking and other Web 2.0 sites, and even more intrusive methods such as deep packet inspection).

112. *See id.* § 3.2.1 (citing a report by the Internet Advertising Bureau ("IAB") estimating that U.S. online advertising spending in 2009 reached $22.7 billion; a second IAB study suggesting that "ad-funded websites represented 2.1% of the U.S gross domestic product and directly employed more than 1.2 million people;" and a McKinsey study that used "conjoint" techniques to estimate that "in the U.S. and Europe consumers received 100 billion euros in value in 2010 from advertising-supported web services"). Similarly, Google published a study analyzing the total economic value received by U.S. advertisers, website publishers, and non-profits in 2010, which it estimated at $64 billion. *See* GOOGLE INC., GOOGLE'S ECONOMIC IMPACT: UNITED STATES | 2010 (2011), http://www.google.com/economicimpact/.

Tucker, online advertising is highly dependent on targeting, which uses customer profiles to find the particular ads most likely to influence a particular customer. Moreover, targeting increases the value of advertising to firms because they no longer have to pay for wasted eyeballs. Indeed, in 2009 the price of behaviorally targeted advertising was estimated at 2.68 times the price of untargeted advertising.[113]

In sum, ad targeting is valuable and privacy safeguards may increase opportunity costs to the extent that they diminish the economic value of online advertising, thereby creating an investment disincentive for firms dependent on advertising revenues. This disincentive may be offset by investments in privacy safeguards if they enable firms to attract new, privacy-sensitive customers or charge them higher prices, but there is scant evidence of this happening.

C. DO REPUTATIONAL SANCTIONS DRIVE PRIVACY INVESTMENTS?

Are firms sufficiently concerned about the reputational harms associated with high-profile privacy incidents to increase their investments in privacy technology? Although there is little data on firm expenditures in response to privacy meltdowns, the data on the reputational impact of security breach notifications is worth examining. More than forty-five states have enacted laws requiring that companies notify individuals of data security incidents involving their personal information.[114] These disclosures result in what Schwartz and Janger call "useful embarrassments" because they force businesses to invest ex ante in data security to avoid reputational sanctions including both diminished trust and potential loss of customers.[115] The Ponemon Institute has studied the costs of data breaches in the United States over the past several years and reports that in 2009, data breaches cost companies an average of $6.75 million per incident and $204 per

113. *See* Tucker, *supra* note 111, § 3.2.2 (citing Howard Beales, *The Value of Behavioral Targeting*, NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (last visited Mar. 5, 2012)); *see also* LENARD & RUBIN, *supra* note 82, at 14–18; Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising*, MGMT. SCI., Jan. 2011, at 57 (finding based on survey results that EU privacy regulation reduces the effectiveness of online advertising by restricting advertisers' ability to collect data on users for ad targeting purposes).

114. According to the National Council of State Legislatures (NCSL), "[f]orty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information." *See State Security Breach Notification Laws*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/Default.aspx?TabId=13489 (last updated Oct. 12, 2010).

115. *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 936 (2007).

compromised record.[116] Over 70% of the latter amount related to indirect costs including "abnormal turnover, or churn of existing and future customers" (down from 75% in 2008); these companies also suffered an average increased churn rate of 3.7% (up from 3.6% in 2008).[117] On the other hand, empirical evidence suggests that the cost of reputation loss (in terms of stock market impact) following incidents of data loss is statistically significant but relatively low in monetary terms and dissipates quickly.[118]

Although several commentators treat these studies as evidence that reputational sanctions pressure companies into improving their security practices,[119] Schwartz and Janger take a more cautious approach. As they note, the influence of reputational sanctions on data security can be quite complex. First, smaller firms and "bad apples" generally are less sensitive to reputational concerns.[120] Second, if sanctions rely on self-reporting, this may create a disincentive for reporting. Third, reputational sanctions are ineffective without "a well-functioning consumer-side market for data security."[121] Switching costs and lack of information about how firms manage data security undermine this market, notwithstanding whatever knowledge customers may derive from receiving, reading, and understanding breach notices.[122] In addition, there are a few drawbacks to the methods relied on in the Ponemon study—for example, it bases churn rates on company estimates, not on a survey of how many customers changed to another firm

116. *See* PONEMON INST., 2009 U.S. COST OF A DATA BREACH STUDY 5 (2009) (based on 45 respondents).

117. *Id.*

118. *See* Alessandro Acquisti, et al., Is There a Cost to Privacy Breaches? An Event Study 13–14 (2006) (unpublished manuscript), *available at* http://weis2006.econinfosec.org/docs/40.pdf (finding a cumulative drop in share prices per privacy incident of close to 0.6% on the day following the event, which equates to an average loss of approximately $10 million in market value).

119. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 10, 147 (2011); SAMUELSON LAW, TECH. & PUB. POLICY CLINIC, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 13–21 (2007), *available at* http://groups.ischool.berkeley.edu/samuelsonclinic/files/cso_study.pdf. *Cf.* Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERKELEY TECH. L.J. 1061 (2009) (arguing that state breach disclosure laws have only a very weak effect on the incidence of data loss).

