

NELCO
NELCO Legal Scholarship Repository

New York University Public Law and Legal Theory
Working Papers

New York University School of Law

8-1-2012

PRIVACY BY DESIGN: A COUNTERFACTUAL ANALYSIS OF GOOGLE AND FACEBOOK PRIVACY INCIDENTS

Ira S. Rubinstein
NYU School of Law, ira.rubinstein@nyu.edu

Nathaniel Good
Good LLC, nathan.good@gmail.com

Follow this and additional works at: http://lsr.nellco.org/nyu_plltwp

 Part of the [Computer Law Commons](#), [Consumer Protection Law Commons](#), and the [Science and Technology Commons](#)

Recommended Citation

Rubinstein, Ira S. and Good, Nathaniel, "PRIVACY BY DESIGN: A COUNTERFACTUAL ANALYSIS OF GOOGLE AND FACEBOOK PRIVACY INCIDENTS" (2012). *New York University Public Law and Legal Theory Working Papers*. Paper 347.
http://lsr.nellco.org/nyu_plltwp/347

This Article is brought to you for free and open access by the New York University School of Law at NELCO Legal Scholarship Repository. It has been accepted for inclusion in New York University Public Law and Legal Theory Working Papers by an authorized administrator of NELCO Legal Scholarship Repository. For more information, please contact tracy.thompson@nellco.org.

PRIVACY BY DESIGN: A COUNTERFACTUAL ANALYSIS OF GOOGLE AND FACEBOOK PRIVACY INCIDENTS

Ira S. Rubinstein[†] & Nathaniel Good^{††}

ABSTRACT

Regulators here and abroad have embraced “privacy by design” as a critical element of their ongoing revision of current privacy laws. The underlying idea is to “build in” privacy—in the form of Fair Information Practices or (“FIPs”)—when creating software products and services. But FIPs are not self-executing. Rather, privacy by design requires the translation of FIPs into engineering *and* usability principles and practices. The best way to ensure that software includes the broad goals of privacy as described in the FIPs and any related corporate privacy guidelines is by including them in the definition of software “requirements.” And a main component of making a specification or requirement for software design is to make it concrete, specific, and preferably associated with a metric. Equally important is developing software interfaces and other visual elements that are focused around end-user goals, needs, wants, and constraints.

This Article offers the first comprehensive analysis of engineering and usability principles specifically relevant to privacy. Based on a review of the technical literature, it derives a small number of relevant principles and illustrates them by reference to ten recent privacy incidents involving Google and Facebook. Part I of this Article analyzes the prerequisites for undertaking a counterfactual analysis of these ten incidents. Part II presents a general review of the design principles relevant to privacy. Part III turns to ten case studies of Google and Facebook privacy incidents, relying on the principles identified in Part II to discover what went wrong and what the two companies might have done differently to avoid privacy violations and consumer harms. Part IV of the Article concludes by arguing that all ten privacy incidents might have been avoided by the application of the privacy engineering and usability principles identified herein. Further, we suggest that the main challenge to effective privacy by design is not the lack of design guidelines. Rather, it is that business concerns often compete with and overshadow privacy concerns. Hence the solution lies in providing firms with much clearer guidance about applicable design principles and how best to incorporate them into their software development processes. Regulators should provide greater guidance on how to balance privacy with business interests, along with appropriate oversight mechanisms.

© 2013 Ira S. Rubinstein & Nathaniel Good.

[†] Adjunct Professor of Law and Senior Fellow, Information Law Institute, New York University School of Law.

^{††} Principal, Good Research LLC.

This Article was presented at the NYU Privacy Research Group and at the 2012 Privacy Law Scholars Conference, and we are grateful for the comments of workshop participants. Ron Lee, Paul Schwartz, and Tal Zarsky provided valuable suggestions on an earlier draft. Thanks are also due to Jeramie Scott and Mangesh Kulkarni for excellent research assistance and to Tim Huang for his help with citations. A grant from The Privacy Projects supported this work.

TABLE OF CONTENTS

I.	BACKGROUND	1335
II.	DESIGN PRINCIPLES	1343
A.	FAIR INFORMATION PRACTICES (“FIPs”) AS THE BASIS OF DESIGN PRINCIPLES.....	1343
1.	<i>FIPs or FIPs-Lite?</i>	1345
2.	<i>Privacy as Control</i>	1347
B.	AN ALTERNATIVE APPROACH TO PRIVACY BY DESIGN.....	1349
1.	<i>Multiple Meanings of Design</i>	1349
a)	Front-End Versus Back-End Design: The New Challenges of Designing for Privacy	1352
b)	Putting Design into Privacy by Design.....	1353
2.	<i>Privacy Engineering</i>	1354
a)	Background	1354
b)	FIPs-Based Privacy Engineering.....	1357
c)	Data Avoidance and Minimization.....	1358
d)	Data Retention Limits	1361
e)	Notice, Choice, and Access	1362
f)	Accountability	1365
3.	<i>Designing for Privacy: A UX Approach</i>	1365
a)	Background	1365
b)	Altman.....	1369
c)	Nissenbaum.....	1372
III.	CASE STUDIES AND COUNTERFACTUAL ANALYSES	1377
A.	GOOGLE	1377
1.	<i>Gmail</i>	1377
2.	<i>Search</i>	1379
3.	<i>Google Street View</i>	1382
4.	<i>Buzz and Google+</i>	1385
5.	<i>Google’s New Privacy Policy</i>	1389
B.	FACEBOOK	1392
1.	<i>News Feed</i>	1393
2.	<i>Beacon</i>	1394
3.	<i>Facebook Apps</i>	1395
4.	<i>Photo Sharing</i>	1398
5.	<i>Changes in Privacy Settings and Policies</i>	1400
C.	SUMMARY.....	1406
IV.	LESSONS LEARNED	1407
V.	CONCLUSION	1412

I. BACKGROUND

Regulators have embraced privacy by design.¹ Both the European Commission (“EC”) and the Federal Trade Commission (“FTC”) have recently called for a new approach to data protection and consumer privacy in which privacy by design plays a key role.² However, the details of what this means in practice will remain unclear until the EC completes its work on the delegated acts and technical standards anticipated by the proposed Regulation,³ or until the FTC refines the meaning of “unfair design” through enforcement actions⁴ and/or develops guidelines based on its ongoing dialogue with private firms.⁵ Indeed, despite the strong expressions of support for privacy by design, its meaning remains elusive.

Presumably, the regulatory faith in privacy by design reflects a commonsense belief that privacy would improve if firms “designed in” privacy at the beginning of any development process rather than “tacking it on” at the end. And yet there is scant relevant data in support of this view. A few firms have adopted privacy guidelines for developing products and services;⁶ however, a search of the literature reveals no before-and-after studies designed to determine if such firms have achieved better privacy

1. See Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1410–11 (2012) (describing statements by regulators in Canada, Europe, and the United States).

2. See *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, Recital 61, art. 23, COM (2012) 11 final (Jan. 25, 2012), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter *Proposed E.U. Regulation*] (requiring data controllers to implement mechanisms ensuring “data protection by design and by default”); FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/os/2012/03/120326_privacyreport.pdf [hereinafter *FTC FINAL REPORT*] (urging companies to “build in privacy at every stage of product development”).

3. *Proposed E.U. Regulation*, *supra* note 2, art. 23(3)–(4).

4. See, e.g., Complaint for Permanent Injunction and Other Equitable Relief at 13, 19, *F.T.C. v. Frostwire LLC*, No. 1:11-CV-23643, 2011 WL 9282853 (S.D. Fla. 2011) (describing default setting of Android application that allowed sharing of all existing files on the device in terms of “unfair design”).

5. See Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 287–89 (2011) (describing various “deliberative and participatory processes promoting dialogue with advocates and industry”).

6. See *The Role of Privacy by Design in Protecting Consumer Privacy*, CTR. FOR DEMOCRACY & TECH. (Jan. 28, 2010), <https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy> [hereinafter *Role of Privacy by Design*] (explaining that IBM, Sun Microsystems, Hewlett-Packard, and Microsoft have adopted privacy by design into their business models and product development procedures).

results. We propose to examine this question in a different fashion—not by gathering empirical data but rather by conducting and reporting on case studies of ten major Google and Facebook privacy incidents.⁷ We then consider whether the firms in question would have averted these incidents if they had implemented privacy by design.

This is a counterfactual analysis: we are asking a “what if?” question and will try to answer it by discussing what Google and Facebook might have done differently to better protect consumer privacy and thereby avoid these incidents. The proposed analysis has two prerequisites. First, we need ready access to a great deal of information about the selected incidents so that we have a reasonably clear idea of what happened as well as how and why the firms responded as they did (for example, by modifying certain features or even withdrawing a service entirely). Absent such information, it would be impossible to consider what the firm might have done differently if it had adopted privacy by design. Second, we need to identify a baseline set of *design* principles that will inform our discussion of alternative outcomes.

The first task is easy because there are so many well-documented major Internet privacy incidents. A non-exhaustive list would include privacy gaffes by AOL, Apple, DoubleClick, Facebook, General Motors, Google, Intel, Microsoft, MySpace, Real Networks, Sony, and Twitter.⁸ This Article focuses on a series of related incidents—five each from Google and from Facebook—for several reasons. To begin with, both firms have experienced serious privacy incidents and suffered major setbacks ranging from negative publicity and customer indignation to government scrutiny, regulatory actions, and law suits. Second, their travails have been well documented by investigative journalists, privacy advocates, and various regulators. And, third, both firms have all of the necessary resources—engineering talent, financial wherewithal, and business incentives—to prevent future incidents by implementing a leading-edge program of privacy by design. Moreover, studying a range of incidents at each company—Gmail, Search, Street View, Buzz (and Google+), and changes in privacy policies for Google; and News Feed, Beacon, Facebook Apps, Photo Sharing, and changes in privacy

7. As used here, the term “incident” is descriptive rather than normative. Thus, a “privacy incident” is no more than an episode or event that raises privacy concerns. Not every privacy incident results from a design failure or causes harm. However, because privacy is highly cherished and causes anxiety if violated, many privacy incidents are associated with negative press coverage, reputational harm, regulatory investigations, and/or enforcement actions.

8. We identified these incidents based on general knowledge and by reviewing the websites of leading privacy organizations for discussion of privacy issues; we also conducted a LexisNexis® search.

policies and settings for Facebook—makes it possible to observe patterns and compare how the two companies think about privacy, especially in similar services such as social networking.⁹

The second task—identifying design principles to rely on for purposes of a counterfactual analysis—is far more difficult. An obvious starting point for understanding what it means to design products and services with privacy in mind is the set of internationally recognized values and standards about personal information known as the Fair Information Practices (“FIPs”).¹⁰ The FIPs define the rights of data subjects and the obligations of data controllers; most privacy laws throughout the world rely on FIPs.¹¹ This Article argues that although the FIPs allocate rights and responsibilities under applicable legal standards, the present task requires something different, namely, *design* principles and related practices.

Another possible source of guidance is the work of Ann Cavoukian, the Information and Privacy Commissioner (“IPC”) of Ontario, Canada. Cavoukian is a tireless champion of privacy by design (or “PbD” to use her preferred acronym) and has authored or coauthored dozens of papers describing both its origins and its business and technology aspects.¹² In 2009, Cavoukian advanced the view that firms may accomplish privacy by design by practicing seven “foundational” principles:

1. Proactive not Reactive; Preventative not Remedial;
2. Privacy as the Default Setting;
3. Privacy Embedded into Design;
4. Full Functionality—Positive-Sum, not Zero-Sum;
5. End-to-End Security—Full Lifecycle Protection;
6. Visibility and Transparency—Keep it Open; and
7. Respect for User Privacy—Keep it User-Centric.¹³

9. See *infra* Part III.

10. The FIPs are a set of internationally recognized privacy principles that date back to the 1970s. They have helped shape not only the main U.S. privacy statutes but also European data protection law. See *infra* Section II.A; see generally *Fair Information Practice Principles*, FED. TRADE COMM’N, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm> (last visited Mar. 15, 2013).

