DRAFT: PLEASE DO NOT CITE WITHOUT AUTHOR'S PERMISSION

REGULATING PRIVACY BY DESIGN

Ira S. Rubinstein*

Privacy officials in Europe and the US 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 (EU DPD) 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) is now calling for data protection principles to be 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]

---

* Adjunct Professor of Law and Senior Fellow, Information Law Institute and, 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'm grateful to the comments of workshop participants. For detailed comments on an early draft, I am indebted to Kelly Caine, Peter Cullen, Erin Egan, Jacques Lawarree, Ron Lee, and Paul Schwartz. 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.

[1] *See* Ann Cavoukian, *Privacy by Design* (2009) *available at* 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 my longstanding mantra, to 'avoid making costly mistakes later on, requiring expensive retrofits'"). *See also* European Commission, *Communication from the Commission to the European Parliament, the Council, et al. on A Digital Agenda for Europe*, COM (2010) 245.

[2] *See* Council Directive 95/46, Art. 17(1), 1995 O.J. (L 281) 31, which 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."

[3] *See* Working Party 29 Opinion WP 168, *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* (Dec. 2009); Information and Privacy Commissioner, Ontario (Canada) and Registratiekamer (Netherlands), Privacy-Enhancing Technologies: The Path to Anonymity, Volume I (1995) *available at* http://www.ipc.on.ca/images/Resources/anoni-v2.pdf (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 European Commission, *Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)*, COM (2007) 228 final. Although the 1995 report views PETs primarily in terms of "identity protectors" (i.e., technologies that "separate one's true identity from the details of one's transactions through the use of "pseudo-identities"), the EC now holds a broader view of PETs as encompassing not only identity protection but various encryption tools, cookie managers and other filtering devices, and data management protocols such as the Platform for Privacy Preferences (P3P); *see* COM 228, *id.*at 3-4.

In the US, a very recent 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. More specifically, privacy by design has two main elements: first, incorporating (four) substantive privacy protections into a firm's practices; and second, maintaining comprehensive data management procedures throughout the life cycle of their products and services.[5] In passing, the report also mentions the use of PETs such as identity management, data tagging tools, transport encryption, and tools to "check and adjust default settings." In short, regulators on both sides of the Atlantic agree on the need for a new legal framework to protect online privacy in the 21st century and that one of its major aspects should be privacy by design.

Despite the enthusiasm of regulators, PETs have not achieved widespread acceptance in the marketplace and relatively few firms have embraced privacy by design. This due to a variety of factors such as confusion over key definitions and how privacy by design relates to specific technologies or organizational measures, and uncertainty as to what regulators really have in mind when they urge firms 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 about the privacy risks associated with web surfing, search, social networks, ecommerce, and other daily Internet activities and their limited understanding of how PETs or privacy by design might help reduce these risks. There is also the problem of cognitive and behavioral biases that prevent individuals from acting in accordance with their stated preference for greater privacy. And, of course, some consumers just don't care very much about privacy.[6] 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 implement voluntarily any PETs or design practices that would limit their ability to collect, analyze, or share valuable consumer data.[7]

Although the European Commission sponsored a study of the economic costs and benefits of PETs, and the UK 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 needs more attention in Europe and is largely absent

[4] Federal Trade Commission (Bureau of Consumer Protection), *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, (Dec. 1, 2010) *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (hereinafter the "Staff Report").

[5] *Id*. at 44-52.

[6] *See infra* Section II.A.

[7] *See infra* Section II.C.

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.

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. It 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-disclosure of personal data and, if successful, make legal protections less important or even superfluous. In contrast, complementary PETs fall into two sub-categories: 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 though cryptographic protocols or other sophisticated measures. Second, it explores the meanings 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, it 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; and 2) situating 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.

I. PETS AND PRIVACY BY DESIGN

The FTC's Proposed Framework states that to ensure proper incorporation of the four substantive principles identified in the report (data security, reasonable collection limitations, sound retention practices, and data accuracy), companies should develop and implement CIPPs. The two core elements of CIPPs are assigning specific personnel the responsibility for privacy training and for 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 staff supports the use of PETs.[8]

Privacy by design as so described in the Staff Report is certainly an enticing idea with great intuitive appeal. Why is this? Beyond conveying that privacy by design generally reduces errors and costs,[9] the FTC's discussion is short on specifics and never quite explains what it means to engage in privacy by design. Does it mean that companies should make more and better use of PETs and, if it does, 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),[10] but no effort is made to differentiate them according to relevant criteria. Alternatively, does it mean that companies should implement specific design practices or compliance measures? Without more detailed guidance on PETs or the meaning of privacy by design, 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 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 25 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.[11] Identity protectors and related PETs were first introduced as a regulatory strategy in the 1995 report on the "path to anonymity."[12] 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.[13]

---

[8] *See* Staff Report, *supra* note 4 at 44-52; for a more detailed FTC statement describing CIPPs in terms of five major elements, *see infra* notes 51to 54 and accompanying text.

[9] 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 AND 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 paper 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,

[10] *See* Staff Report, *supra* note 4 at 52.

[11] *See* Joan Feigenbaum et al, *Privacy Engineering in Digital Rights Management Systems,* ACM Workshop in Security and Privacy in Digital Rights Management (2001), *available at* http://web.archive.org/web/20020207202634/www.star-lab.com/sander/spdrm/index.html.

[12] *See supra* note 3.