120. Schwartz & Janger, *supra* note 115, at 930–31.

121. *Id.* at 944.

122. *Id.* at 947.

following a breach disclosure,[123] and it fails to explain the variance from the pre-breach churn rate or what other possible co-factors might exist.[124]

Even assuming that reputational sanctions help bring about increased security expenditures, there is reason to question their impact on privacy investments. An obvious difference is that while unauthorized access to personal data triggers existing breach notification laws, there are no laws requiring notification of privacy incidents *other than* data breaches.[125] In the absence of laws mandating disclosure of such matters, businesses are disinclined to self-report their privacy failures. Although investigative journalists and privacy activists may take up the slack, even if they do a good job the net result is that less data is available on how customers react to privacy incidents and whether firms respond to customer backlash by investing more in privacy safeguards. And this lack of data makes empirical study quite difficult.[126] One result is that there are no studies on the costs of privacy failure akin to the Ponemon series on data breaches. At the same time, the other factors noted by Schwartz and Janger remain in place. Thus, small firms and "bad apples" will free ride on the reputational efforts of larger firms, while information asymmetries and behavioral biases prevent consumers from understanding how a privacy incident might affect them or

123. *See* PONEMON INST., *supra* note 116, at 11, 35 (noting that the study required each company contact person to estimate opportunity costs based on her professional experience).

124. *See* ADAM SHOSTACK & ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 190 (2008). For an interesting counterpoint to the Ponemon study, see Larry Dignan, *The TJX Data Breach: Why Loss Estimates Are Overblown*, ZDNET: BETWEEN THE LINES (May 8, 2007), http://www.zdnet.com/blog/btl/the-tjx-data-breach-why-loss-estimates-are-overblown/5000 (noting that anticipated "brand impairment" was less severe than expected); Jaikumar Vijayan, *One Year Later: Five Takeaways from the TJX Breach*, COMPUTERWORLD (Jan. 17, 2008), http://www.computerworld.com/s/article/9057758/One_year_later_Five_takeaways_from_the_TJX_breach (noting that TJX's comparable-store sales increased 4% in the year following the breach).

125. These other incidents may range from objectionable data collection practices (such as profiling or targeting) to unauthorized secondary use of personal data to various processing errors that may lead to economic or non-economic harm. *See* Smith & Milberg, *supra* note 77. Although Acquisti et al. title their study "Is There a Cost to Privacy Breaches? An Event Study," they limit their analysis to data breaches. As a result, their findings have little bearing on the reputational costs of privacy incidents that fall beyond the scope of security breach notification laws.

126. *See* LONDON ECON. STUDY, *supra* note 30, at 52 (noting that "[d]espite the importance of reputation, relatively little reliable empirical work has been undertaken to measure its value in the context of privacy. This is partly because it is difficult to measure the value of an intangible asset such as reputation. But, it is also difficult to obtain good quality data on the costs of reputation loss (e.g. through privacy breaches) since firms may be unwilling or unable to quantify their losses"). *See* SHOSTACK & STEWART, *supra* note 124, at 74–76, 149–53 (discussing the value of breach data in understanding information security).

what they can do about it. The point is that in the absence of a well-functioning consumer-side market for privacy safeguards, firms will remain reluctant to spend more on PETs or privacy by design, notwithstanding potential reputational sanctions.[127]

What about longstanding industry forecasts suggesting that firms lose billions of dollars in online sales due to privacy concerns?[128] It is unclear whether this truly happens. As noted, consumers' self-reported attitudes about the high importance of privacy to their online shopping decisions do not always match their actual behavior. To the contrary, many consumers (all of Westin's "unconcerned" and at least some of his "pragmatists") seem willing to trade away privacy for discounts or convenience.[129] This is not to say that firms are—or should be—indifferent to their reputation for privacy and trustworthiness. Firms do seem to care, not only because consumer perceptions have some impact on sales and profits, but because any rational firm would prefer to avoid the expenses associated with a major privacy incident. These include legal fees, call center staffing costs, lost employee productivity, regulatory fines, diminished customer trust, and potential customer desertions, all of which can be costly.[130]

And yet the impact of these reputational sanctions on investments in privacy technology remains ambiguous. A spate of recent privacy incidents—in years past, from Microsoft (Word, Windows Media Player, Passport), and more recently from Google (Gmail, Search, Street View, Buzz), Facebook (Beacon, Newsfeed), and Apple (iPhone locational-tracking data)—raises similar concerns about transparency, notice, choice, and data retention. Advocates respond to these incidents in similar ways, with public outcries, open letters, and complaints to regulators. Newspapers publish major stories and editorials, privacy officials open investigations and issue opinions, and a few customers file class action law suits. But the outcomes in terms of investments in privacy safeguards vary widely, suggesting that negative publicity may be important to increased investments only when accompanied by two additional factors: sustained attention by government officials and a blatant violation of users' expectations that provokes an

127. Of course, this may vary by business sector, with more regulated industries or professions showing a greater willingness to invest in remediation of privacy breaches than a typical Internet firm.