11. See, e.g., Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn’t Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 44 (2001).

12. These publications are available on the IPC website. *Discussion Papers*, IPC, <http://www.ipc.on.ca/english/Resources/Discussion-Papers> (last visited Mar. 6, 2013).

13. ANN CAVOUKIAN, *PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES* (2011), www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf.

Although Cavoukian's many publications offer valuable lessons in how the public and private sector might apply the "PbD approach" to new information systems and technologies, it is not at all clear for present purposes that her seven principles are of any greater assistance than the FIPs.

To begin with, Cavoukian's seven principles are more aspirational than practical or operational. Principles 1–3 provide useful, if somewhat repetitive, guidance about the importance of considering privacy issues early in the design process and setting defaults accordingly, but they stop far short of offering any design guidance. Granted, Cavoukian offers more practical advice in several of her technology-specific papers,¹⁴ but she makes little effort to systematize or even summarize the design principles found therein.¹⁵ Principle 4 seems unrealistic in an era when some view personal data as the "new oil" of the Internet and privacy controls only tend to limit the exploitation of this valuable commodity.¹⁶ Principle 5 emphasizes lifecycle management, which is a key aspect of privacy engineering. Principle 6 resembles the familiar transparency principle found in all versions of FIPs, while Principle 7 functions primarily as a summing up of the earlier principles. Moreover, Cavoukian associates PbD with many other concepts,

14. Among the topics covered are smart grids, Radio Frequency Identification ("RFID"), biometric systems, mobile communications, Wi-Fi positioning systems, and mobile near field communications ("NFC"). See *Publications: Papers*, PBD, <http://www.privacybydesign.ca/index.php/publications/papers> (last visited Mar. 15, 2013).

15. Instead, many of the papers merely restate or elaborate the seven foundational principles. See, e.g., ANN CAVOUKIAN, *OPERATIONALIZING PRIVACY BY DESIGN: A GUIDE TO IMPLEMENTING STRONG PRIVACY PRACTICES* (Dec. 4, 2012), <http://www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf>; ANN CAVOUKIAN, *ACCESS BY DESIGN: THE 7 FUNDAMENTAL PRINCIPLES* (May 10, 2010), http://www.ipc.on.ca/images/Resources/accessbydesign_7fundamentalprinciples.pdf; ANN CAVOUKIAN & MARILYN PROSCH, *PRIVACY BY REDESIGN: BUILDING A BETTER LEGACY* (May 20, 2011), <http://www.ipc.on.ca/images/Resources/PbRD-legacy.pdf>.

16. See Meglena Kuneva, European Consumer Commissioner, Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling 2 (Mar. 31, 2009), http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm; see also Julia Angwin & Jeremy Singer-Vine, *Selling You on Facebook*, WALL ST. J. ONLINE (Apr. 7, 2012), <http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html>.

Angwin and Singer-Vine wrote:

This appetite for personal data reflects a fundamental truth about Facebook and, by extension, the Internet economy as a whole: Facebook provides a free service that users pay for, in effect, by providing details about their lives, friendships, interests and activities. Facebook, in turn, uses that trove of information to attract advertisers, app makers and other business opportunities.

Id.

including accountability,¹⁷ risk management,¹⁸ FIPs,¹⁹ and privacy impact assessments (“PIAs”).²⁰ This breadth tends to dilute, rather than clarify, Cavoukian’s definition of PbD. As several European computer scientists recently concluded, the principles as written do not make it clear “what ‘privacy by design’ actually is and how it should be translated into the engineering practice.”²¹

Of course, various commentators have taken different approaches to privacy by design. Some see PbD as an offshoot of privacy-enhancing technologies (“PETs”);²² others in terms of a life cycle approach to software development and/or data management (i.e., one that considers privacy at all stages of product design and development);²³ and still others in terms of implementing “accountability based mechanisms” such as risk-based privacy impact assessments.²⁴ Some regulators combine all of these ideas under the

17. See ANN CAVOUKIAN, SCOTT TAYLOR & MARTIN ABRAMS, *PRIVACY BY DESIGN: ESSENTIAL FOR ORGANIZATIONAL ACCOUNTABILITY AND STRONG BUSINESS PRACTICES* 3 (Nov. 2009), http://www.privacybydesign.ca/content/uploads/2009/11/2009-11-02-pbd-accountability_HP_CIPL.pdf (describing accountability as a business model wherein “organizations tak[e] responsibility for protecting privacy and information security appropriately and protecting individuals from the negative outcomes associated with privacy-protection failures”).

18. See ANN CAVOUKIAN, INFO. & PRIVACY COMM’N, *PRIVACY RISK MANAGEMENT: BUILDING PRIVACY PROTECTION INTO A RISK MANAGEMENT FRAMEWORK TO ENSURE THAT PRIVACY RISKS ARE MANAGED, BY DEFAULT* 17 (Apr. 2010), <http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf> (asserting that privacy risks may be “[m]anaged in a fashion similar to conventional risks . . . by employing the principles of privacy by design”).

19. See ANN CAVOUKIAN, *THE 7 FOUNDATIONAL PRINCIPLES: IMPLEMENTATION AND MAPPING OF FAIR INFORMATION PRACTICES* (2011), <http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf> (comparing FIP principles with privacy by design principles).

20. See PAT JESELON & ANITA FINEBERG, *A FOUNDATIONAL FRAMEWORK FOR A PBD-PIA* (Nov. 2011), <http://privacybydesign.ca/content/uploads/2011/11/PbD-PIA-Foundational-Framework.pdf> (offering a framework for a privacy by design privacy impact assessment).

21. Seda Gürses et al., *Engineering Privacy by Design*, International Conference on Privacy and Data Protection (“CPDP”) (2011), <http://www.dagstuhl.de/mat/Files/11/11061/11061.DiazClaudia.Paper.pdf> (arguing that many of the seven principles include the term “privacy by design” in the explanation of the principle itself resulting in recursive definitions).

22. See generally Rubinstein, *supra* note 1, at 1414–26.

23. See FTC FINAL REPORT, *supra* note 2, at 46–47.

24. See E.U. ARTICLE 29 DATA PROTECTION WORKING PARTY, *OPINION 3/2010 ON THE PRINCIPLE OF ACCOUNTABILITY* (WP 173) 3 (July 2010) [hereinafter WP 173], http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf; see also Paula J. Bruening, *Accountability: Part of the International Public Dialogue About Privacy Governance*, BNA INT’L WORLD DATA PROTECTION REP. 2 (October 2010) (describing the work of an

umbrella of privacy management programs that include policies, procedures, and systems architecture; several recent FTC consent decrees have required companies like Google, Facebook, Twitter, and MySpace to adopt identical five-part programs combining accountability, risk assessment, design processes, due diligence in selecting vendors, and ongoing program adjustments.²⁵ But the FTC offers firms no guidance about how to implement such programs.

Fortunately, a few private sector firms have developed more detailed privacy guidelines, explaining how to integrate privacy into the several stages of the software development process (requirements, design, implementation, verification, and release).²⁶ For example, in 2006 Microsoft published a comprehensive set of guidelines that explores nine specific development scenarios and identifies over 120 required and recommend practices for “creating notice and consent experiences, providing sufficient data security, maintaining data integrity, offering customers access [to their data], and supplying [other privacy] controls.”²⁷ Although the guidelines are full of sound advice and would benefit both established and start-up firms, they also have several shortcomings. First—and this is not a problem limited to Microsoft—the tools and techniques concerning “privacy by design” are quite immature, especially as compared with those relied upon for “security by design.”²⁸ Second, the guidelines have not kept up with the transition from client-server products to social media and Web 2.0 services and largely omit this topic, which makes them badly outdated. Finally, the guidelines

expert group convened by the Irish Data Protection Commissioner for the purpose of defining the essential elements of accountability).

25. *See, e.g.*, Agreement Containing Consent Order, Google, Inc., F.T.C. No. 102-3136, 4–5 (Mar. 30, 2011) [hereinafter Google Settlement], <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagrecorder.pdf>; Agreement Containing Consent Order, Facebook, Inc., F.T.C. No. 092-3184, 5–6 (Nov. 29, 2011) [hereinafter Facebook Settlement], <http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>. The third element specifically requires firms to engage in “the design and implementation of reasonable controls and procedures to address the risks identified through the privacy risk assessment.” *Id.*

26. *See Role of Privacy by Design, supra* note 6.

27. *Privacy Guidelines for Developing Software Products and Services, v. 3.1*, MICROSOFT, 5 (Sept. 2008), <http://www.microsoft.com/en-us/download/details.aspx?id=16048> [hereinafter *Microsoft Privacy Guidelines*]. Ira Rubinstein was an Associate General Counsel at Microsoft when these guidelines were first developed but did not contribute to them.

28. In security engineering, there is consensus on the meaning of key concepts and there are tried-and-true design principles and canonical texts, international standards, and a large cadre of certified security experts. Additionally, security professionals may draw upon a variety of technical resources including sophisticated threat-modeling processes, secure coding practices, and automated development and testing tools. Privacy professionals enjoy few of these advantages or resources.

allow business units within Microsoft to balance privacy requirements against business purposes but offer limited guidance on this delicate task.²⁹ For example, while “essential” actions such as processing of real-time location data, waiver of certain notice requirements, and transfer of sensitive personal information require “Company Approval,”³⁰ there is little discussion of the relevant factors for granting or withholding such approval. Similarly, the guidelines state that when data transfers or updates are “essential” to the functioning of a product (as defined by Microsoft), this justifies a weaker “all-or-nothing” form of user controls.³¹ More generally, Microsoft’s internal decision-making process under the guidelines remains opaque to customers and policy makers, which has led to accusations that business or competitive considerations sometimes overwhelm privacy requirements.³²

All of these varied attempts at fleshing out the meaning of privacy by design are valuable and we have no wish to disparage them. This Article takes a different approach, however. We contend that although FIPs underlie privacy by design, they are not self-executing. Rather, privacy by design requires the translation of FIPs into engineering and design principles and practices. An example helps illustrate what we have in mind. One of the FIPs, the purpose specification principle, is the basis for limits on how long a company may retain personal data. But there is a vast difference between a company promising to observe reasonable limitations on data retention and designing a database that automatically tags personal and/or sensitive information, keeps track of how long the information has been stored, and deletes it when a fixed period of time has expired. To adapt a familiar distinction, one is just words, while the other is action realized through code.

We argue that FIPs must be translated into principles of privacy engineering and usability and that the best way to accomplish this task is to

29. *Microsoft Privacy Guidelines*, *supra* note 27, at § 1.2; *see also infra* notes 456, 461–63 and accompanying text (discussing balancing).

30. The Microsoft Privacy Guidelines define “Company Approval” as “[t]he consent of the authorized privacy council or privacy decision makers within the Company, which may include legal counsel.” *Microsoft Privacy Guidelines*, *supra* note 27, at 26.

31. *Id.* at 30, 33, 36.