[13] 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, *supra* note 11 at

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.[14] In contrast, other privacy tools permit data collection and analysis but seek to assist knowledgeable and motivated consumers in 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), although 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.[15] Other researchers classify PETs based on their underlying conception of privacy (e.g., control, autonomy, seclusion), but this has not proven very useful.[16] 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 or "complementary" PETs, and that this categorization is far more likely to result in useful guidance to the private sector on their adoption of PETs than any of these earlier attempts.[17]

B. A Taxonomy of PETs: Substitutes vs. Complements

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).

[14] For an explicitly normative treatment of PETs, *see, e.g.,* Roger Clarke, *Introducing PITs and PETs: Technologies Affecting Privacy* (2001) *available at* http://www.rogerclarke.com/DV/PITsPETs.html#PITs (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).

[15] *See, e.g.*, Lorrie F. Cranor, *The Role of Privacy Enhancing Technologies* (2003), *available at* http://old.cdt.org/privacy/ccp/roleoftechnology1.pdf; COLIN J. BENNETT AND CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 180-202 (2006); NATIONAL RESEARCH COUNCIL, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 107-16 (2007); Ian Goldberg, *Privacy Enhancing Technologies for the Internet III: Ten Years Later*, in DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES, 2-4 (A. Acquisti et al., eds., 2007).

[16] *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); Herman T. Tavani and James H. Moor, *Privacy Protection, Control of Information, and Privacy-Enhancing Technologies*, 31 COMPUTERS & SOCIETY 6 (2001); L.J. Camp and C. Osorio, *Privacy-Enhancing Technologies for Internet Commerce* in TRUST IN THE NETWORK ECONOMY, (O. Petrovic et al., eds., 2003).

[17] *See* BENNETT AND RAAB, THE GOVERNANCE OF PRIVACY, *supra* note 15 at 198 (noting that in Europe, PETs are often regarded as "a useful complement to existing regulatory and self-regulatory approaches" while in the U.S. they have sometimes been positioned as "an alternative to regulatory intervention").

Substitute PETs seek to protect privacy by ensuring that little or no personal data is collected in the first place, thereby making legal protections superfluous. 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.[18] 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).[19] Some substitute PETs also require ongoing maintenance, research and support from non-profits and volunteers (e.g., the Tor 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[20] 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.[21] This is hardly surprising: profit-motivated Internet firms collect and analyze personal data for multiple purposes—serving targeted ads; personalizing their services; and charging prices that extract as much surplus as possible from any sale (which economists refer to as price discrimination).[22] 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 legislative 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 but attempt to minimize potential consumer harms by ensuring that data is collected and

---

[18] *See* S. Spiekermann and L. Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 67 (2009).

[19] 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.

[20] 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 (2005) http://www.rsf.org/IMG/pdf/Bloggers_Handbook2.pdf (last visited Apr. 30, 2010).

[21] *See* Goldberg, *supra* note 15 at 8. Nevertheless, firms persist in trying to distinguish themselves on the basis of privacy. For recent examples of search engine that seek to maximize user privacy, *see* www.ixquick.com and www.duckduckgo.com.

[22] *See* LONDON ECONOMICS, 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 Economics 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 Interne*, in ICEC2003: Fifth Int'l Conf. on Elec. Comm. (ed., N.Sadeh, 2003), *available at* http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf.

processed in compliance with regulatory requirements based on Fair Information Practice Principles or FIPPs. Some complementary PETs focus on the "front-end" user experience (e.g., informed consent mechanisms, access tools, and preference managers), while others 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).[23]

Complementary PETs fall into two sub-categories: First, *privacy-friendly* PETs, whose overall goal is to give people more control over their personal data through improved notice and consent mechanisms, browser management tools, digital dashboards, and so on; and second, *privacy-preserving* PETs, which (in many cases) resemble substitute PETs in relying on sophisticated cryptographic protocols that may lead to deployable solutions with strong privacy guarantees but that also complement 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*[24] and privacy-preserving *targeted advertising*.[25]

Why are these distinctions important?[26] 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, business 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

---

[23] On the front-end/back-end distinction, *see* London Economics Study, *supra* note 22 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"); *see infra* Section I.C.1.

[24] *See* R. Agrawal and R. Srikant, *Privacy-Preserving Data Mining*, 29 SIGMOD RECORD 439 (2000).

[25] *See* V. Toubiana et al *Adnostic: Privacy preserving targeted advertising*, in 17th Annual Network and Distributed System Security Symposium, NDSS, 2010, *available at* http://crypto.stanford.edu/adnostic/adnostic.pdf.

[26] 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 COMMUNICATIONS OF THE ACM 82 (June. 2008)(describing an accountability framework, which combines strict legal rules on the permissible uses of data with a technical architecture that supports policy-aware transaction logs, a policy-languages, and policy-reasoning tools); THE PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY (PCAST), REALIZING THE FULL POTENTIAL OF HEALTH INFORMATION TECHNOLOGY TO IMPROVE HEALTHCARE FOR AMERICANS: THE PATH FORWARD (Dec. 2010), Chaps. 4 and 5 (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 "meta data tag" that describes the attributes, provenance, and required privacy and security protections of the data).

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.[27] This section concludes with a brief description of relevant tools in each of the main categories of PETs distinguished above:

1. Substitute PETs: Various anonymity tools are available that would 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, directly or indirectly, in their web services. 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 manager, 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 or her 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.[28] This proposed system

[27] See FED. TRADE COMMISSION, STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 9 n.21 (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (last visited Feb. 1, 2011(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* Staff Report, *supra* note 4 at 63-69 (discussing the "do not track" option).

[28] V. Toubiana, *Adnostic*, *supra* note 25.

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. 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.[29] 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.