128. *See* ALESSANDRO ACQUISTI, THE ECONOMICS OF PERSONAL DATA AND THE ECONOMICS OF PRIVACY 21 (2010).

129. *See supra* Section III.A.

130. Google recently paid $8.5 million to settle lawsuits concerning its Buzz service, *see* Damon Darlin, *Google Settles Suit over Buzz and Privacy*, N.Y. TIMES, Nov. 23, 2010, and will no doubt incur additional costs in complying with the FTC consent agreement.

immediate outcry (as when firms cross the invisible boundary between appropriate and inappropriate data sharing).[131] This requires further empirical study and analysis but is beyond the scope of this paper.[132]

IV. RECOMMENDED REGULATORY INCENTIVES

The previous Part concluded that economic incentives are not enough to increase firm investments in privacy safeguards. To summarize, the weak consumer demand for PETs, the opportunity costs to businesses associated with many PETs, and a lack of relevant data needed for cost-benefit analyses of investments in privacy safeguards all work against the further implementation of PETs in the marketplace. As noted, reputational sanctions do play a role especially when firms are also subject to sustained attention by regulators or cross a subtle boundary beyond which certain data processing practices are vigorously opposed by the general public. In these cases, even internet giants like Microsoft, Google, Facebook, and Apple are forced to retreat and to modify or withdraw disputed features.

Does this imply that self-regulation is working, or is government intervention still needed? Over the past twelve months, Congress has considered or introduced new privacy legislation, ranging from narrow bills that would mainly protect consumers against online tracking to omnibus privacy bills.[133] In anticipation of these bills, industry has unveiled new self-regulatory initiatives including both voluntary codes of conduct from the advertising industry and privacy-friendly tools from search firms, network

131. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE (2010) (analyzing privacy as "contextual integrity," which she defines in terms of appropriate information flows).

132. The author is undertaking a series of studies relating to privacy by design including empirical work that may shed light on these issues.

133. Narrow bills: *See* Staff of Richard Boucher, Discussion Draft of House Bill To Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to That Individual, 111th Cong. § 3(e) (May 3, 2010), *available at* http://dataprivacy.foxrothschild.com/uploads/file/Privacy_Draft_5-10.pdf (exempting network advertisers from having to obtain explicit, opt-in consent to engage in online tracking provided they allow consumers to access and manage their profiles); Do Not Track Me Online Act of 2011, H.R. 654, 112th Cong. (directing the FTC to develop standards for a "do not track" mechanism allowing individuals to opt out of the collection, use or sale of their online activities and requiring covered entities to respect the consumer's choice). Omnibus bills: *See* Best Practices Act, H.R. 611, 112th Cong. (2010); Commercial Privacy Bill of Rights Act of 2011 (the Kerry-McCain bill), S. 799, 112th Cong., *available at* http://www.govtrack.us/congress/bill.xpd?bill=s112-799.

advertisers, and browser vendors.[134] It remains to be seen whether these activities will be successful in warding off new legislation.[135]

On the other hand, privacy advocates reject these self-regulatory efforts as too little and too late. They argue that government intervention is needed to correct privacy market failures, implying that the demand for privacy safeguards will remain low and that firms will not increase their investments absent new legislation.[136] Accordingly, they insist that Congress at long last enact comprehensive legislation establishing baseline privacy requirements for online and offline data processing practices and empower the FTC to engage in rulemaking.[137] Of course, new default privacy rules may correct market failures but will also constrain profit-making activities at a significant cost to firms and the public.

In a recently published article, I suggested that self-regulation and prescriptive government regulation should not be viewed as mutually exclusive options from which policy makers are forced to choose. This is a false dichotomy and ignores the wide variety of co-regulatory alternatives that could be playing a larger role in the privacy arena.[138] Drawing on this earlier work and that of privacy scholars Kenneth Bamberger and Deirdre Mulligan, this Article concludes with a number of recommendations for how regulators might achieve better success in promoting the use of privacy by design by identifying best practices and/or situating these best practices within an innovative regulatory framework. This analysis considers co-regulatory solutions in two distinct environments: first, where Congress fails to enact new legislation but the FTC continues to play an activist role in defining CIPPs; and second, where Congress enacts a new privacy law

134. *See* Tanzina Vega, *Google and Mozilla Announce New Privacy Features*, N.Y. TIMES (Jan. 24, 2011), http://nyti.ms/y0g3fb (describing new "do not track" features by Google, Mozilla, and Microsoft as well as several self-regulatory programs).

135. *See* John Eggerton, *Q&A with FTC Chairman Jon Leibowitz*, MULTICHANNEL NEWS (Feb. 21, 2011), *available at* http://www.multichannel.com/article/print/464262-Privacy_Please_Q_A_With_FTC_Chairman_Jon_Leibowitz.php (noting that "the business community really has it in its hands to avoid regulation, it just has to step up to the plate").