32. *See* Nick Wingfield, *Microsoft Quashed Efforts to Boost Online Privacy*, WALL ST. J. ONLINE (Aug. 1, 2010), <http://online.wsj.com/article/SB10001424052748703467304575383530439838568.html> (describing an internal debate in 2008 over privacy features in Microsoft’s Internet Explorer (“IE”) 8 browser that the advertising division feared would undermine both Microsoft’s and its business partners’ targeted advertising abilities). Microsoft later reversed this decision and added a very similar feature to IE 9. *See* Nick Wingfield & Jennifer Valentino-DeVries, *Microsoft To Add ‘Tracking Protection’ to Web Browser*, WALL ST. J. ONLINE (Dec. 7, 2010), <http://online.wsj.com/article/SB10001424052748703296604576005542201534546.html>.

review the relevant technical literature and distill the findings of computer scientists and usability experts.³³ This is a departure from most discussions of privacy by design, which tend to slight the small but significant design literature in favor of advocating broad discourse on policy principles and business practices. We seek to remedy this omission and put the design back into privacy by design.

This Article proceeds as follows: In Part II, we present a general review of the design principles relevant to privacy. This requires a brief analysis of the strengths and weaknesses of FIPs as a source of privacy design principles. Here we mainly focus on the failure of the notice-and-choice model of FIPs and the shortcomings of all versions of FIPs insofar as they rely primarily on a control conception of privacy. Next, we closely examine what it means to design for privacy, defining “design” in terms of two broad and at times overlapping ideas: back-end software implementations of networking and related systems infrastructure, which are generally hidden from the user but drive the heart of any system; and front-end user interfaces, which (in the privacy setting) handle tasks such as notification, consent, access, preference management, and other user experiences.³⁴ We therefore analyze privacy by design from two complementary perspectives: *privacy engineering*, which refers to the design and implementation of software that facilitates privacy, and *usable privacy design*, which refers to design tasks involving human-computer interaction (“HCI”). The former focuses on building software to satisfy the abstract privacy requirements embodied in the FIPs (in some cases overlapping with security engineering), the latter on ensuring that users understand and benefit from well-engineered privacy controls. Our discussion of privacy engineering draws mainly on four key papers in the technical design literature and the works cited therein.³⁵ In contrast, our discussion of usable privacy design looks at a rather different body of work

33. We also suggest that FIPs must be extended to address the “social dynamics” of privacy. See *infra* notes 59–68, 85–86 and accompanying text.

34. This distinction is by no means absolute. Back-end systems may come with user interfaces and front-end interfaces may rely on sophisticated engineering techniques. For more on this distinction, see generally Rubinstein, *supra* note 1, at 1418, 1422.

35. See George Danezis & Seda Gürses, *A Critical Review of 10 Years of Privacy Technology*, in PROCEEDINGS OF SURVEILLANCE CULTURES: A GLOBAL SURVEILLANCE SOCIETY? (2010), <http://homes.esat.kuleuven.be/~sguurses/papers/DanezisGuersesSurveillancePets2010.pdf>; Joan Feigenbaum et al., *Privacy Engineering for Digital Rights Management Systems*, in REVISED PAPERS FROM THE ACM CCS-8 WORKSHOP ON SECURITY AND PRIVACY IN DIGITAL RIGHTS MANAGEMENT 79 (Tomas Sander ed., 2002), available at <http://dl.acm.org/citation.cfm?id=760739>; Gürses et al., *supra* note 21; Sarah Spiekermann & Lorrie Faith Cranor, *Engineering Privacy*, 35 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 67 (2009).

that finds inspiration in the writings of Irwin Altman, a social psychologist, and Helen Nissenbaum, a philosopher of technology—both of whom analyze privacy in terms of social interaction.

Subsequently, in Part III, we offer ten case studies of Google and Facebook privacy incidents and then rely on the principles identified in Part II to discover what went wrong and what the two companies might have done differently to avoid privacy violations and consumer harms. We conclude in Part IV by considering what lessons regulators might learn from this counterfactual analysis.

II. DESIGN PRINCIPLES

A. FAIR INFORMATION PRACTICES (“FIPS”) AS THE BASIS OF DESIGN PRINCIPLES

FIPs describe the rights of individuals and the obligations of institutions associated with the transfer and use of personal data.³⁶ There are many different formulations and they vary in crucial respects.³⁷ The different versions coalesce around the following nine principles:

1. Defined limits for controllers and processors of personal information on the collection, processing, and use of personal data (often referred to as data minimization);
2. Data quality (accurate, complete, and timely information);
3. Limits on data retention;
4. Notice to individual users;
5. Individual choice or consent regarding the collection and subsequent use of personal information;
6. Reasonable security for stored data;
7. Transparent processing systems that affected users can readily understand and act on;
8. Access to one’s personal data; and
9. Enforcement of privacy rights and standards (including industry self-regulation, organizational measures implemented by individual firms, regulatory oversight and/or enforcement, and civil litigation).³⁸

36. See DANIEL J. SOLOVE & PAUL M. SCHWARTZ, *INFORMATION PRIVACY LAW* 699 (4th ed. 2010) (explaining that “personal data” generally refers to any data that relates or is linkable to an identifiable individual, including aggregations of data).

37. See Fred H. Cate, *The Failure of Fair Information Practice Principles*, in *CONSUMER PROTECTION IN THE AGE OF THE ‘INFORMATION ECONOMY’* 341, 341–53 (Jane K. Winn ed., 2006) (discussing six different versions of FIPs).

38. This formulation draws on the work of Paul Schwartz & William Treanor. See Paul M. Schwartz & William M. Treanor, *The New Privacy*, 101 *MICH. L. REV.* 2163, 2181 (2003).

FIPs have many strengths. First, FIPs are universally recognized as the foundation of international privacy law.³⁹ Second, they are open-ended and, therefore, permit data controllers to take account of all relevant factors.⁴⁰ For example, the scope and content of notices depend on a business's specific data processing practices. Similarly, data security measures must be appropriate to a company's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information it holds. Finally, FIPs are both flexible, allowing for social and technological change,⁴¹ and technology neutral, thereby permitting a wide range of solutions.⁴² While regulators on both sides of the Atlantic are busy reinterpreting or supplementing FIPs, no one rejects them outright or seriously proposes replacing them.⁴³

FIPs have two main weaknesses. First, some versions of FIPs are less comprehensive than others, which may result in a weak foundation for privacy engineering efforts.⁴⁴ Second, FIPs mainly reflect a control conception of privacy and therefore provide limited guidance on how to address privacy issues associated with Web 2.0 services in which users generate content and voluntarily share personal data about themselves and their associates.⁴⁵

39. See Rotenberg, *supra* note 11.

40. See ORG. FOR ECON. CO-OPERATION & DEV. ("OECD"), THE EVOLVING PRIVACY LANDSCAPE: 30 YEARS AFTER THE OECD PRIVACY GUIDELINES 12 (2011), available at <http://dx.doi.org/10.1787/5kgf09z90c31-en> [hereinafter OECD, EVOLVING PRIVACY LANDSCAPE] (describing the eight principles of the OECD Guidelines (which parallel FIPs) as "remarkably adaptable to the varying government and legal structures of the implementing countries and the changing social and technological environment"). For the purpose of this discussion, we frequently examine FIPs through the lens of the OECD Guidelines, which evolved out of the FIPs and share many of the same attributes. See Cate, *supra* note 37, at 346 ("Fair Information Practices . . . played a significant role in the development of the [OECD Guidelines] . . .").

41. *Id.* at 12.

42. *Id.*

43. See WP 173, *supra* note 24, § 4, at 10; FTC FINAL REPORT, *supra* note 2; see also OECD, EVOLVING PRIVACY LANDSCAPE, *supra* note 40; WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 9–22 (2012) (incorporating FIPs into a "Consumer Privacy Bill of Rights").

44. See Cate, *supra* note 37, at 355 (discussing how "the FTC first narrowed the OECD's eight principles down to five—notice, choice, access, security, and enforcement—and then later abandoned enforcement as a 'core' principle").

45. See OECD, EVOLVING PRIVACY LANDSCAPE, *supra* note 40, at 27. This is true of most Web 2.0 services, but especially of a social network service ("SNS") such as Facebook.

1. *FIPs or FIPs-Lite?*

It is the received wisdom among most privacy scholars⁴⁶ that U.S. privacy law relies on a scaled-down version of FIPs as compared to the more robust version adopted in Europe and other nations that base their national privacy laws directly on the OECD Privacy Guidelines⁴⁷ or the E.U. Data Protection Directive.⁴⁸ In the United States, both regulators and firms tend to think of FIPs primarily in terms of a notice-and-choice model of online privacy, which requires that businesses post clear and accurate privacy policies describing how they handle consumers' personal information, thereby enabling them to make informed decisions "as to whether and to what extent to disclose personal information."⁴⁹ This approach mainly emphasizes procedural requirements over substantive obligations such as fair processing, data minimization, or data quality.⁵⁰ As a result, privacy advocates often deride the U.S. version of FIPs as "FIPs-lite."⁵¹

Obviously, if privacy engineering were premised on FIPs-lite, this would severely limit its value. Under this model, firms may collect whatever data they wish to as long as they provide consumers with notice and obtain opt-

46. See Bamberger & Mulligan, *supra* note 5, at 256–57; Cate, *supra* note 37, at 353–54.

47. ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), <http://www.oecd.org/sti/interneteconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalDataBackground.htm>.

48. Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter E.U. Directive], available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf; see also Article 29 Data Protection Working Party, *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* at 2 (Dec. 1, 2009), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf (explaining "that the main principles of data protection are still valid despite the new technologies and globalisation").

49. *Fair Information Practice Principles*, FED. TRADE COMM'N (Nov. 23, 2012), <http://www.ftc.gov/reports/privacy3/fairinfo.shtm> (limiting FIPs to five core principles—“(1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress”—and stating that “the most fundamental principle is notice”).

50. See Cate, *supra* note 37, at 353.

51. See *Privacy Today: A Review of Current Issues*, PRIVACY RIGHTS CLEARINGHOUSE, <http://www.privacyrights.org/ar/Privacy-IssuesList.htm> (last visited Apr. 10, 2013); see also Bamberger & Mulligan, *supra* note 5, at 254. There are two main criticisms of FIPs-lite: first, there is overwhelming evidence that privacy notices are largely futile because so few people read or understand them properly, with the result that most individuals are unaware of the choices available to them; and second, individual choice, even if achieved, does not equate with privacy protection. See Bamberger & Mulligan, *supra* note 5, at 256–58; Cate, *supra* note 37, at 356–67.

out consent. Nothing in the FIPs-lite version obligates firms to build systems that minimize data collection and use, discard (or anonymize) personal data once it has served its purpose, ensure data quality, or provide extensive access rights.⁵²

And yet, recent developments suggest that over the past decade, U.S. privacy standards have evolved a great deal since the days of FIPs-lite. For example, in its recent enforcement actions, the FTC has begun to embrace a broader notion of privacy based on “consumer expectations.”⁵³ Indeed, the preliminary FTC staff report took issue with the notice-and-choice model quite explicitly.⁵⁴ Similarly, in identifying privacy by design as one of its three key recommendations, the FTC Final Report indicates that companies should incorporate “substantive privacy protections” into their practices such as “data security, reasonable collection limits, sound retention practices, and data accuracy.”⁵⁵ Finally, the White House framework on consumer data privacy abandons FIPs-lite entirely in favor of a new formulation of FIPs consisting of seven principles,⁵⁶ which match up quite well with both the OECD Privacy Guidelines and the E.U. Directive.

In short, the gap between the U.S. and E.U. versions of FIPs is beginning to close, although it will not close entirely until Congress enacts new privacy legislation. Unless and until they are equivalent, however, the applicable version of FIPs will make a significant difference to what it means to build FIPs into products and services. For purposes of this Article, we will discuss

52. See Bamberger & Mulligan, *supra* note 5, at 273. In comparison, Article 6 of the E.U. Directive codifies the full set of FIPs by requiring that all personal data must be processed fairly and lawfully; processed in a way strictly limited to the purpose for which such data was collected; adequate, relevant, and not excessive in relation to these purposes; accurate and up-to-date; and kept in a form that permits identification of individuals for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Article 7(a) establishes high standards for obtaining informed consent. Articles 10 and 11 set detailed, minimum transparency requirements for collecting personal data from individuals. Article 12 grants strong rights of access. Article 17 requires that confidentiality and security of processing be guaranteed. See E.U. Directive, arts. 6, 7(a), 10–12 & 17, *supra* note 48.