C. Analyzing Privacy by Design

Privacy by design is a nebulous concept. At the very least, it means implementing FIPPs in the design and operation of products and service 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 consist in the adoption of certain processes, systems, procedures, and policies, any of which may also have a technological dimension, and which may be referred to collectively as privacy safeguards. EU privacy officials have always liked PETs, but have begun to embrace a more expansive approach to privacy by design that emphasizes sound design practices as well. In the US, the Commission gives short shrift to PETs,[30] 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 in an integrated set of development and management processes and practices. As with PETs, it is necessary to differentiate front-end software development activities from back-end data management practices. 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 transfer, storage and use). At the same time, it seeks to minimize the risks of privacy incidents (such as

[29] *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).

[30] For example, the Staff Report discusses privacy-friendly choice mechanisms for online behavioral advertising (including "Do Not Track") but otherwise barely mentions any substitution or privacy-preserving PETs.

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. The former is 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); the latter consists in data management processes and practices 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 also depend on back-end data handling.

This front-end/back-end distinction is generally consistent with the chief concerns discussed in sections V(B)(1) and V(B)(2) of the Staff Report. The former advises companies on "incorporating substantive privacy protections into their practices," while the latter recommends that companies maintain "comprehensive data management procedures." Yet there are shortcomings in the Commission's analysis, notably a lack of detail in describing design guidelines or data management practices and too little discussion of best practices or other actionable steps that companies should take if they wish to deploy privacy by design. 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.[31] The SDL aims to integrate privacy and security principles into the software development lifecycle, but each of the five stages of the development lifecycle (requirements, design, implementation, verification, and release) also includes privacy guidelines, which range from the mandatory to the recommended and from the procedural to the technical. Privacy impact ratings are given to each project and these ratings determine the design specifications needed for compliance. The SDL guidelines are supplemented by Microsoft's "Privacy Guidelines for Developing Software and Services," a 51-page document that lays out basic concepts and definitions based on the FIPPs and related US privacy laws; discusses different types of privacy controls and special considerations raised by shared computers, third parties,

[31] *See* Michael Howard and Steve Lipner, *The Trustworthy Computing Security Development Lifecycle* (2006), *available at* 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* http://www.microsoft.com/security/sdl/learn/measurable.aspx. The Department of Homeland Security, Software Assurance Program adopts a similar approach, which it refers to as "Build Security In"; *see* https://buildsecurityin.us-cert.gov/bsi/home.html.

and other situations; and then enumerates detailed guidelines for nine specific software product and Web site development scenarios.[32] 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.

On the data management side, IBM's Tivoli Privacy Manager is a comprehensive enterprise privacy management system that supports a variety of privacy functionalities.[33] 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 with the FIPPs) and a framework for managing these obligations. 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.[34]

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,[35] formal languages for representing such rules,[36] and

---

[32] *See* Microsoft Privacy Guidelines for Developing Software Products and Services, v. 3.1 (Feb. 2008), *available at* http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&DisplayLang=en (describing nine scenarios at length). Although the Microsoft 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 set of privacy guidelines is the European Privacy Seal (EuroPriSe) for IT-products and services, which has developed a 59-page document with four sets of detailed criteria that firms must satisfy to demonstrate compliance with the EU DPD; *see* EuroPriSe Criteria (2010), *available at* https://www.european-privacy-seal.eu/criteria/EuroPriSe%20Criteria%20201011.pdf.

[33] *See* Paul Ashley and David Moore, *Enforcing Privacy Within an Enterprise Using IBM Tivoli Privacy Manager for E-business* (2002), *available at* 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).

[34] *See* Marco Mont, *On Privacy–Aware Information Lifecycle Management in Enterprises: Setting the Context*, HPL-2006-109 (2006), *available at* http://www.hpl.hp.com/techreports/2006/HPL-2006-109.html (describing five core properties and functionalities of privacy–aware, information lifecycle management solutions).

[35] *See* Travis D. Breaux and Annie I. Anton, *Analyzing Regulatory Rules for Privacy and Security Requirements*, 34 IEEE TRANS. ON SOFTWARE ENG. 5 (2008).

[36] *See* A. Barth et al., *Privacy and Contextual Integrity: Framework and Applications*, in Proceedings of 27th IEEE Symposium on Security and Privacy, (May 2006), *available at* http://www.andrew.cmu.edu/user/danupam/bdmn-oakland06.pdf (describing a language for representation of rules

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.[37] 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."[38] The idea of using formal languages to align 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 require 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.[39] 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

---

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).

[37] *See* D. Garg et al., *A Logical Method for Policy Enforcement over Evolving Audit Logs*, (Feb. 2011), *available at* http://arxiv.org/abs/1102.2521. 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.

[38] Breaux and Anton *supra* note 35 (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 and David G. Gordon, *Regulatory Requirements as Open Systems: Structures, Patterns and Metrics for the Design of Formal Requirements Specifications*, Carnegie Mellon University Technical Report # CMU-ISR-11-100 (2010), *available at* http://reports-archive.adm.cs.cmu.edu/anon/isr2011/abstracts/11-100.html (describing a formal requirements specification language that allow 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).

[39] *See, e.g.*, U.S. Department of Homeland Security, *Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 2008)(identifying eight principles including purpose specification and use limitation).

threats consistent with customer expectations and legal requirements.[40] In Section V(B)(2), the report's guidance consists mainly in recommending first, that firms implement CIPPs and, second, that they assess risks (in a manner akin to 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 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.[41] 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, Privacy Impact Assessment or PIAs are the most widely used tool for privacy risk assessments, especially in the public sector.[42] 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.[43] But the Staff Report discussion of privacy assessments is too brief to infer whether it concurs with DOC's reasoning or would

---

[40] In fact, Sections V(C) and (D) of the Staff Report, *see supra* note 4 at 58-77, examine a number of scenarios involving choice, notice, access and material changes. Unfortunately, the report does not incorporate this analysis into the discussion of privacy by design.