136. *See* CDD Press Release, *supra* note 83.

137. *See* Juliana Gruenwald, *Lawmakers Looking for Right Balance on Privacy*, NATIONALJOURNAL TECH DAILY DOSE (Mar. 16, 2011), http://techdailydose.nationaljournal.com/2011/03/lawmakers-looking-for-right-ba.php.

138. *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POL'Y INFO. SOC'Y 355, 358 (2011) (noting that "[i]n co-regulatory approaches, industry enjoys considerable flexibility in shaping self-regulatory guidelines, while government sets default requirements and retains general oversight authority to approve and enforce these guidelines").

making FIPPs broadly applicable to firms that collect PII and possibly authorizing the FTC to establish a co-regulatory safe harbor program.[139]

A. THE FTC AS PRIVACY REGULATOR

If Congress enacts a new privacy law requiring firms to integrate privacy into their regular business operations and at every stage of the product development and data management lifecycle, and authorizing FTC rulemaking, then the Commission would address privacy by design by issuing implementing regulations. This would be quite analogous to the FTC drafting a rule covering the security and confidentiality requirements of financial institutions under the Gramm-Leach-Bliley Act ("GLBA").[140] If new legislation is not enacted, does the Commission already have authority under section 5 of the FTC Act to define the elements of CIPPs and require commercial firms to implement them? The short answer is yes—with a caveat.

Section 18 of the FTC Act grants the Commission *limited* authority to prescribe rules defining "unfair or deceptive acts or practices in or affecting commerce."[141] For better or worse, these procedures are burdensome and time-consuming as compared to conventional Administrative Protection Act ("APA") rulemaking.[142] As a result, the Commission often prefers to rely on strategic enforcement actions to achieve its regulatory goals, which is the procedure it followed in developing information security programs applicable to commercial firms.[143] In laying the foundations for CIPPs, the Commission has also relied on its section 5 powers to issue agency guidance regarding

139. For examples of a privacy bill providing safe harbor option, see the omnibus bills cited *supra* note 133. For a broader discussion of "co-regulatory" safe harbors and what they might contribute to the privacy debate, see generally Rubinstein, *supra* note 138, at 405–20 (arguing that such programs incentivize organizations to meet high standards of data protection by shielding safe harbor participants from various "sticks" such as a private right of action, and rewarding them with various "carrots" such as allowing greater flexibility in how they implement statutory requirements).

140. *See supra* note 69.

141. *See* 15 U.S.C. § 57a(a)(2) (2006).

142. *See* § 57a(b)(1), (2) (requiring that, before engaging in rulemaking, the FTC provide advance rulemaking notice to Congress and the public, hold public hearings at which interested parties have limited rights of cross-examination, and submit a statement of basis and purpose addressing both the prevalence of the acts or practices specified by the rule and its economic effect). Congress imposed these additional requirements on the Commission in 1980 in response to perceived abuses of the agency's rulemaking authority. *See generally* JULIAN O. VON KALINOWSKI ET AL., ANTITRUST LAWS AND TRADE REGULATION § 5.14 (1997).

143. *See* FTC STAFF REPORT, *supra* note 4, at 10–11.

commercial privacy practices. This has proven a flexible and effective tool.[144] Overall, this combination of strategic enforcement and agency guidelines developed in collaboration with industry demonstrates the FTC's "ability to respond to harmful outcomes by enforcing evolving standards of privacy protection" in keeping with changes in "the market, technology, and consumer expectations."[145]

Building from this foundation, the Commission can and should supplement the small number of enforcement cases related to privacy design practices by pursuing a strategic enforcement strategy. Indeed, it should look for cases that would further refine the core elements of CIPPs by establishing more prohibited, required, and recommended practices. This is necessary both because the analogy between CIPPs and CISPs is imperfect at best and the underlying design, coding, and testing practices for the former are far less developed than those of the latter. The Commission should consider several additional steps such as (1) convening a new round of workshops at which experts from industry, academia, and advocacy organizations identify useful PETs and discuss best practices in privacy by design, followed by a staff report and other guidance as appropriate; (2) supporting ongoing efforts by the ISO and others to define international privacy design standards; and (3) working with the National Institute of Standards or other federal agencies to fund research in requirements engineering, formal languages, and related tools and techniques that would transform privacy by design from a rallying cry into an engineering discipline.

B. REGULATORY INNOVATION

On the other hand, if Congress enacts new privacy legislation and authorizes the FTC to issue implementing regulations, this would open up several new pathways for regulatory innovation ranging from company-specific experimentation with new technologies and engineering practices to multi-stakeholder agreements on how to implement "do not track" practices to flexible safe harbor arrangements. This Section briefly examines several steps that the FTC should take if it is granted new regulatory authority.

1. Project XL for Privacy

The FTC should borrow a page from the environmental regulatory playbook by sponsoring a "Project XL for Privacy."[146] In a nutshell, Project

144. Bamberger & Mulligan, *supra* note 119, at 128–29.

145. *Id.*

146. *See* Rubinstein, *supra* note 138, at 374–76 (describing Project XL generally); *id.* at 406–10 (describing a modified version of Project XL attuned to the needs of privacy regulation).