53. See Bamberger & Mulligan, *supra* note 5, at 284–92.

54. BUREAU OF CONSUMER PROTECTION, FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (PRELIMINARY FTC STAFF REPORT) 19–20 (2010), www.ftc.gov/os/2010/12/101201privacyreport.pdf (“Additionally, the emphasis on notice and choice alone has not sufficiently accounted for other widely recognized fair information practices, such as access, collection limitation, purpose specification, and assuring data quality and integrity.”). This report from December 2010 was largely incorporated into the FTC Final Report, published March 2012. Compare *id.*, with FTC FINAL REPORT, *supra* note 2.

55. See FTC FINAL REPORT, *supra* note 2, at 23.

56. See WHITE HOUSE, *supra* note 43, at 1, 9–22.

engineering and usability principles in the context of a robust conception of FIPs, not FIPs-lite.

2. *Privacy as Control*

Most privacy scholars also agree that at the heart of FIPs is an understanding of privacy as control over personal information. This idea is expressed in Alan Westin's canonical definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."⁵⁷ More generally, individual control underpins the protections offered by FIPs, and this cuts across any differences in national privacy laws.

The control paradigm has a major shortcoming: namely, it seems highly unsuited to address a new class of privacy risks associated with social media and Web 2.0 services. When individuals use Facebook or any other social networking service ("SNS"), they voluntarily disclose personal—and often very sensitive—information to their friends and acquaintances. Recent scholarship on social network sites rejects the view that users (especially young users) willingly share personal information because they do not care about privacy⁵⁸ in favor of a more nuanced approach based on what James Grimmelmann calls the "social dynamics" of privacy.⁵⁹ According to Grimmelmann, the reason that so many Facebook users entrust Facebook with so much personal information is that "people have *social* reasons to participate on *social* network sites, and these social motivations explain both why users value Facebook notwithstanding its well-known privacy risks and why they systematically underestimate those risks."⁶⁰

Grimmelmann's rich and detailed analysis of the social dynamics of privacy leads him to an important insight: many privacy violations on social networks are not caused by the SNS operator; rather they are peer-produced.⁶¹ For example, unwanted disclosures occur when the wrong person sees something intended for a different audience.⁶² Users create profiles that are widely available but feel violated by the "snooping" of

57. ALAN F. WESTIN, *PRIVACY AND FREEDOM* 7 (1967).

58. See Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, in *HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION* 202 (Andrea Matwyshyn ed., 2009).

59. James Grimmelmann, *Saving Facebook*, 94 *IOWA L. REV.* 1137 (2009).

60. *Id.* at 1151.

61. *Id.* at 1164 ("Users' privacy is harmed when *other users* learn sensitive personal information about them. Facebook enters the picture as catalyst; it enables privacy violations more often than it perpetrates them." (emphasis added)).

62. *Id.* at 1164–66.

college administrators, legal investigators, or potential employers.⁶³ Multiple users may tag group photos of embarrassing events but—in the sober light of day—the tagger and the subject of the tag may disagree when the latter asks the former to remove the tag.⁶⁴ And the very fact that the structure of one’s social network is visible to others may cause spillover harms in which patterns of association leak sensitive information.⁶⁵

Not surprisingly, then, Grimmelmann takes issue with any proposal to “fix” Facebook that disregards the social dynamics of privacy.⁶⁶ This includes technical controls, which are ineffective precisely because if they “get in the way of socializing, users disable and misuse them.”⁶⁷ There is an “irreconcilable tension” between *ex ante* controls and unplanned social interactions for the simple reason that privacy controls, especially if a user sets them when first registering for an account, utterly fail to capture the nuances of evolving social relationships.⁶⁸ Moreover, redistribution of information is inevitable in a social network whose very purpose is to make information accessible to others. And it is these other people who ultimately decide what to do with this shared information irrespective of any privacy controls.⁶⁹

Grimmelmann’s argument is compelling but we endorse it with two caveats. The first is to emphasize that not all privacy violations involving social network sites are peer-produced. Rather, as demonstrated by several recent regulatory investigations, many Facebook privacy incidents reflect more traditional privacy concerns such as changing privacy practices without obtaining approval from users, inadequate disclosure and lack of consent to sharing of personal information with third-party applications, insufficient user access to their personal information, and inadequate disclosure about the information made available to advertisers.⁷⁰ Granted, these are not the

63. *Id.* at 1164–68.

64. *Id.* at 1171–72.

65. *Id.* at 1174–75.

66. Grimmelmann analyzes and rejects a range of policy options all of which fail because they miss the social dynamics of privacy. *See id.* at 1178–95 (discussing market forces, privacy policies, technical controls, commercial data collection rules, user restrictions, and “data ‘ownership’”).

67. *Id.* at 1140.

68. *Id.* at 1185–86 (noting that many users do not understand or ignore Facebook’s extensive privacy controls or never modify the default privacy settings).

69. *Id.* at 1186–89.

70. *See* ELIZABETH DENHAM, OFFICE OF THE PRIVACY COMM’R OF CAN., REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (July 16, 2009),

issues that animate Grimmelmann's analysis but they are problems nonetheless, for which privacy controls may provide adequate solutions. Second, the ex ante technical controls that Grimmelmann rejects do not exhaust the range of possible design-based solutions. In Section II.B, we discuss a set of design practices that are much better suited to address the social dynamics of privacy than are technical controls premised on FIPs.

B. AN ALTERNATIVE APPROACH TO PRIVACY BY DESIGN

Software design encompasses multiple interests and expertise and hence the coordination of multiple parties, each with their own set of concerns, such as business, engineering, marketing, legal, and policy to name a few. Designing a product is also about managing risk, which has both internal sources (engineering, security, compliance) and external sources (market response, press coverage, competition).⁷¹ In a nutshell, good product design creates something the market wants while minimizing these assorted risks. As researchers in behavioral economics have pointed out, however, part of the challenge of designing products to account for privacy risks is that they are not well understood.⁷² Privacy risk management is an ongoing but still unsettled area of inquiry for international privacy regulators. For present purposes, we assume that regulators and companies alike agree that it should be incorporated into the design process. But the question is "how?" We turn, now, to the heart of this Article—saying what it means to translate privacy into design practices.

1. *Multiple Meanings of Design*

For background we will walk through a highly generalized design process. A software product or service typically begins as an idea. Through a series of brainstorming sessions, analysis of feedback, requirements, and iterations, this idea achieves some concrete form, which depends on the user goals and

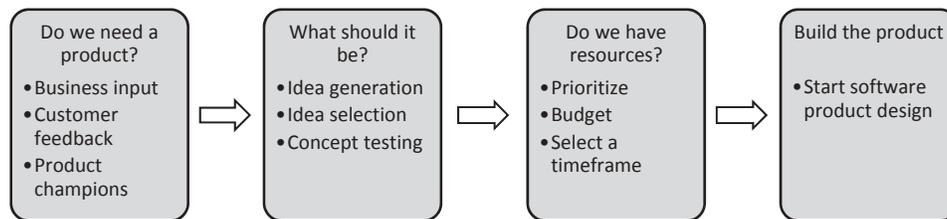
http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf; Facebook Settlement, *supra* note 25; OFFICE OF THE DATA PROT. COMM'R, FACEBOOK IRELAND LTD.: REPORT OF AUDIT, § 3.6 (Dec. 21, 2011) [hereinafter IRISH AUDIT], http://dataprotection.ie/documents/facebook_report/final_report/report.pdf.

71. See Sarah Spiekermann, *The Challenges of Privacy by Design*, 55 COMM. ACM 38 (2012).

72. For a good overview of the dichotomy of expressed privacy preferences and user actions, see Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting*, in *THE ECONOMICS OF INFORMATION SECURITY* 171 (L. Jean Camp & Stephen Lewis eds., 2004) [hereinafter Acquisti & Grossklags, *Privacy Attitudes and Privacy Behavior*]. Follow-up work in 2007 explores how behavioral economics can be used to learn about these issues. See Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, in *DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES* 364–65 (Alessandro Acquisti et al. eds., 2007).

the technical processes relied upon to realize them. Initially, these ideas exist as lists of requirements, flow diagrams, wireframes, and related concepts. They are shared with other team members who build out the software design, decide how they are going to define and solve problems, and begin coding the actual product. Figure 1 illustrates this process. This conceptualization phase may seem trivial, but it is an important step in the process, as it motivates the overall way the product will work. This process includes determining the look and feel, the functional requirements, the product goals, and the software architecture of the final product. In some cases, more time is spent on the idea phase than on actual software development. And from a “privacy by design” perspective, influencing the conceptualization phase is essential to ensuring that privacy concepts are taken into account throughout the product development cycle.⁷³

Figure 1: High Level Overview of Product Conceptualization



After completing the conceptual phase and deciding to build a product, the next phase consists of “design.” The elements of design vary widely by project and timeframe. Factors that typically influence design include the maturity of a company, the motivation behind the design task (i.e., building a new product or updating an existing one), the intended audience, available resources, and so on.⁷⁴ Software development methodologies also vary with the nature of the product and constantly evolve.⁷⁵ For example, software built for an enterprise may have longer development cycles and use the “waterfall” model, which follows design stages in order (requirements,

73. This is central to Cavoukian’s thinking. See CAVOUKIAN, *supra* note 13; see also Spiekermann, *supra* note 71.

74. See Michael Keeling, *Choosing a Software Design Strategy*, REFLECTIONS ON SOFTWARE ENG’G (Aug. 2, 2010), <http://neverletdown.net/2010/08/choosing-a-software-design-strategy>.

75. See, e.g., FREDERICK BROOKS, *THE MYTHICAL MAN MONTH: ESSAYS ON SOFTWARE ENGINEERING* 7–8 (2d ed. 1995) (describing the ongoing evolution of software development and the difficulty of predicting or increasing the pace and quality of software development).

design, implementation, testing, release).⁷⁶ Software developed by a startup or for fast-moving Internet markets is more likely to rely on the “agile” development processes, which allows small teams to make changes very quickly and measures iterations in days or hours, rather than years or months.⁷⁷ Not surprisingly, waterfall or similar top-down approaches are well suited for regulatory compliance (including security and privacy requirements), whereas most agile and lightweight development approaches tend to be more feature-focused. Consequently, the latter methodologies tend to overlook security and privacy requirements at the outset and address them only over the course of several iterations—and sometimes neglect them entirely.⁷⁸

Regardless of which methodology is appropriate to a given project, most programmers have come to rely on a host of software toolkits to assist them with the complex tasks associated with coding and testing software. As software has become more modular, programmers also borrow freely from code libraries, with the overall result that much of the code a programmer uses to build a product or service originates with a variety of third parties. Additionally, business and marketing managers, lawyers, and other non-engineers are now heavily involved in the design of software. Most importantly for present purposes, the growing needs and demands of consumers have encouraged software developers to pay far more attention to the applied art and science of user experience (“UX”) design in order to improve the aesthetics, ergonomics, and usability of a product. Thus, a software development team for a popular Web 2.0 service would now typically include industrial designers, graphic artists, visual designers, and usability experts.