[41] *See* OMB, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22 (Sep. 26, 2003)(further specifying when PIAs are required).

[42] *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*, (forthcoming 2011), *available at* http://idpl.oxfordjournals.org/content/early/2011/02/15/idpl.ipr002.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 … narrowly circumscribed legal requirements." *Id.* at 7.

[43] DEPT. OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 34-36 (2010) (hereinafter DOC Green Paper), *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf. 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 (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 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., provides for suitable controls, practices, and accountability) or if a corrective action plans need 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* Working Party 29, Opinion 9/2011, *Revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 3-4 (Feb. 2011).

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,[44] and how to increase transparency in data practices,[45] 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.[46]

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 discernable in the FTC's letter to Google closing the Street View investigation.[47] 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 WiFi 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."[48] 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

---

[44] *See* Staff Report, *supra* note 4 at 53-63.

[45] *Id*. at 69-77.

[46] *See infra* Appendix A, which identifies the relevant cases and additional discussion in the Staff Report and organizes them into a list of prohibited, required or recommended privacy design practices.

[47] *See* Letter to Albert Gidari, Esq., Counsel for Google, from David C. Vladeck, Director, Bureau of Consumer Protection, Closing Google Inquiry (Oct. 27, 2010) *available at* http://www.ftc.gov/os/closings/101027googleletter.pdf. 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. April 29, 010.

[48] Letter to Gidari, *supra* note 47.

maintaining the privacy and security of information collected and stored."[49] 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[50] and numerous FTC enforcement actions.[51] 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.[52]

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.[53] Similarly, although 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," in the security world, such benchmarks exist, while in the privacy world, they do not, although this

---

[49] *Id*.

[50] The Safeguards Rule, 16 C.F.R. pt. 314, implements the security and confidentiality requirements of the Gramm-Leach-Bliely Act (GLBA), 15 U.S.C. §§ 6801-09.

[51] For a list of relevant cases, *see* Staff Report, *supra* note 4 at 10-11. For a very recent example of an enforcement action defining a CISP, *see* Agreement Containing Consent order, *In re* Twitter, Inc., File No. 0923093 (June 24, 2010).

[52] *See* Agreement Containing Consent Order, *In the Matter of* Google, FTC File. No. 102 3136 (March 30, 2011). 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, *supra* note 51. 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. 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; and 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.

[53] For a description of relevant tools and techniques, *see generally* MICHAEL HOWARD AND DAVID LEBLANC, WRITING SECURE CODE (2000); MARK GRAFF AND KENNETH VAN WYK, SECURE CODING: PRINCIPLES AND PRACTICES (2003) GARY MCGRAW, SOFTWARE SECURITY: BUILDING SECURITY IN (2006).

is changing.[54] Lastly, it is worth noting that while the 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 FTC refers to these requirements.

II. MARKET INCENTIVES

This section 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 levels. 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 UK ICO insists that privacy by design will yield a "privacy dividend"[55] echoing Ann Cavoukian's earlier claim of a "privacy payoff" for firms that respect privacy and earn customer trust,[56] and her more recent assertion that "full functionality—*positive sum*, not zero sum" is a "foundational" principle of what she refers to as "PbD."[57] 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.[58] However, this view assumes that consumers understand how to recognize and protect themselves against both tangible harms, such as 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"

---

[54] 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 Security Techniques, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45306&development=on (last visited Mar. 14, 2011).

[55] *See* U.K.INFORMATION COMMISSIONER'S OFFICE, THE PRIVACY DIVIDEND: THE BUSINESS CASE FOR INVESTING IN PROACTIVE PRIVACY PROTECTION 3 (2010).

[56] *See* ANN CAVOUKIAN AND TYLER J. HAMILTON, THE PRIVACY PAYOFF: HOW SUCCESSFUL BUSINESSES BUILD CUSTOMER TRUST 36 (2002).

[57] *See* Ann Cavoukian, *Privacy by Design: The 7 Foundation Principles*, Principle 4, (revised, Jan. 2011), *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").

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

associated with them.[59] 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.[60] 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.[61]

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. 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 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."[62] 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.[63] In what follows, the goal is not to resolve these longstanding disputes or

---

[59] 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* (unpublished paper) (2010), *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 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).

[60] *See* London Economics Study, *supra* note 22 at 32-45.

[61] *See, e.g.*, Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2076-84 (2004); SOLOVE, THE DIGITAL PERSON, *supra* note 59 at 76-92.

[62] *See, e.g.*, THOMAS M. LENARD AND 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.

[63] *See* Center for Digital Democracy & U.S. Public Interest Research Groups, CDD and U.S. PIRG Call on FTC to Develop Stronger Online Privacy Framework (2011), *available at* http://www.democraticmedia.org/cdd-and-us-pirg-call-ftc-develop-stronger-online-privacy-framework.

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 isn't 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.[64] The recent FTC Staff Report provided similar statistics on downloads or usage of popular ad-blocking tools.[65]

Are these numbers indicative of growing consumer demand for privacy tools to which companies should rationally respond by offering more PETs 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,[66] and miniscule compared to the nearly 2 billion worldwide Internet users.[67] The only contradictory data comes from a privacy official at Facebook, who recently indicated that almost 35% of the company's 350 million users customized their privacy settings when Facebook released new privacy controls in December of 2009.[68] 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 that sharing personal data exposes them to.[69] 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

---

[64] *See* 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); 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, p2p network had been downloaded over 1.2 million times since its launch in 1999); Kim Zetter, *Rogue Nodes Turn Tor Anonymizer into Eavesdropper's Paradise*, WIRED, Sep. 10, 2007 (noting that Tor has hundreds of thousands of users around the world).