XL is a program under which the Environmental Protection Agency ("EPA") negotiates agreements with individual firms to modify or relax existing regulatory requirements in exchange for enforceable commitments to achieve better environmental results. While these projects come in several flavors, the most useful for present purposes is the experimental XL project, in which the EPA takes the lead in identifying an innovative regulatory approach or technology and testing it out in a small number of pilot projects subject to rigorous evaluation by the EPA and other stakeholders. Conceived of as experiments from the outset, these projects may have industry-wide implications if they succeed or they may be abandoned if they fail to yield better results.

An obvious candidate for experimental XL projects for privacy might be in the area of privacy decision making. Several of the proposed privacy bills include lengthy and detailed notice requirements. These provisions are motivated by a desire to inform consumers of all relevant practices concerning personal data in a clear and conspicuous manner and to ensure that important information is not unduly vague or buried away. These efforts at ensuring rigorous and complete privacy notices are at once understandable and regrettable: no doubt many web sites and merchants engage in unfair or deceptive notice practices and yet more prescriptive notice requirements are not the remedy for the underlying problems, which range from asymmetric information to lack of readability to limited comprehension to consumer inertia.[147] However, researchers have developed a variety of tools to make privacy information more usable to consumers, such as standardized, easy-to-read privacy notices akin to nutrition labeling on food,[148] usability enhancements to P3P,[149] and a search engine that orders search results based on their computer-readable privacy policies.[150] The FTC should encourage firms to adopt these privacy-friendly PETs in exchange for regulatory relief on otherwise overly prescriptive notice requirements.

147. *See* Aleecia M. Mcdonald et al., *A Comparative Study of Online Privacy Policies and Formats*, *in* PROCEEDINGS OF THE 9TH INTERNATIONAL SYMPOSIUM ON PRIVACY ENHANCING TECHNOLOGIES (Ian Goldberg & Mikhail J. Atallah eds., 2009) and related studies cited therein; Egelman et al., *supra* note 108, at 1 (noting that "these policies rarely help consumers because they often go unread, or do not address the most common consumer concerns, [or] are difficult to understand").

148. PATRICK G. KELLEY ET AL., STANDARDIZING PRIVACY NOTICES: AN ONLINE STUDY OF THE NUTRITION LABEL APPROACH (Carnegie Mellon Univ., Report No. CMU-CyLab-09-014, 2010), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.

149. *See* PRIVACY BIRD, http://www.privacybird.org/ (last visited Nov. 8, 2011).

150. *See Frequently Asked Questions*, PRIVACY FINDER, http://www.privacyfinder.org/faq (last visited Nov. 8, 2011).

2. Negotiated Rulemaking

Congress may enact one of several pending bills that include a "do not track" requirement. If it does so and authorizes the FTC to promulgate a rule implementing a "do not track" provision, the FTC should forgo conventional rulemaking in favor of negotiated rulemaking.[151] In conventional FTC rulemaking—as exemplified by the rulemaking in the Children's Online Privacy Protection Act ("COPPA")[152]—the Commission first issues a Notice of Proposed Rulemaking ("NPR") soliciting comments from interested parties. Next, it conducts a review of the issues raised by these comments, which also includes holding a public workshop to obtain additional information regarding specific issues from industry, privacy advocates, consumer groups, and other government agencies. Lastly, the Commission publishes a Final Rule, which includes the agency's analysis of the public comments (which are also published) and its reasons for accepting or rejecting changes proposed pursuant to the NPR.[153]

Negotiated rulemaking, on the other hand, is a statutorily-defined alternative to conventional rulemaking in which agencies are granted the discretion to bring together representatives of the affected parties in a negotiating committee for face-to-face discussions. If the committee achieves consensus (defined as unanimous concurrence unless the committee agrees on a different definition such as general concurrence), the agency can then issue the agreement as a proposed rule subject to normal administrative review processes; but if negotiations fail to reach consensus, the agency may proceed with its own rule.[154]

Why might it be desirable to negotiate a "do not track" rule rather than rely on conventional rulemaking?[155] The core insight underlying negotiated rulemaking is that conventional rulemaking discourages direct communication among the parties, often leading to misunderstanding and even costly litigation over final rules. In contrast, the promise of negotiated

151. *See* Rubinstein, *supra* note 138, at 410–14 (describing negotiated rulemaking generally); *id.* at 377–80 (describing the application of negotiated rulemaking to the privacy issues associated with online behavioral advertising).

152. Pub. L. No. 105-277, 112 Stat. 2581 (1998) (codified at 15 U.S.C. §§ 6501–6506 (2006)).

153. *See COPPA Rulemaking and Rule Reviews*, FTC BUREAU CONSUMER PROTECTION BUS. CTR., http://business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews (last updated Sept. 15, 2011).