76. The waterfall method is one of the oldest in software engineering and is covered in standard textbooks. For a good description, see *Software Process Models*, TARGET: THE SOFTWARE EXPERTS, http://www.the-software-experts.de/e_dta-sw-process.htm (last visited July 23, 2012). This approach emphasizes advance planning but tends to be inflexible in the face of evolving requirements. *Id.*

77. The agile method was first mentioned in the *Manifesto for Agile Software Development*, <http://agilemanifesto.org/> (last visited July 23, 2012), as a way to describe an emerging trend in rapid iterative software development. It has since become very popular, especially among start-ups, and has spawned a very large literature.

78. See MICROSOFT, SECURITY DEVELOPMENT LIFECYCLE FOR AGILE DEVELOPMENT (June 30, 2009), http://www.blackhat.com/presentations/bh-dc-10/Sullivan_Bryan/BlackHat-DC-2010-Sullivan-SDL-Agile-wp.pdf (defining a way to embrace lightweight software security practices when using Agile software development methods).

a) Front-End Versus Back-End Design: The New Challenges of Designing for Privacy

The design of systems that meet privacy requirements as described in the FIPs has traditionally relied on back-end implementations and system protections, which have largely been the domain of security engineers and legal teams. In fact, some consider privacy design not an engineering discipline at all but merely an adjunct of security engineering “used to ensure that privacy rights are protected to the extent specified by law and organizational policy.”⁷⁹ We reject this position for two reasons.

First, privacy engineering is an emerging discipline with its own structure and topics, and it is not reducible to security engineering.⁸⁰ Second, not all privacy concerns are resolvable by reference to the FIPs or use of associated security-based controls. Several of the privacy incidents that arise in the Google and Facebook case studies illustrate this emerging trend.⁸¹ They are not the result of failures in back-end security engineering but rather nuanced violations of users’ perceptions of privacy and of their choices regarding the *context* in which to share and post personal information.⁸²

These developments in turn raise an interesting and still-unanswered question: Which part of an organization should be responsible for designing in privacy and addressing these context-based requirements? More importantly, how should we define these requirements or measure them for engineering purposes? In what follows, we offer some preliminary answers to these questions but for the moment merely wish to emphasize the importance of including UX designers in the conversations on privacy and product design.⁸³ We maintain that UX designers should have a strong role in defining privacy requirements. By working closely with legal and security engineers early on in the development and design process, they help ensure that privacy expectations as understood by end users are taken into account in a nuanced way.

79. DEBRA S. HERRMANN, A COMPLETE GUIDE TO SECURITY AND PRIVACY METRICS: MEASURING REGULATORY COMPLIANCE, OPERATIONAL RESILIENCE AND ROI 523 (2007).

80. See Spiekermann & Cranor, *supra* note 35, at 67–68.

81. See *infra* Part III.

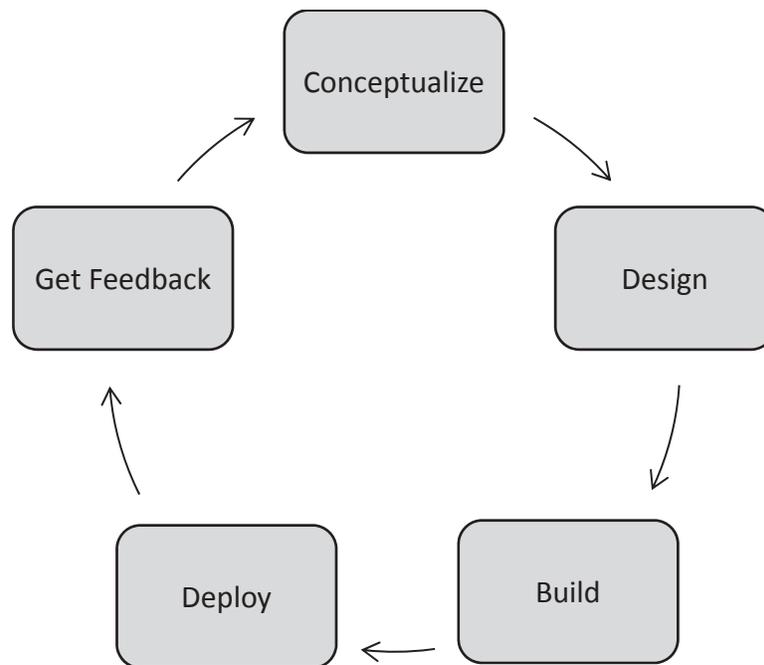
82. For an overview of Nissenbaum’s theory of privacy as contextual integrity, see *infra* notes 204–17 and accompanying text.

83. On the value of incorporating HCI factors into privacy by design, see Deirdre Mulligan & Jennifer King, *Bridging the Gap Between Privacy and Design*, 14 U. PA. J. CONST. L. 989, 1019–26 (2012).

b) Putting Design into Privacy by Design

The most reliable way to incorporate privacy design into product development is to include privacy considerations in the definition of software “requirements” or specifications. This “roadmap” or product blueprint typically guides the creation of a software product, codifying what needs to be implemented as part of the product iteration, whether it is a short sprint or a longer term multi-phase development cycle, as depicted in Figure 2. If the privacy concerns are addressed by the FIPs, defining and implementing the relevant requirements are fairly straightforward tasks, and may even lend themselves to engineering metrics.⁸⁴

Figure 2: A Schema for Software Development



In many of the cases discussed below, however, the privacy concerns have less to do with FIPs than with the social dynamics of privacy, which makes defining software requirements a fuzzier and hence more difficult task. Whereas legal teams play a significant role in advising development

84. For example, measurements can track how long a search engine stores personal data and whether it is deleted in a timely fashion in accordance with applicable legal requirements or corporate privacy guidelines. For a discussion of data retention issues, see *infra* notes 132–38 and accompanying text.

teams on how to implement the FIPs, UX designers are much better suited than lawyers at interpreting HCI requirements (and they contribute to back-end design tasks as well).⁸⁵ For example, a startup may want to implement functionality for requesting access to a user's address book or contact list for use with a mobile service. A UX designer would respond by researching consumer expectations about the use of such private data in a mobile application and develop insights about what approaches work best to balance competing goals such as transparency and a high rate of user interest and acceptance. UX designers perform these tasks in tandem with engineering teams and business managers and play an increasingly important role in developing consumer software, making them highly sought after by top companies.⁸⁶

In what follows, we flesh out the meaning of “privacy by design” by separately discussing privacy engineering and usable privacy design. This is mainly an expository convenience and does not necessarily reflect the nature or goals of the software development process, which ideally incorporates both engineering and design in a unified manner. Another reason to discuss engineering principles separately from design principles is that they take their inspiration from different sources and have been explored in different research literatures.

2. *Privacy Engineering*

a) Background

We suggested earlier that privacy by design requires a translation of FIPs into engineering principles. Ten years ago, Joan Feigenbaum and her colleagues attempted to do just that for digital rights management (“DRM”) systems.⁸⁷ Their paper argues that blind signatures, zero knowledge proofs, selective disclosure of credentials, and other sophisticated cryptographic protocols that form the basis of most PETs have not solved the privacy

85. Policy makers have been hesitant to make specific design recommendations because they lack the relevant expertise and are wary of stifling innovation. In the absence of any legally enforceable design principles analogous to the FIPs, designers have considerable leeway in determining best practices. FTC decisions generally support this flexible approach, as long as a user interface is not “unfair or deceptive” and users are given “clear and prominent notice.” *See* F.T.C. v. Frostwire LLC, No. 1:11-CV-23643-DLG at 9, 11 (S.D. Fla. 2011), <http://www.ftc.gov/os/caselist/1123041/111012frostwirestip.pdf>.

86. *See* Lance Whitney, *Facebook Hires Former Apple Design Manager*, CNET (June 22, 2012), http://news.cnet.com/8301-1023_3-57458870-93/facebook-hires-former-apple-design-manager.

87. *See* Feigenbaum et al., *supra* note 35. We use the term “privacy engineering” partly because it suggests the entire range of software engineering and design techniques as applied to the protection of personal data and partly because it overlaps with many aspects of better-known security engineering practices.

problems raised by DRM.⁸⁸ Indeed, they reject cryptographic PETs—citing a number of shortcomings that we believe remain true today⁸⁹—and instead put forward the thesis that if DRM were “properly designed, implemented, and used,” it could provide “reasonable user-privacy protection and simultaneously supply businesses with information necessary for their basic functionality at a fair cost.”⁹⁰

This is the approach we adopt here. Before developing our own set of privacy engineering principles, however, we need to clarify two points. The first is that the privacy research community has by no means abandoned PETs based on cryptographic protocols.⁹¹ Indeed, a recent and important paper by Seda Gürses et al. strongly reaffirms the cryptographic approach.⁹² We have no quarrel with this analysis or with the attempt to generalize the lessons learned from them. Rather, we reject the binary choice of Gürses et al. (strong cryptography or no privacy) in favor of the more nuanced analysis of Feigenbaum et al., which concludes that in spite of the apparent profusion of cryptographic technologies, few are in widespread use and even if they were, they would not necessarily overcome the technical and economic barriers blocking their deployment.⁹³ In fact, exposure of sensitive information remains a problem even when systems utilize encryption techniques.⁹⁴ That said, we also agree with the view of Feigenbaum et al. that

88. For a review of these technologies as of 2002, see IAN GOLDBERG, PRIVACY-ENHANCING TECHNOLOGIES FOR THE INTERNET, II: FIVE YEARS LATER pt. 3, at 4–7 (2002), available at <http://www.cypherpunks.ca/~iang/pubs/pet2.pdf>.

89. Feigenbaum et al., *supra* note 35, at 82–88 (citing both technical issues such as overdependence on abstract models as opposed to real-world uses, insecure implementations, ease-of-use issues, difficulties integrating PETs with legacy systems, and excessive technical costs; and a variety of economic issues).

90. *Id.* at 78 (citations omitted).

91. For a review of contemporary privacy technology, see Danezis & Gürses, *supra* note 35.

92. See Gürses et al., *supra* note 21, § 2.2 (arguing that data minimization with strong, technical guarantees “must be the foundational principle in applying privacy by design” to systems that collect data in massive databases).

93. Compare *id.*, with Feigenbaum et al., *supra* note 35, at 81–88. While cryptographic techniques might find their way into government-managed systems, there is little evidence that businesses will adopt them absent much stronger incentives or a government mandate as in the *Proposed E.U. Regulation*. See Rubinstein, *supra* note 1, at 1431–44.

94. See Nathaniel Good & Aaron Kreckelberg, *Usability and Privacy: A Study of KaZaA P2P File Sharing*, in SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 651, 652–53 (Lorrie Faith Cranor & Simon Garfinkel eds., 2005) [hereinafter SECURITY AND USABILITY] (discussing inadvertent sharing of personal information in P2P software as an early example of usability issues resulting in loss of private information). For a more recent incident in which address books were uploaded over a secure channel but without users’ consent, see Joshua Topolsky, *Privacy Controversy over Path for iPhone, iPad Should*

even if cryptography cannot by itself solve the privacy problems raised by businesses collecting, storing, and sharing data and using it for profitable purposes, “it *can* play a role in various solutions.”⁹⁵

The second point we need to clarify is that the term “privacy engineering” encompasses not only the work of Feigenbaum et al. but also a variety of other approaches.⁹⁶ These include the analysis of data minimization of Gürses et al.,⁹⁷ in addition to works on requirements engineering,⁹⁸ privacy policy languages and user preference tools,⁹⁹ privacy-aware access controls,¹⁰⁰ privacy rights management,¹⁰¹ identity management,¹⁰² and privacy threat modeling.¹⁰³ In what follows, we give no or only passing mention to most of these alternatives, not because they lack value but rather because the FIPs-based approach of Feigenbaum et al., supplemented by the “architectural” approach of Spiekermann and Cranor,¹⁰⁴ better suit our purposes.