[65] *See* Staff Report, *supra* note 4 at note 69.

[66] Statistics on anti-virus use are *available at* http://www.internetworldstats.com/stats.htm (last visited Feb. 9, 2011).

[67] Statistics on world Internet usage are *available at* http://www.internetworldstats.com/stats4.htm.

[68] *See* Staff Report, *supra* note 4 at note 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*, ACM CHI Conference on Human Factors in Computing Systems (submitted 2011).

[69] *See* Alessandro Acquisti and Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy? in* ALESSANDRO ACQUISTI, ET AL., DIGITAL PRIVACY: THEORY, TECHNOLOGIES AND PRACTICES 364, 366-68 (2007) ("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").

data has very little value.[70] Well-known examples of such behavior include consumers giving away personal data in exchange for loyalty cards, discounts, and other conveniences such as access to free content and services.[71] Privacy expert Alan Westin cites variable privacy sensitivities.[72] More recently, behavioral economists have developed explanations based on bounded rationality[73] and behavioral biases such as immediate gratification or optimism bias.[74]

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.[75]

---

[70] *See, e.g.* Luc Wathieu and Allan Friedman, *An Empirical Approach to Understanding Privacy Valuation* (2007), *available at* http://www.hbs.edu/research/pdf/07-075.pdf. In *U.S. West, Inc. v. FCC*, 182 F. 3d 1224 (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 assuming that they would not bother to opt-out even if given the chance. *Compare* James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. Col. 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).

[71] *See* Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study* 3 (2007), 22 INFO. SYSTEMS RES. 1 (2011)(citing several relevant studies).

[72] *See Hearing on Opinion Surveys: What Consumers Have To Say About Information Privacy Before the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection*, 107th Cong. (2001) (testimony of Alan K. Westin) *available at* http://energycommerce.house.gov/107/hearings/05082001Hearing209/Westin309.htm. (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… the Privacy Pragmatists (63% or 125 million strong), [who] ask what's the benefit to them, what privacy risks arise, what protections are offered, and do they trust the company or industry to apply those safeguards and to respect their individual choice).

[73] *See* Acquisti and Grossklags, *What Can Behavioral Economics Teach Us About Privacy?, supra* note 69 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).

[74] *See* Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification* (2004) *available at* http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf 2 (highlighting various forms of psychological inconsistencies such as "self-control problems, hyperbolic discounting, present-biases, etc." that clash with the fully rational view of the economic agent).

[75] Adam Shostack and Paul Syverson, *What Price Privacy? (and Why identity Theft is About Neither Identity Nor Theft)* in ECONOMICS OF INFORMATION SECURITY 7 (L. Camp and S. 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 don't understand how the technology works when, for example, they visit a website that hosts "beacons" (i.e., invisible 1x1 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.[76] 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 a product or service's worth.[77] 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.[78]

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 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.[79] For the sake of analysis, however, we will assume that firms approach both investments in roughly the same manner.[80] This section also examines a factor largely neglected when *regulators* make the

---

[76] 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).

[77] Privacy seal programs seek to fill this role but have done so with limited success.

[78] *See* Tony Vila et al., *Why We Can't Be Bothered to Read Privacy Policies: Models of Privacy Economics as a Lemons Market* 3 (2003), *available at* http://www.eecs.harvard.edu/~greenie/econprivacy.pdf (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).

[79] *See* London Economics Study, *supra* note 22 at 59.

[80] 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* IAPP/PONEMON, BENCHMARK PRIVACY: AN EXECUTIVE SUMMARY STUDY (2010); ERNST & YOUNG, ACHIEVING SUCCESS IN A GLOBALIZED WORLD: IS YOUR WAY SECURE? (2006). On the other hand, if weak security has clear

business case for privacy by design, namely, the opportunity costs businesses would incur if pursuing this approach limits the scope of commercial exploitation of personal data.[81]

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[82] 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 but 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).[83]

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 10% of the total (as compared to 23% and 24% devoted to a privacy office (staff and related overhead) and training programs, respectively).[84] The second study pegs this range at from $500,000 to $2.5 million per year.[85] In any event, these figures are low given that the total average IT budget of a Fortune 500 firm is X , and that Y% (or approximately Z) is spent on security.[86]

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

---

economic costs and inadequate privacy does not, then perhaps firms will approach the relevant investment decisions in a different manner.

[81] *But see* London Economics Study, *supra* note 22, which does take into account this factor.

[82] 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.

[83] *See, e.g.*, Lawrence Gordon and Martin Loeb, *Budgeting Process for Information Security Expenditures*, 49 COMMUNICATIONS OF THE ACM 121 (June 2006). Brent R. Rowe and Michael P. Gallagher, *Private Sector Cyber Security Investment Strategies: An Empirical Analysis* (2006) *available at* http://weis2006.econinfosec.org/docs/18.pdf.

[84] *See* IBM AND PONEMON INST., THE COSTS OF PRIVACY STUDY (Feb. 17, 2004).

[85] *Compare* IAPP/PONEMON BENCHMARK STUDY (finding that more than 70% of companies with over $10 billion in revenue reported privacy budgets between $500,000 and $2.5 million).