154. *See generally* Negotiated Rulemaking Act of 1990 (NRA), Pub. L. No. 101-648, § 2(3)–(5), 104 Stat. 4969, 4969 (codified as amended at 5 U.S.C. §§ 561–570 (2006)).

155. The following treatment draws from a more detailed discussion of regulatory options, including their strengths and weaknesses, in Rubinstein, *supra* note 138, at 412–14.

rulemaking is that by enlisting diverse stakeholders in the rulemaking process, responding to their concerns, and reaching informed compromises, better-quality rules will emerge at a lower cost and with greater legitimacy. Negotiated rulemaking works best when the underlying rule requires information sharing between the regulators, the regulated industry, and other affected parties, and when the parties believe they have something to gain from working together and achieving a compromise.[156] Arguably, these conditions would be met if the FTC formed a negotiated rulemaking committee to tackle a "do not track" rule.

Clearly, the parties would come to the table with different views. Industry would hope to minimize any burdens on its ability to collect and analyze the data needed for ad targeting, thereby maintaining the free flow of information. For example, it might suggest that privacy-friendly PETs suffice to achieve legislative goals. Advocates seeking better and more effective protection against profiling and targeting might demand that any opt-out mechanisms be turned on by default as opposed to requiring user-initiated action,[157] or they might otherwise require that industry adopt privacy-preserving PETs. These differences are deep-seated and perhaps ideological, and thus not easily overcome. Yet there is reason to believe that all of the affected parties—the regulated industry, the advocates representing the public interest, and the regulators—might be highly motivated to engage in face-to-face negotiations and would benefit from the information sharing that inevitably occurs in this setting.

As to motivation, industry may be concerned about whether the FTC lacks the necessary expertise to understand the complex technologies and business models underlying online advertising; and, if not, whether the Commission might issue a "do not track" rule lacking in flexibility and nuance with highly negative results for industry revenues and profitability. They may also fear that in the wake of new legislation, the Commission will pursue a more aggressive enforcement strategy. Advocates may worry that even if Congress enacts "do not track" legislation, this is no guarantee of a successful rulemaking. To begin with, the online advertising industry will persist in arguing that profiling and tracking for advertising purposes cause little if any real consumer harm whereas new advertising restrictions (especially a default opt-out rule) will not only lower advertising revenues but

156. *Id.* at 373 nn.69–72.

157. *See* Art. 29 Data Protection Working Party, 00909/10/EN, WP 171, *Opinion 2/2010 on Online Behavioural Advertising* 15 (June 22, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (arguing that default privacy-protective settings should require users "to go through a privacy wizard when they first install or update the browser").

imperil the subsidization of free online content and services, resulting in higher costs to consumers.[158] Moreover, advocates may worry that private factions will capture the conventional rulemaking process or that in implementing new legislation with unknown economic effects, the FTC will proceed very cautiously. In short, both sides may have something to gain from putting forward their best arguments in face-to-face negotiations, making reasonable concessions, and agreeing on a compromise.

As to information sharing, the negotiated rulemaking process by its very nature encourages more credible transmission of information among the parties. To begin with, the online advertising industry undoubtedly possesses greater expertise and insight into its own technology and evolving business models than either privacy advocates or FTC staff. In the past, this information has been shared or elicited mostly through one-sided communications—unilateral codes of conduct, complaints filed with the FTC, comments on FTC reports, or charges and countercharges at public forums. In a negotiated rulemaking process, however, the logic of Coasian bargaining prevails. In other words, each party seeks to "maximize its share of the gains produced by departure from standard requirements," and this requires that parties "educate each other, pool knowledge, and cooperate in problem solving."[159] In short, when both sides engage in explicit bargaining over priorities and tradeoffs, they are far more likely to achieve a satisfactory compromise than by relying on the indirect communications that characterize conventional rulemaking,[160] especially given their understanding that if negotiations fail, the FTC will proceed with its own rule.

3. Safe Harbor Programs

Finally, if Congress enacts into law either of the proposed bills that authorize safe harbor programs, the FTC should take a co-regulatory approach to rulemaking, i.e., one in which industry enjoys considerable flexibility in shaping self-regulatory guidelines in exchange for providing

158. *See, e.g.*, *'Do-Not-Track' Dissected: ClickZ Sends Feedback to FTC*, CLICKZ (Feb. 18, 2011), http://www.clickz.com/clickz/news/2027495/-track-dissected-clickz-sends-feedback-ftc.

159. *See* Jody Freeman & Laura I. Langbein, *Regulatory Negotiation and the Legitimacy Benefit*, 9 N.Y.U. ENVTL. L.J. 60, 69 (2000). For a very similar point, see Andrew P. Morriss et al., *Choosing How To Regulate*, 29 HARV. ENVTL. L. REV. 179, 201 (2005) (observing that "agencies may need the negotiation process to allow one set of interests to make credible commitments or disclosures to another set of interests that enable the regulation to be recognized as a Pareto improvement").