Be a Wake-Up Call, WASH. POST (Feb. 15, 2012), http://www.washingtonpost.com/business/technology/privacy-controversy-over-path-for-iphone-ipad-should-be-a-wake-up-call/2012/02/15/gIQA8oHVGR_story.html (“[W]hen you logged into the app on an Apple iOS device—an iPhone or iPad—it automatically uploaded your entire address book to its servers. Without asking.”).

95. Feigenbaum et al., *supra* note 35, at 76 (emphasis added).

96. See Paolo Guarda & Nicola Zannone, *Towards the Development of Privacy-Aware Systems*, 51 INFO. & SOFTWARE TECH. 337 (2009).

97. See *supra* note 92 and accompanying text.

98. See Travis D. Breaux & Annie I. Antón, *Analyzing Regulatory Rules for Privacy and Security Requirements*, 34 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 5 (2008) (describing formal methods for extracting descriptions of rules from the policies and regulations that govern stakeholder actions).

99. See *infra* notes 146–52 and accompanying text (discussing P3P).

100. See Guarda & Zannone, *supra* note 96, at 343.

101. See Larry Korba & Steve Kenny, *Towards Meeting the Privacy Challenge: Adapting DRM* (Nat’l Research Council of Can., Paper No. 44,956, 2002), <http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf>.

102. See generally DIGITAL PRIVACY: PRIME—PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE (Jan Camenisch et al. eds., 2011).

103. See M. Deng et al., *A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements*, 16 REQUIREMENTS ENGINEERING 3 (2011) (describing a threat modeling approach that maps privacy threats to elements in a system model and identifies countermeasures based on existing PETs).

104. See Spiekermann & Cranor, *supra* note 35, at 67 (distinguishing “architecture” from “policy” and suggesting that if a firm implements a privacy architecture, it should be exempted from providing notice and choice). We reject this sharp distinction, which stems, in part, from thinking of policy in terms of FIPs-lite. Instead, we rely on a more robust version of FIPs, and argue that the FIPs-based approach to privacy engineering described here bridges the gap between architecture and policy.

b) FIPs-Based Privacy Engineering

We organize the following discussion around the FIPs. Not all of the FIPs are equally relevant; hence, we focus especially on data avoidance and minimization, data retention limits, transparency, individual choice and access, and accountability.¹⁰⁵ As a preliminary matter, FIPs only apply to personally identifiable information (“PII”). Although there is no uniform definition of PII,¹⁰⁶ privacy laws “all share the same basic assumption—that in the absence of PII, there is no privacy harm.”¹⁰⁷ It follows that the two most basic privacy engineering principles are protecting PII against unauthorized access and limiting the linkability of data to personal identifiers. This may entail encrypting PII in transit and in storage and/or the use of anonymity services that delink users from all traces of their online activity,¹⁰⁸ or of user-centric identity management systems that enable anonymous or pseudonymous credentials.¹⁰⁹ Other techniques for limiting linkability are better characterized as data avoidance or minimization techniques. These include not recording IP addresses and/or not enabling User ID cookies, or using a third party proxy server to strip out an IP address; and a variety of techniques that protect, shield, and minimize location data,¹¹⁰ from which identity is readily inferred.

In practice, few companies build services that implement these techniques, and those that do labor in obscurity. Rather, most companies treat privacy (like security) as primarily a compliance task best left to lawyers, not product developers.¹¹¹ As a result, the vast majority of Internet services collect information about web activity and link it to IP addresses or other identifiers.¹¹² Of course, consumer advocates encourage users to rely on a

105. Security also belongs on this list but we omit it here because the topic requires a separate paper of which there are many.

106. See SOLOVE & SCHWARTZ, *supra* note 36, at 1828–36 (identifying three approaches to defining PII).

107. *Id.* at 1816. Although Schwartz and Solove limit this observation to U.S. privacy law, it holds true for E.U. data protection law as well. See *id.*

108. This can be done, for example, by using proxies or “mix” systems that shield or hide a user’s IP address and other identifiers. See Danezis & Gürses, *supra* note 35, at 2–3.

109. *Id.* at 5–6.

110. See KIM CAMERON & ANN CAVOUKIAN, WI-FI POSITIONING SYSTEMS: BEWARE OF UNINTENDED CONSEQUENCES 16 (June 2011), <http://www.ipc.on.ca/images/Resources/wi-fi.pdf> (identifying techniques such as “location fuzzing or obfuscation, ambient notices, two-way communication for privacy notices and consent, user-generated identifiers, substitution of MAC addresses, cloaking, changing identifiers in mix zones, etc.” (citations omitted)).

111. See Spiekermann, *supra* note 71.

112. *Id.*

variety of self-help strategies that would prevent companies from associating their browsing activity with identifiers or linking their browsing activity across different websites.¹¹³ But our focus here is not on what *users* can do to defeat privacy invasions, but on what *companies* can do to build privacy protections into their own systems by implementing privacy engineering principles. It follows that these self-help strategies are outside the scope of this Article and that where we discuss anonymization techniques, we will do so under the broader heading of data avoidance and minimization.

c) Data Avoidance and Minimization

Data avoidance and minimization are central tenets of the FIPs, the E.U. Directive, and certain U.S. privacy laws and play a key role in the work of Feigenbaum et al. as well. For example, she recommends that DRM systems enable users to “easily configure the system to accommodate their preferred information-collection and handling procedures,” which she refers to as “customizable privacy.”¹¹⁴ In order for configurable systems to support data minimization, however, they must by default be set to avoid or minimize the collection of PII, which in turn requires that engineers analyze information needs and flows at the outset of any design project, and consider techniques for disassociating functionality that requires PII (e.g., paying for music or movies with a credit card) from activation, recommendation services, and other functionality, for which pseudonyms should suffice. As Feigenbaum et al. points out, this also requires that businesses determine at the outset which information is necessary for different business practices and whenever possible build systems that achieve business purposes without collecting PII.¹¹⁵ It also requires serious attention to database architecture and management. “Data may be segmented,” Feigenbaum et al. suggest, “according to the different groups that are interested in it—a principle of *split databases* and *separation of duty*.”¹¹⁶

113. See, e.g., *EPIC Online Guide to Practical Privacy Tools*, ELEC. PRIVACY INFO. CTR. (EPIC), <http://epic.org/privacy/tools.html> (last visited Feb. 27, 2013) (describing various ways to enhance personal privacy online).

114. Feigenbaum et al., *supra* note 35, at 91.

115. *Id.* at 16–17; cf. Gürses et al., *supra* note 21, § 3.1 (discussing the use of advanced cryptographic protocols to minimize data collection and maintain anonymity).

116. Feigenbaum et al., *supra* note 35, at 92 (discussing, for example, separating accounting and customer service data requirements from those of marketing and risk management). For a similar approach, see MICROSOFT, MICROSOFT’S PRIVACY PRINCIPLES FOR LIVE SEARCH AND ONLINE AD TARGETING (July 2007), <http://www.reallyfirst.com/ad-targeting/microsofts-privacy-principles-for-live-search-and-online-ad-targeting.shtml> (“We will store our Live Search service search terms separately from account information

Spiekermann and Cranor offer the most comprehensive discussion of the importance of architectural choices to privacy engineering.¹¹⁷ They argue that “engineers typically can make architectural choices on two dimensions: network centrality and identifiability of data.”¹¹⁸ Network centrality refers to “the degree to which a user’s system relies on a network infrastructure to provide a service, as well as the degree of control a network operator can exercise over a client’s operations.”¹¹⁹ The extent of privacy protection lies on a continuum between network-centric systems and client-centric systems. Not surprisingly, businesses prefer network-centric architectures, which gives them much greater control over how their systems work, and competitive advantages if they can design a better system than others. Unfortunately, privacy risks are also greater with network-centric systems (which must collect and store personal data in providing a service to users). In contrast, privacy problems on client-centric systems are greatly reduced because these systems have less or no need to transfer personal data to a web server, thereby eliminating data retention issues and/or unwanted secondary use.¹²⁰

User identifiability refers to “the degree to which data can be directly attributed to an individual.”¹²¹ The authors note that many service providers are already familiar with this approach to reducing privacy concerns and offer their users pseudonymous access to their services. But pseudonyms alone are insufficient because they allow service providers to reidentify users.¹²² This occurs in either of two ways: the service combines a user’s pseudonymous profile with PII stored in a billing or shipping database (i.e., it fails to follow the principle of Feigenbaum et al. of split databases and separation of duty),¹²³ or the service applies data mining techniques to pseudonymous

that personally and directly identifies the user, such as name, email address, or phone numbers . . .”).

117. Spiekermann & Cranor, *supra* note 35.

118. *Id.* at 74.

119. *Id.*

120. *Id.* Spiekermann and Cranor offer two examples: a collaborative filtering system (for use in various recommendation services) in which users have control over and access to all data recorded about their preferences, and a location-based service enabling smart phones and other clients to calculate their own positions without having to share location-information with a central server. *Id.*; see also Mikhail Bilenko et al., Targeted, Not Tracked: Client-Side Solutions for Privacy-Friendly Behavioral Advertising (Sep. 25, 2011) (Telecommunications Policy Research Conference Accepted Paper Series), <http://petsymposium.org/2011/papers/hotpets11-final3Bilenko.pdf> (discussing “methods that facilitate behavioral targeting while providing consumer privacy protections”).

121. Spiekermann & Cranor, *supra* note 35, at 74.

122. *Id.* at 75.

123. See *supra* note 116 and accompanying text.

transaction logs or otherwise links user data to personal identifiers by pattern matching.¹²⁴

Arguing that “the degree of privacy friendliness of a system is inversely related to the degree of user data identifiability,” the authors discuss concrete steps that engineers can take to specify the degree of user identifiability in a given system.¹²⁵ They describe four privacy stages and their corresponding system characteristics as illustrated in their framework for privacy-friendly system design. At one end of the spectrum, Stage 0, privacy is limited and identifiability is easy because systems utilize unique identifiers across databases and store contact information with profile information, thus linking data to personal identifiers. Stage 1 provides a minimal degree of privacy by eliminating unique identifiers and common attributes across databases while storing contact information separately from profile or transaction information (which is stored under a pseudonym).¹²⁶ But reidentification of users is still possible with a reasonable effort (as in the AOL case)¹²⁷ and may even be automated, rendering it cost effective.¹²⁸

At the other end of the spectrum, Stage 2 systems are “actively designed for non-identifiability of users” and thereby achieve what the authors denote as “privacy-by-architecture.” These systems have all of the characteristics of Stage 1 but also take steps to generate identifiers randomly to prevent future databases from reintroducing common identifiers and endeavor to collect long-term personal characteristics at a low level of granularity (e.g., year of birth where possible rather than date of birth).¹²⁹ Even if these steps are taken, however, data-mining techniques may still be used to reidentify a user based on comparisons of an anonymous database and a subset of similar, identified data, although such linking attempts would require a relatively high level of effort compared with Stage 1.¹³⁰ Thus, the coauthors also describe

124. Spiekermann & Cranor, *supra* note 35, at 75.

125. *Id.*

126. *Id.* at 76.

127. *See infra* note 249 and accompanying text; *see also* Complaint, Myspace LLC, F.T.C. No. 102-3058 (May 8, 2012), *available at* <http://ftc.gov/os/caselist/1023058/120508myspacecmpt.pdf> (charging MySpace with misrepresenting whether advertisers could link user IDs to their broader web-browsing activities).

128. As a result, Stage 1 systems must be supplemented by policies that prohibit or restrict reidentification and give users adequate notice of these policies and other steps they might take to protect their privacy. *See* Spiekermann & Cranor, *supra* note 35, at 75–76.

129. *Id.* at 76.