[86] [still searching for appropriate source]

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.[87] There is some experimental evidence of consumers' willingness to pay a "privacy premium" to online merchants with superior privacy practices even thought they offer goods at higher prices.[88] Economists 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.[89] These are intriguing ideas but they have almost no commercial uptake despite the fact that the relevant technology is readily available.[90]

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.[91] This data collection and analysis for online advertising purpose is big business.[92] According to Tucker, online advertising is highly dependent on targeting, which use 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

---

[87] *See* London Economics Study, *supra* note 22 at 32-45; R. Böhme and S. Koble, *On the Viability of Privacy-Enhancing Technologies in a Self-Regulated Business-to-Consumer Market: Will Privacy Remain a Luxury Good?* (2007), *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 (2003) *available at* http://www.homeport.org/~adam/econbar-wes02.pdf.

[88] *See* Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study* 3 (2007), 22 INFO. SYSTEMS RES. 1 (2011) (lab study demonstrating that consumers are willing to pay more to shop at websites that have better privacy policies); and Serge Egelman, *Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators, Timing is Everything?* 1 (2009), *available at* http://www.guanotronic.com/~serge/papers/chi09a.pdf (follow-up study demonstrating that consumers are willing to pay more for higher level of privacy when privacy indicators were presented alongside of search results).

[89] *See* Alessandro Acquisti , A. (2004), *Privacy and Security of Personal Information: Economic Incentives and Technological Solutions*, in THE ECONOMICS OF INFORMATION SECURITY (J. Camp and S. Lewis, eds., 2004); Alessandro Acquisti , *Identity Management, Privacy, and Price Discrimination*, 6 IEEE SEC. & PRIV. 46 (2008); Böhme and Koble, *supra* note 87.

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

[91] *See* Catherine E. Tucker, *The Economic Value of Online Customer Data*, (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).

[92] *See* Tucker, *id*. at section 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 and website publishers in 2009, which it estimated at $1,110 billion; *see Google's Economic Impact United States, 2009* (2010), *available at* www.google.com/economicimpact/.

wasted eyeballs; indeed, in 2009 the price of behaviorally targeted advertising was estimated at 2.68 times the price of untargeted advertising.[93]

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. Almost all 50 states have enacted laws requiring that companies notify individuals of data security incidents involving their personal information. 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.[94] The Ponemon Institute has studied the costs of data breaches in the US 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 compromised record.[95] 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).[96] 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.[97]

---

[93] *Id*. at section 3.2.2, citing Howard Beales, *The Value of Behavioral Targeting* (2010) *available at* http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf. *See also* LENARD & RUBIN, IN DEFENSE OF DATA, *supra* note 62 at 14-18; Avi Goldfarb and Catherine E. Tucker , *Privacy Regulation and Online Advertising* (2010), *available at* http://www.rotman.utoronto.ca/~agoldfarb/GoldfarbTucker-Privacy.pdf (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).

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

[95] *See* PONEMON INSTITUTE, 2009 U.S. COST OF A DATA BREACH STUDY 5 (2009) (based on 45 respondents).

[96] *Id*.

[97] *See* Alessandro Acquisti, et al., *Is There a Cost to Privacy Breaches? An Event Study*, Workshop on the Economics of Information Security 13-14 (2006), *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).

Although several commentators treat these studies as evidence that reputational sanctions pressure companies into improving their security practices,[98] 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. Second, if sanctions rely on self-reporting, this may create a disincentive for reporting. Third, sanctions are ineffective without "a well-functioning consumer-side market for data security,"[99] but 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.[100] 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 following a breach disclosure;[101] and it fails to explain the variance from the pre-breach churn rate or what other possible co-factors might exist.[102]

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.[103] 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

---

[98] *See* Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 10, 147 (2010); 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. *Compare* Sasha Romanosky and Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 BERK.TECH. L. J. 1042 (2009)(arguing that state breach disclosure laws have only a very weak effect on the incident of data loss).

[99] Schwartz and Janger *supra* note 94 at 944.

[100] *Id*. at 947.

[101] *See* PONEMON INSTITUTE, *supra* note 95 at 12 and 36 (noting that the study required each company contact person to estimate opportunity costs based on her professional experience).

[102] *See* ADAM SHOSTACK AND ANDREW STEWART, THE NEW SCHOOL OF INFORMATION SECURITY 190 (2008). For an interesting counterpoint to the Ponemon study, *see* Blog post of Larry Dignan, *The TJX data breach: Why loss estimates are overblown* (May 8, 2007) *available at* http://www.zdnet.com/blog/btl/the-tjx-data-breach-why-loss-estimates-are-overblown/5000?tag=mantle_skin;content (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)(noting that TJX's comparable-store sales increased 4% in the year following the breach).

[103] 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 58. Although Acquisti et al. entitle their study "Is There a Cost to *Privacy* Breaches? An Event Study" (emphasis added), 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.

privacy safeguards. And this lack of data makes empirical study quite difficult.[104] One result is that there are no "costs of privacy failure" studies 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 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.[105]

What about longstanding industry forecasts suggesting that firms lose billions of dollars in online sales due to privacy concerns?[106] 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. 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.[107]

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), more recently from Google (Gmail, Search, Street View, Buzz), Facebook (Beacon, Newsfeed) and Apple (iPhone locational-tracking data), all raise 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 immediate outcry (as when firms cross the invisible boundary between appropriate and

---

[104] *See* London Economics Study, *supra* note 22 at 52 (noting that "Despite 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 AND STEWART, *supra* note 102 102 at74-76, 149-53 (discussing the value of breach data in understanding information security).

[105] 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.

[106] *See* Alessandro Acquisti, *The Economics of Personal Data and the Economics of Privacy* 21 (2010).