160. *See* DOC GREEN PAPER, *supra* note 62, at 5–6 (encouraging the development of codes of conduct using multi-stakeholder groups).

privacy protections that exceed default statutory requirements.[161] Section 5503 of the COPPA establishes an optional safe harbor that, in theory, would allow "flexibility in the development of self-regulatory guidelines" in a manner that "takes into account industry-specific concerns and technological developments."[162] In practice, the COPPA regulations are not very flexible, in part because the safe harbor approval process requires a side-by-side comparison of the substantive provisions of the COPPA rule with the corresponding sections of the self-regulatory guidelines. As a result, the four approved COPPA safe harbor programs are alike in reproducing the statutory requirements, and they show little differentiation by sector or technology. Nor do they benefit from face-to-face negotiations among the interested parties. The new privacy legislation provides a welcome opportunity to improve upon this first effort at implementing safe harbors.

For example, H.R. 611 specifically directs the FTC to implement safe harbor programs that allow for and promote "continued evolution and innovation in privacy protection, meaningful consumer control, simplified approaches to disclosure, and transparency" and provide "additional incentives" for participation in self-regulation.[163] One way for the Commission to accomplish this goal would be to permit the kind of experimentation described above. The Commission could then decide whether to allow an industry sector to comply with the notice requirements under Title I of the Act through some combination of "nutrition labels" for privacy, P3P user agents, and privacy search services. Or, even though subsections 403(1)(A) and (B) require that safe harbor programs provide consumers with a universal opt-out mechanism and various preference management tools, the Commission could decide whether firms satisfy these requirements (partially or in full) by adopting privacy-preserving targeted ad systems like Adnostic.

In addition, the Commission should treat safe harbor implementation as a perfect opportunity to experiment with negotiated rulemaking.[164] The Kerry-McCain bill should also be read as encouraging experimentation given that section 103 imposes a privacy by design requirement and section 501 requires the FTC to promulgate a rule establishing safe harbor programs that

161. *See* Rubinstein, *supra* note 138, at 414–20.

162. *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888, 59,906 (Nov. 3, 1999) (codified at 16 C.F.R. pt. 312).

163. H.R. 611, 112th Cong. § 404(4), (5) (2010).

164. Under the NRA, agencies have discretion to determine whether to rely on negotiated rulemaking provided they determine that the use of this procedure serves the public interest based on consideration of the seven factors identified in 5 U.S.C. § 563(a) (2006).

implement the requirements of the Act with regard to certain uses of personal data, while subsection 701(1) requires the DOC to contribute to the development of commercial data privacy policy by "convening private sector stakeholders, including members of industry, civil society groups, academia, in open forums, to develop codes of conduct in support of applications for safe harbor programs."[165] This language amounts to an open invitation to appoint a negotiating committee to flesh out the meaning of privacy by design in the context of a safe harbor program.

V. CONCLUSION

The endorsement by privacy officials of PETs and privacy by design presents both exciting opportunities and serious challenges. While firms could improve their data practices by adopting appropriate PETs or building privacy into the design of new products and services, they are unlikely to seize the initiative as long as the economic incentives remain inadequate and the meaning of privacy by design or PET remains inexact. In the face of weak consumer demand, a lack of relevant data to engage in cost-benefit analyses, high opportunity costs for any voluntary restrictions on collecting and analyzing valuable personal data, and reputational sanctions that frequently are not compelling enough to drive new privacy investments, regulatory incentives are required.

In the coming years, Congress may or may not enact new privacy legislation. In the absence of new legislation, the FTC may continue to pursue strategic enforcement actions and, on its own or in conjunction with the DOC, convene experts from industry, advocacy groups, and academia to develop best practices for privacy by design. Alternatively, new legislation may authorize FTC-supervised experimentation with innovative regulatory approaches that relax one-size-fits-all requirements in exchange for better privacy results, negotiated solutions to emerging regulatory challenges such as how best to implement a "do not track" rule, and/or the use of safe harbor programs that permit flexible self-regulatory arrangements for implementing CIPPs subject to FTC oversight and enforcement. In short, regardless of which path Congress follows, a co-regulatory approach not only overcomes the false dichotomy of purely voluntary industry codes of conduct versus highly prescriptive government regulation, but it also helps encourage innovation and experimentation with privacy technology.

165. The Kerry-McCain bill, S. 799, 112th Cong., § 701(1) (2010).

APPENDIX

PRELIMINARY LISTING OF BEST PRACTICES IN PRIVACY DESIGN BASED ON FTC ENFORCEMENT CASES AND THE STAFF REPORT[166]

Prohibited practices. Companies shall not:

- Exploit any security vulnerability to download or install software.[167]
- Distribute software code bundled with "lureware" that tracks consumers' internet activity or collects other personal information, changes their preferred homepage or other browser settings, inserts new toolbars onto their browsers, installs dialer programs, inserts advertising hyperlinks into third-party web pages, or installs other advertising software.[168]
- Install content protection software that hides, cloaks, or misnames files, folders, or directories or misrepresents the purpose or effect of files, directory folders, formats, or registry entries.[169]

Required practices. Companies must:

- Clearly and conspicuously disclose when free software is bundled with harmful software (malware) creating security and privacy risks for consumers who install it.[170]

166. This preliminary listing of privacy design practices is premised entirely on a subset of FTC enforcement cases and the views stated in the Staff Report. It is therefore a work in progress and necessarily incomplete in its current form. For alternative lists of privacy best practices, see *Privacy and Security | Privacy Overview*, ACM US PUB. POLICY COUNCIL, http://usacm.acm.org/privsec/category.cfm?cat=7&Privacy%20and%20Security (describing 24 recommended practices for developing systems that utilize PII); Marilyn Prosch, *Protecting Personal Information Using Generally Accepted Privacy Principles (GAPP) and Continuous Control Monitoring To Enhance Corporate Governance*, 5 INT'L J. DISCLOSURE & GOVERNANCE 153 (2008) (describing the development of a privacy framework that resulted in the formulation of the GAPP, which consists in 10 privacy principles and 66 auditable criteria).

167. Stipulated Final Order for Permanent Injunction and Settlement of Claims for Monetary Relief, FTC v. Odysseus Mktg., Inc., Civil No. 05-CV-330 (D.N.H. Oct. 24, 2006), *available at* http://www.ftc.gov/os/caselist/0423205/061121odysseusstipfinal.pdf.

168. Stipulated Final Order for Permanent Injunction and Monetary Judgment as to Defendants Enternet Media, Inc., Conspy & Co., Inc., Lida Rohbani, Nima Hakimi, and Baback (Babak) Hakimi, FTC v. Enternet Media, Inc., Civil No. CV 05-7777 (C.D. Cal. Aug. 22, 2006), *available at* http://www.ftc.gov/os/caselist/0523135/060823enternetmediastlmnt.pdf.

169. Decision and Order, Sony BMG Music Entm't, Docket No. C-4195 (FTC June 28, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/0623019do070629.pdf.

- Clearly and conspicuously disclose that the installation of software from a CD may limit a consumer's ability to copy or distribute audio files from the CD or other digital content; and, if such software causes information about consumers, their computes, or their use of a product to be transmitted via the Internet (so-called "phone home" features), then companies must disclose this prior to any such transmission and obtain the consumer's opt-in consent.[171]
- Provide a readily identifiable means for consumers to uninstall any adware or similar programs that monitor consumers' internet use and display frequent, targeted pop-up ads, where the companies deliberately made these adware programs difficult for consumers to identify, locate, and remove from their computers.[172]
- Clearly and prominently disclose the types of data that certain tracking software will monitor, record, or transmit prior to installing this software and separate from any user license agreement.[173]
- Provide prominent disclosures and obtain opt-in consent before using consumer data in a materially different manner than claimed when the data was collected, posted, or otherwise obtained.[174]

Recommended practices. Companies should do or adhere to the following:

- Develop and implement reasonable procedures concerning the collection and use of any personally identifiable information, including collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored.[175]
- Incorporate a formal privacy review process into the design phases of new initiatives.[176]

170. Decision and Order, Advertising.com, Docket No. C-4147 (FTC Sept. 12, 2005), *available at* http://www.ftc.gov/os/caselist/0423196/050916do0423196.pdf.

171. *Sony BMG*, Decision and Order, *supra* note 169.

172. Decision and Order, Zango, Inc., Docket No. C-4186 (FTC Mar. 9, 2007), *available at* http://www.ftc.gov/os/caselist/0523130/0523130c4186decisionorder.pdf.

173. Decision and Order, Sears Holdings Management Corp., Docket No. C-4264 (FTC Sept. 9, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf.

174. *See* Decision and Order, Gateway Learning Corp., Docket No. C-4120 (FTC Sept. 10, 2004), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf.

175. Letter from David C. Vladeck to Albert Gidari, *supra* note 66.

176. *Id.*

- Implement a "sliding scale" approach to access, taking into account the costs and benefits of access in different situations.[177]
- Provide "clear, comparable, and concise descriptions of a company's overall data practices" in privacy notices.[178]
- Seek affirmative express consent before collecting, using, or sharing any "sensitive information" including "information about children, financial and medical information, and precise geolocation data."[179]
- Where consumers elect not to have their information collected, used, or shared, "that decision should be durable and not subject to repeated additional requests from the particular merchant."[180]
- Where a company has a relationship with a consumer, it should offer a choice mechanism "at the point when the consumer is providing data or otherwise engaging with the company."[181]
- Where a company is engaged in online behavioral advertising, it should use a special choice mechanism consisting in "do not track."[182]
- Where a social media firm conveys consumer information to a third-party application developer, "the notice-and-choice mechanism should appear at the time the consumer is deciding whether to use the application and in any event, before the application obtains the consumer's information."[183]

177. FTC STAFF REPORT, *supra* note 4, at 72–73.
178. *Id.* at 71.
179. *Id.* at 61.
180. *Id.*
181. *Id.* at 58.
182. *Id.* at 63–69.
183. *Id.* at 59.