130. *See* Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, in PROCEEDINGS OF 29TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111 (2008), *available at* <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4531148> (discussing successful efforts at reidentifying

Stage 3, in which privacy is very well protected and users remain anonymous, either because there is no collection of contact information or of long-term personal characteristics, or profiles are deleted and anonymized via more sophisticated techniques.¹³¹

d) Data Retention Limits

As noted above, Article 6(1)(e) of the Directive specifically limits the period of time a controller may retain identifiable data to a period “no longer than is necessary” for the purposes for which they were collected or processed.¹³² Consequently, this implies that data must be erased or de-identified as soon as they are no longer needed. Both in Europe and the United States, questions over the appropriate length of retention periods and the technique used for anonymization or de-identification play out mainly in the context of search engines and targeted advertising,¹³³ and, more recently, SNSs.¹³⁴ Feigenbaum et al. argues that the practice of data erasure should be addressed in the context of database architecture and management and recommends that the PII can and should be removed from usage records on

some poorly anonymized data records of Netflix movie rankings by comparing this data with public, identifiable information in the Internet Movie Database, IMDB, <http://www.imdb.com> (last visited Mar. 25, 2013)).

131. See Spiekermann & Cranor, *supra* note 35, at 76 (noting that stage 2 “does not guarantee unlinkability; rather, it ensures that the process of linking a pseudonym to an individual will require an extremely large effort”). For the ongoing debate over the effectiveness of even the most sophisticated anonymization techniques, compare Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (arguing that anonymization fails to protect privacy due to the threat of reidentification of anonymized data sets), with Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J. LAW & TECH. 1 (2011) (arguing that properly de-identified data is not only safe, but has high social utility). Cf. Felix T. Wu, *Privacy and Utility in Data Sets*, U. COLO. L. REV. (forthcoming 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031808 (staking out a middle ground and explaining that the debate over anonymization turns on society’s goals for privacy and utility in specific contexts).

132. See *supra* note 52.

133. This debate included security experts objecting to the weak anonymization techniques relied on by certain firms. See, e.g., Chris Soghoian, *Debunking Google’s Log Anonymization Propaganda*, CNET (Sep. 11, 2008), http://news.cnet.com/8301-13739_3-10038963-46.html. Soghoian took issue with Google’s method of removing the last eight bits in the IP address and changing the cookie information by pointing out that:

Since each octet (the numbers between each period of an IP) can contain values from 1–255, Google’s anonymization technique allows a user, at most, to hide among 254 other computers. In comparison, Microsoft deletes the cookies, the full IP address and any other identifiable user information from its search logs after 18 months.

Id.

134. See *supra* note 70.

a massive scale, “before those records are inserted into a long-lived data warehouse.”¹³⁵ Spiekermann and Cranor’s privacy framework takes account of recent developments in pattern matching techniques¹³⁶ but shifts the debate from how to reduce the risks of reidentification to how to design systems that avoid identification of users in the first place.¹³⁷ As to data retention limits, they recommend not only the deletion of PII after its purpose has been fulfilled but also the “purging [of] nonidentified data as well, to minimize the risk of reidentification based on pattern matching.”¹³⁸

e) Notice, Choice, and Access

We have already rehearsed the limits of the notice-and-choice model, but the fact remains that whatever their shortcomings as a standalone privacy strategy, notice and choice, together with access, are not going away.¹³⁹ Despite the serious design challenges presented by this model, this section very briefly considers a few design options.

Most commentators agree that adequate notice must be understandable, timely, and widely disseminated (not only to consumers but also to other systems that must respect the assumptions under which consumers make privacy decisions).¹⁴⁰ The Microsoft Privacy Guidelines contain a useful discussion of different types of notice¹⁴¹ and different notice mechanisms.¹⁴² This guidance remains highly relevant today, especially in light of the recent controversies over Google’s decision to consolidate its many separate privacy

135. Feigenbaum et al., *supra* note 35, at 93.

136. See Narayanan & Shmatikov, *supra* note 130.

137. See Spiekermann & Cranor, *supra* note 35, at 76. Spiekermann and Cranor wrote:

Separate databases for profile and contact information must be created in such a way that common attributes are avoided. In addition, steps should be taken to prevent future databases from reintroducing common identifiers. Identifiers should therefore be generated at random and any information that is highly specific to an individual (e.g., birth dates or contact data) should be avoided whenever possible.

Id.

138. *Id.*

139. For example, notice, choice, and access remain central to both the Proposed E.U. Regulation and the White House’s proposed Consumer Privacy Bill of Rights. See *Proposed E.U. Regulation*, *supra* note 2; WHITE HOUSE, *supra* note 43.

140. See Feigenbaum et al., *supra* note 35, at 93; Spiekermann & Cranor, *supra* note 35, at 77–79.

141. See *Microsoft Privacy Guidelines*, *supra* note 27, § 1.3.1 (distinguishing prominent notice, discoverable notice, and layered notice).

142. *Id.* § 1.4 (distinguishing just-in-time notice, first-run notice, installation-time notice, and “out of the box” notice).

policies into a single, comprehensive policy.¹⁴³ There is a large literature on how to improve privacy policies, describing a number of different approaches.¹⁴⁴ Here we distinguish and briefly discuss both an engineering approach, which relies on the Platform for Privacy Preferences (“P3P”) standard for specifying and handling privacy policies in an automated and integrated fashion, and a usability approach, which seeks to redesign cookie handling in browsers based on a model of informed consent.¹⁴⁵

P3P is the oldest and best-known specification of privacy policies.¹⁴⁶ This W3C standard enables websites and services to encode their privacy practices in machine-readable XML format and allows user agents “to make automated privacy choices based on a user’s stored privacy preferences.”¹⁴⁷ In practice, P3P has been sharply criticized on technical, legal, and policy grounds.¹⁴⁸ It also has difficult user interface problems.¹⁴⁹ Microsoft’s adoption of the P3P framework in Internet Explorer (“IE”) has very broad reach but limits P3P functionality to merely signaling whether a website meets a user’s cookie preferences; even so, few users are likely even to be aware of the “Privacy Report” icon on the IE status bar.¹⁵⁰ In contrast, more robust P3P implementations, such as Privacy Bird, have a very small audience.¹⁵¹ In short, P3P has yet to fulfill its supposed potential, although research and experimentation continues with P3P-based privacy tools.¹⁵²

In 2000, a group of researchers developed a model of informed consent for information systems based on six components: disclosure, comprehension,

143. See *infra* notes 320–37 and accompanying text.

144. Much of this literature originates at the Carnegie Mellon CyLab, in the work of Lorrie Cranor and her colleagues. CYLAB, CARNEGIE MELLON UNIV., <http://www.cylab.cmu.edu/index.html> (last visited Feb. 27, 2013).

145. See LORRIE CRANOR ET AL., THE PLATFORM FOR PRIVACY PREFERENCES 1.0 (P3P1.0) SPECIFICATION, W3C RECOMMENDATION (Apr. 16, 2002), <http://www.w3.org/TR/P3P>.

146. *Id.*

147. See Spiekermann & Cranor, *supra* note 35, at 78 (citations omitted).

148. For technical issues, see Guarda & Zannone, *supra* note 96, at 342–43. For legal and policy issues, see William McGeeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U. L. REV. 1812 (2001).

149. See Mark S. Ackerman, *The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility* 15 HUM.-COMPUTER INTERACTION 179, 184–87 (2000).

150. See Tom Spring, *First Look at Microsoft IE 6.0*, PCWORLD (Aug. 28, 2001), <http://www.pcworld.com/article/59928/article.html> (describing the implementation of P3P into Microsoft’s IE and noting some of the privacy concerns of privacy advocates).

151. PRIVACY BIRD, <http://www.privacybird.org> (last visited Mar. 17, 2013).

152. See Aleecia M. McDonald, et al., *A Comparative Study of Online Privacy Policies and Formats*, in PRIVACY ENHANCING TECHNOLOGIES: 9TH INTERNATIONAL SYMPOSIUM, PETS 2009, SEATTLE, WA, USA, AUGUST 5–7 2009, PROCEEDINGS 37 (Ian Goldberg & Mikhail Atallah, eds., 2009).

voluntariness, competence, agreement, and minimal distraction.¹⁵³ In subsequent papers, they explored how cookie technology and web browser design have responded to concerns over informed consent and found significant design problems, which they sought to remedy through the development of new technical mechanisms for cookie management using a value-sensitive design methodology.¹⁵⁴ A later paper reviews the design possibilities for implementing informed consent not only in web browsers but also in other widely deployed technologies, such as secure web connections and a web email service, and proposed ten design principles.¹⁵⁵ Interestingly, these principles overlap to some extent with Cavoukian's emphasis on proactive design and attention to default,¹⁵⁶ while also raising classic HCI concerns such as the system interactions with both direct and indirect stakeholders, the use of icons that support an accurate mental model of information flows, and extensive field testing to validate and refine initial designs.¹⁵⁷ Unfortunately, few companies follow this approach in developing their information and computer systems.

Finally, turning to access, it is now commonplace for both e-commerce and Web 2.0 services to provide users with direct online access to their PII by means of a password-protected account. The scope of access varies with the service but may include the ability to view or edit user profiles, billing and account information, and privacy settings, as well as data sharing and communications preferences. For example, Google allows users to review data associated with their Google Accounts via Dashboard and to remove or edit their interests and inferred demographics associated with their cookies via Ads Preferences.¹⁵⁸ Additionally, when Facebook was inundated with over 40,000 access requests from European users within a period of weeks, it quickly developed technical means to expand the range of data it made

153. See BATYA FRIEDMAN ET AL., INFORMED CONSENT ONLINE: A CONCEPTUAL MODEL AND DESIGN PRINCIPLES 1–4 (2000), available at <ftp://ftp.cs.washington.edu/tr/2000/12/UW-CSE-00-12-02.pdf>.

154. See LYNETTE I. MILLETT ET AL., COOKIES AND WEB BROWSER DESIGN: TOWARD REALIZING INFORMED CONSENT ONLINE 7–8 (2001), available at <ftp://ftp.cs.washington.edu/tr/2000/12/UW-CSE-00-12-03.pdf>; Batya Friedman, et al., *Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design*, in PROCEEDINGS OF THE THIRTY-FIFTH HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (IEEE 2002), <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=994366>.