[107] Google recently paid $8.5 million to settle law suits 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.

inappropriate data sharing).[108] This requires further empirical study and analysis, but is beyond the scope of this paper.[109]

III. RECOMMENDED REGULATORY INCENTIVES

The previous section concluded that economic incentives were not enough to increase firm investments in privacy safeguards given weak consumer demand for PETs and a lack of relevant data needed for cost-benefit analyses of investments in privacy safeguards, especially given the opportunity costs associated with many PETs and design-based safeguards. As noted, reputational sanctions 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.[110] 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 advertisers and browser vendors. It remains to be seen whether these activities will be successful in warding off new legislation.[111]

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. Accordingly, they insist that Congress at long last enact comprehensive legislation establishing baseline privacy requirements for online and offline data

---

[108] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY AND THE INTEGRITY OF SOCIAL LIFE (2010) (discussing privacy in terms of appropriate information flows).

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

[110] Narrow bills: *See* STAFF OF RICHARD BOUCHER, STAFF DISCUSSION DRAFT (2010) §3(e), *available at* http://dataprivacy.foxrothschild.com/stats/pepper/orderedlist/downloads/download.php?file=http%3A//dataprivacy.foxrothschild.com/uploads/file/Privacy_Draft_5-10.pdf (last visited Feb. 1, 2011) (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. (2011) *available at* http://speier.house.gov/uploads/Do%20Not%20Track%20Me%20Online%20Act.pdf (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), *available at* http://house.gov/rush/pdf/hr611-bestpractices-act-20110211.pdf (last visited Feb. 1, 2011); Commercial Privacy Bill of Rights Act of 2011, (April 12 , 2011)(the Kerry-McCain bill) *available at* http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Text.pdf .

[111] *See Q&A With FTC Chairman Jon Leibowitz* (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").

processing practices and empower FTC to engage in rulemaking.[112] 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.[113] 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 under two distinct conditions: first, if Congress fails to enact new legislation but the FTC continues to play an activist role in defining CIPPs; and, second, if Congress enacts a new privacy law making FIPPs broadly applicable to firms that collect PII and possibly authorizing the FTC to establish a co-regulatory safe harbor program.[114]

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 GLBA.[115] 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."[116] For better or worse, these procedures are burdensome and time-consuming as compared to conventional

---

[112] *See* Juliana Gruenwald, "Lawmakers Looking for Right Balance on Privacy," NAT'L JNL., March 16, 2011, *available at* http://techdailydose.nationaljournal.com/2011/03/lawmakers-looking-for-right-ba.php

[113] *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, __ I/S: __ forthcoming 2011), *available at* http://ssrn.com/abstract=1510275 (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").

[114] For examples of a privacy bill providing safe harbor option, *see* H.R. 611 and the Kerry-McCain bill. For a broader discussion of "co-regulatory" safe harbors and what they might contribute to the privacy debate, *see generally* Rubinstein, *id.* (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 by allowing greater flexibility in how they implement statutory requirements).

[115] S*ee* the Safeguards Rule, *supra* note 50.

[116] *See* 15 U.S.C. §57a(a)(2).

Administrative Protection Act (APA) rulemaking.[117] 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.[118] In laying the foundations for CIPPs, the commission has also relied on its Section 5 powers to issue agency guidance regarding commercial privacy practices. This has proven a flexible and effective tool.[119] 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."[120]

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 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 FTC should take if it is granted new regulatory authority.

---

[117] *See* 15 U.S.C. §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 AND TRADE REGULATION §5.14 (1997).

[118] *See* Staff Report, *supra* note 4 at 10-11.

[119] Bamberger and Mulligan, *Privacy on the Books and on the Ground*, *supra* note 98 at 128.

[120] *Id*.

1. Project XL for Privacy. The FTC should borrow a page from the environmental regulatory playbook by sponsoring a "Project XL for Privacy."[121] In a nutshell, Project XL is a program under which the Environmental Protection Agency (EPA) negotiates agreement 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 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 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.[122] 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;[123] usability enhancements to P3P;[124] and a search engine that orders search results based on their computer-readable privacy policies.[125] The FTC should encourage firms to adopt these privacy-friendly PETs in exchange for regulatory relief on otherwise overly prescriptive notice requirements.

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 forego conventional rulemaking in favor of negotiated rulemaking.[126] In conventional FTC rulemaking—as exemplified by the

---

[121] *See* Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, *supra* note 113 at 13-15 (describing Project XL generally) and 34-37 (describing a modified version of Project XL attuned to the needs of privacy regulation).

[122] *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 and Mikhail J. Atallah, eds. 2009) and related studies cited therein; Egelman, *supra* note 88 (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").

[123] Patrick G. Kelley et al., *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach* (2010) *available at* www.cylab.cmu.edu/research/techreports/2009/tr-cylab09014.html.

[124] See http://www.privacybird.org/.

[125] *See* http://www.privacyfinder.org/faq.

[126] *See* Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, *supra* note 113 at 15-17 (describing negotiated rulemaking generally) and 37-39 (describing the application of negotiated rulemaking to the privacy issues associated with online behavioral advertising).

rulemaking in the Children's Online Privacy Protection Act (COPPA)—the Commission issues a Notice of Proposed Rulemaking (NPR) soliciting comments from interested parties; conducts a review of the issues raised by these comments, which in this case also included holding a public workshop to obtain additional information regarding specific issues from industry, privacy advocates, consumer groups, and other government agencies; and then 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 proposed changes to the NPR.[127] 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.[128]

Why might it be desirable to negotiate a "do not track" rule rather than rely on conventional rulemaking?[129] 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 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.[130] 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 are "on" by default as opposed to requiring user-initiated action[131] or otherwise require that industry adopt privacy-preserving PETs. These differences are deep-seated and perhaps ideological, and thus

---

[127] *See* http://business.ftc.gov/documents/coppa-rulemaking-and-rule-reviews.

[128] *See generally* Negotiated Rulemaking Act of 1990 (NRA), Pub. L. 101-648, § 2(3)-(5), 104 Stat. 4,969 (codified as amended at 5 U.S.C. §§ 561-570).

[129] The following discussion draws from the more detailed discussion in Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, *supra* note 113 at 15-17 and 37-39.

[130] *Id* at notes **Error! Bookmark not defined.-Error! Bookmark not defined.** and accompanying text.

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

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 causes little if any "real" consumer harm whereas new advertising restrictions (especially a default opt-out rule) will not only lower advertising revenues but imperil the subsidization of free online content and services, resulting in higher costs to consumers.[132] 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."[133] 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,[134] especially given their understanding that if negotiations fail, the FTC will proceed with its own rule.

---

[132] *See, e.g.,* ClickZ News Staff, "'Do-Not-Track' Dissected: ClickZ Sends Feedback to FTC," (Feb. 18, 2011) *available at* http://www.clickz.com/clickz/news/2027495/-track-dissected-clickz-sends-feedback-ftc.

[133] *See* Jody Freeman & Laura I. Langbein, *Regulatory Negotiation and the Legitimacy Benefit*, 9 N.Y.U. ENVTL. L.J. 60, 69. 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").

[134] *See* DOC Green Paper, *supra* note 43 at 5-6 (encouraging the development of codes of conduct using multi-stakeholder groups).

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 privacy protections that exceed default statutory requirements.[135] Section 5503 of 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."[136] 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 very much alike and 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. 611specifcally 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."[137] 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 Section 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.[138] The Kerry-McCain bill should also be read as encouraging experimentation given that Section 103 imposes a privacy by design requirement, Section 501 requires the FTC to promulgate a rule establishing safe harbor programs that implement the requirements of the Act with regard to certain uses of personal data, while Section 701(1) requires the Commerce Department 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

---

[135] *See* Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, *supra* note 113 at 39-43.

[136] *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).

[137] Sections 404(4) and (5).

[138] 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).

support of applications for safe harbor programs."[139] 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.

IV. CONCLUSION

The endorsement by privacy officials of PETs and privacy by design present 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, provided they know what this means, they are unlikely to seize the initiative as long as the economic incentives remain inadequate. 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. A co-regulatory approach would overcome the false dichotomy of relying on purely voluntary industry codes of conduct or highly prescriptive government regulation. Rather, co-regulation would encourage innovation and experimentation with privacy technology in either of two ways: the FTC's use of strategic enforcement actions and the convening of experts from industry, advocacy groups and academia, to develop best practices for privacy by design; or, if Congress enacts new legislation, 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 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 these ways will PETs and privacy by design achieve what they can now only promise.

[139] The Kerry-McCain bill, *supra* note 110.

Appendix A: Preliminary Listing of Best Practices in Privacy Design

1. *Prohibited practices.* Companies shall not:

    a. Exploit any security vulnerability to download or install software;[140]
    b. 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;[141]
    c. Install content protection software that that hides, cloaks or misnames files, folders, or directories, or misrepresents the purpose or effect of files, directory folders, formats, or registry entries.[142]

2. *Required practices.* Companies must:

    a. Clearly and conspicuously disclose when free software is bundled with harmful software (malware) creating security and privacy risks for consumers who install it;[143]
    b. 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;[144]
    c. 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.[145]
    d. 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. Sears also must disclose whether any data will be used by a third party.[146]

---

[140] *FTC v. Odysseus Marketing, Inc.*, No. 05-CV-330 (D.N.H. Oct. 24, 2006).
[141] *FTC v. Enternet Media, Inc.*, CV 05-7777 CAS (C.D. Cal., Aug. 22, 2006).
[142] Decision and Order, *In re* Sony BMG Music Entm't, FTC Docket No. C-4195 (June 28, 2007).
[143] Consent Order, *In re* Advertising.com, FTC File No. 042 3196 (Sept. 12, 2005).
[144] Decision and Order, *In re* Sony BMG Music Entm't, , FTC Docket No. C-4195 (June 28, 2007).
[145] Decision and Order, *In re* Zango, , FTC Docket No. C-4186 (March 9, 2007).
[146] *In re* Sears Holdings Management Corporation, FTC File No. 082 3099 (Sept. 9, 2009).

e. 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.[147]

3. *Recommended practices.* Companies should:

a. 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.[148]
b. Incorporate a formal privacy review process into the design phases of new Initiatives;[149]
c. 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" (Staff Report, p. 58).
d. 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" (Staff Report, p. 59).
e. 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" (Id.).
f. Seek affirmative express consent before collecting, using, or sharing any "sensitive information" including "information about children, financial and medical information, and precise geolocation data" (Staff Report, p. 61).
g. Where companies are engaged in online behavioral advertising, they should use a special choice mechanism consisting in "Do Not Track" (Staff Report, 63-69).
h. "Privacy notices should provide clear, comparable, and concise descriptions of a company's overall data practices" (Staff Report, 71).
i. Implement a "sliding scale" approach to access, taking into account the costs and benefits of access in different situations (Staff Report, 72-73)

[147] *See Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004)
[148] Letter to Albert Gidari, Esq., Counsel for Google, From David C. Vladeck, Director, Bureau of Consumer Protection, Closing Google Inquiry (Oct. 27, 2010).
[149] *Id.*