155. See Batya Friedman et al., *Informed Consent by Design*, in SECURITY AND USABILITY 495.

156. See CAVOUKIAN, *supra* note 13.

157. See Friedman et al., *supra* note 155.

158. See Dennis O'Reilly, *How to Prevent Google from Tracking You*, CNET (Jan. 30, 2012, 12:57 PM), http://howto.cnet.com/8301-11310_39-57368016-285/how-to-prevent-google-from-tracking-you.

available via a user's activity log profiles, a user-accessible database, and a new download tool.¹⁵⁹

f) Accountability

We noted previously that many regulators think of privacy by design as one way of achieving accountability, defined as data governance by organizations for the purpose of demonstrating compliance with FIPs.¹⁶⁰ Here we observe that companies may also adopt technical measures to audit and enforce their data privacy practices. Both Feigenbaum et al., and Spiekermann and Cranor, make this point: the former favor a combination of privacy notices and audits but emphasize that effective auditing requires stronger tools,¹⁶¹ while the latter identify some new tools that help automate the evaluation of data access requests according to a set of privacy rules.¹⁶² Both recognize that even if such accountability measures control who can access PII for legitimate purposes, they cannot control whether such data will be misused once accessed. In other words, auditing offers no cryptographic guarantees of privacy, but it does provide practical solutions that are both familiar and cost-effective.¹⁶³ Auditing can also “help[] protect against unintentional privacy violations” and assist management in determining “who may be responsible should a breach occur.”¹⁶⁴

3. *Designing for Privacy: A UX Approach*

a) Background

As distinct from translating FIPs into engineering principles and practices, a complementary approach consists of embedding privacy into UX design processes, which generally handle both usability and visual and aesthetic design. Design, of course, is a discipline unto itself, with strong roots in the creative arts, and it plays an important role in today's modern engineering practice. Apple is often cited as a proponent of excellence in the design of consumer goods, and its enormously popular devices and software systems seem to confirm the wisdom of obsessive attention to design details.¹⁶⁵ Furthermore, Apple's success tends to support the notion that a

159. See IRISH AUDIT, *supra* note 70, at 63–68.

160. See *supra* note 24 and accompanying text.

161. See Feigenbaum et al., *supra* note 35, at 96.

162. See Spiekermann & Cranor, *supra* note 35, at 79.

163. See Feigenbaum et al., *supra* note 35, at 96–97.

164. Spiekermann & Cranor, *supra* note 35, at 79.

165. See, e.g., Matt Brian, *Apple Wins Prestigious UK Design Awards, Flies Entire Design Team to London to Pick Them Up*, THE NEXT WEB (Sept. 19, 2012 9:24 AM), <http://thenextweb.com/apple/2012/09/19/apple-wins-prestigious-uk-design-awards-flies-entire-design-team-london-pick>

design-centric approach helps avoid usability problems that otherwise undermine many desirable products—everything from medical software and devices, to enterprise software, to security and even encryption software.¹⁶⁶

Arguably, good design in software is more prevalent than ever. For example, content management systems such as WordPress¹⁶⁷ and Drupal¹⁶⁸ make it easy for novice web users to construct entire websites with a click of a mouse and thereby incorporate good aesthetics and design principles. Indeed, one could claim that the proliferation of well-designed and easy-to-use consumer products, coupled with the wide availability of alternatives in most product categories, has led consumers to take good design for granted. However, this design boom, as it relates to software aesthetics and usability, has created many different, and sometimes conflicting, approaches to incorporating design elements into the software development process. Design is now the domain of several different disciplines including visual designers, illustrators, content and copy designers, and both user interface (“UI”) and UX designers, along with creative directors and project managers tasked with pulling together these diverse elements. While the design process can vary significantly from one organization to another, a few generally accepted practices and processes have emerged.

For example, user-centered design seeks to develop software and software interfaces that are focused around end-user goals, needs, wants, and constraints. This methodology depends on learning as much about the end-user as is necessary to create the best user experience for the specific software product. The process begins with a UX researcher who may create ethnographic and field studies, interviews, surveys, heuristic evaluations,¹⁶⁹ user tests, and related methods to generate data regarding user requirements, pain points, and expectations. This data forms the basis for the creation of narratives (known as use cases or use scenarios) that help drive software engineering requirements, which are then incorporated into the overall development plan.¹⁷⁰ Beyond this initial stage, the typical software

(describing the ceremony in which Apple won an award for being the “best design studio of the last 50 years”).

166. See Alma Whitten & J. D. Tygar, *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*, in SECURITY AND USABILITY, *supra* note 94, at 669 (arguing that effective computer security measures require enhanced and particularized user interface standards).

167. WORDPRESS, <http://wordpress.org> (last visited Mar. 17, 2013).

168. DRUPAL, <http://drupal.org> (last visited Mar. 17, 2013).

169. See Jakob Nielsen, *How to Conduct a Heuristic Evaluation*, NIELSEN NORMAN GROUP (Jan. 1, 1995), <http://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation>.

170. For background on the traditional software engineering process, see generally JAKOB NIELSEN, USABILITY ENGINEERING (1993).

development process is iterative, alternating between testing, design tweaks, and coding changes, the extent of which depends on the complexity of the project. In the simplest case, a software developer receives requirements from the design team, devises an architecture and system design, and then relies on this design to develop the software in a matter of days. See *supra*, Figures 1 and 2. In more complex cases, several iterations and multiple departments and stakeholders contribute to a project that may take months or even years to complete.

UX design is growing in importance as a design discipline, with almost every major software company incorporating it into their product design process.¹⁷¹ Recently cited examples of privacy by design such as the Google+ user interface were at least partially the result of work done by UX designers examining socialization in the “real world.”¹⁷² Indeed, privacy by design—insofar as it seeks to anticipate and address potential privacy problems that customers may have in using any product—may be understood as an extension of existing UX design. However, making this a reality would require adjusting current user research protocols to include probes on the relationship of privacy and consumer expectations. This is not always a straightforward task.¹⁷³ In many cases, privacy is a latent concern, and it may be difficult to recognize without additional training or awareness. However, it should not be an insurmountable task for UX designers to develop a better

171. See, e.g., Aaron Marcus, *The ROI of Usability*, USABILITY PROF'LS' ASS'N, http://www.upassoc.org/usability_resources/usability_in_the_real_world/roi_of_usability.html (last visited Apr. 10, 2013) (illustrating the added value for companies implementing usability principles and practices).

172. See Paul Adams, *The Real Life Social Network*, Remarks at the Voices that Matter: Web Design Conference (June 29, 2010) (presentation available at <http://www.slideshare.net/padday/the-real-life-social-network-v2>) (describing research in social engagement in the offline world and how this maps to online social networks).

173. Research in behavioral economics reveals the highly contextual and nuanced nature of consumer decisions and how stated preferences related to privacy are not necessarily adhered to in practice. See generally Acquisti & Grossklags, *Privacy Attitudes and Privacy Behavior*, *supra* note 72; see also Somini Sengupta, *Letting Down Our Guard*, N.Y. TIMES, Mar. 31, 2013, at BU1 (describing Alessandro Acquisti's research).

sense of privacy issues by extending existing concepts.¹⁷⁴ Indeed, Lederer et al. and other HCI experts have already begun doing this.¹⁷⁵

As institutional knowledge of privacy expectations and related social norms develop, it is likely that UX practitioners will get better at recognizing and incorporating them into their user research protocols. Initially, they may have to rely on trial and error to determine what interpretations of privacy values work best for UX privacy research. User experience design was founded on work from pioneers such as Jakob Nielsen and has strong roots in academia that persist to this day. According to Nielsen, usability is a “quality attribute” for determining the ease-of-use of any user interface.¹⁷⁶ Usability in the privacy (and security) domains has additional, unique aspects. First, users consider usable privacy and security controls secondary to completing some primary task (like searching the Internet), so they must be accessible without getting in the way; second, they must accommodate a broad range of users with different skill levels and not only be designed for technical elites; and, third, if sophisticated security and privacy systems lack usability, they may put users at a higher risk than less sophisticated, but more easily used systems. The increased risk of error provides an even greater incentive to ensure that privacy and security are more usable than in many other domains.¹⁷⁷

Usability may be studied throughout the several stages of the software development cycle (requirements, design, release), but it is a large topic and well beyond the scope of this Article.¹⁷⁸ Here, we focus on a narrow slice of the relevant literature that is directly concerned with the interface design aspects of social networks generally, their implications for privacy, and the usability of privacy features in Google+ and Facebook.

174. Many examples of UX guidelines exist. *See, e.g.*, UI WIZARDS, <http://www.uiwizards.com> (last visited Feb. 27, 2013) (offering services, classes, and books for designing user interfaces); Steve Krug, ADVANCED COMMON SENSE, <http://www.sensible.com> (last visited Feb. 27, 2013). Many companies have their own guidelines as well. *See, e.g.*, *What Makes a Design “Googley”?*, GOOGLE OFFICIAL BLOG (Apr. 23, 2008), googleblog.blogspot.com/2008/04/what-makes-design-googley.html (listing Google’s ten design guidelines for interfaces).

175. *See infra* notes 183–202 and accompanying text.

176. *See* Jakob Nielsen, *Usability 101: Introduction to Usability*, NIELSEN NORMAN GROUP, <http://www.nngroup.com/articles/usability-101-introduction-to-usability> (last visited Feb. 27, 2013).

177. *See* Claire-Marie Karat et al., *Usability Design and Evaluation for Privacy and Security Solutions*, in SECURITY AND USABILITY, *supra* note 94, at 47, 48–50.

178. For key reference books in the field, *see* SECURITY AND USABILITY, *supra* note 94, at 49. For an overview of HCI as it relates to privacy, *see* Mark S. Ackerman & Scott D. Mainwaring, *Privacy Issues and Human-Computer Interaction*, in SECURITY AND USABILITY, *supra* note 94, at 381.

In reviewing the strengths and weaknesses of FIPs, we previously argued that the control paradigm on which FIPs are based has limited relevance to the social dynamics of privacy.¹⁷⁹ This line of thinking is borne out by the fact that when usability experts analyze the privacy implications of user interfaces, they do not turn to FIPs as a source of understanding.¹⁸⁰ Rather, they rely on the writings of Irwin Altman—a social psychologist who studied personal space and territoriality and conceptualized privacy as a dynamic process of negotiating personal boundaries in intersubjective relationships¹⁸¹—and Helen Nissenbaum—a philosopher of technology, who understands privacy in terms of norms governing distinct social contexts, a framework that she refers to as “contextual integrity.”¹⁸² Both reject the view that privacy is solely concerned with control over personal information or that the notion of “privacy in public” is somehow an oxymoron. We will briefly describe Altman’s views and their influence on two important essays on the design implications of understanding privacy as a dynamic process.¹⁸³ We then turn to a group of researchers who have sought to analyze and suggest remedies for interface design flaws in Facebook by reference to both Altman’s work and Nissenbaum’s contextual integrity framework.¹⁸⁴

b) Altman

Altman views privacy as an “interpersonal boundary process” by which individuals become more or less accessible and open to others through a variety of behavioral mechanisms.¹⁸⁵ These include verbal and para-verbal behavior (what we say and how we say it—i.e., tone, intensity, pitch, and inflection of voice), personal spacing (distance and angle of orientation to

179. See *supra* Section II.A.

180. See Benjamin Brunk, *A User-Centric Privacy Space Framework*, in SECURITY AND USABILITY, *supra* note 94, at 401, 407 (explaining that the “primary drawback” of using FIPs for understanding user experiences and privacy solutions is “that none of them are particularly user centered”).

181. IRWIN ALTMAN, *THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, AND CROWDING* (1975).

182. See HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE* (2010) [hereinafter NISSENBAUM, *PRIVACY IN CONTEXT*]; Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 101 (2004) [hereinafter Nissenbaum, *Privacy as Contextual Integrity*].

183. See Scott Lederer et al., *Personal Privacy Through Understanding and Action: Five Pitfalls for Designers*, 8 PERS. & UBIQUITOUS COMPUTING 440 (2004); Leysia Palen & Paul Dourish, *Unpacking “Privacy” for a Networked World*, 5, in CHI 2003: NEW HORIZONS: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 129 (2003), available at <http://dl.acm.org/citation.cfm?id=642635>.

184. See notes 218–24 and accompanying text.

185. ALTMAN, *supra* note 181, at 6.

others), and additional forms of non-verbal behavior such as facial expression and body language, territorial behavior (i.e., use, possession, and ownership of places or objects), and cultural norms that regulate contact with others.¹⁸⁶ For example, if we are conducting an intimate conversation in public, we achieve the desired level of privacy by relying on familiar mechanisms such as speaking softly to make the conversation inaudible to others, standing with our backs to the crowd, and avoiding eye contact with anyone who might approach. Analogous mechanisms are generally lacking in online settings, even in SNSs, despite the fact they are all about social interactions.

Clearly, Altman rejects traditional views of privacy as a form of social withdrawal that goes on only in “private” spaces.¹⁸⁷ Rather, privacy is a process that is dynamic (i.e., shaped by personal and collective experiences and expectations),¹⁸⁸ dialectical (i.e., informed by a continuous balancing act over what to disclose or conceal),¹⁸⁹ and optimizing.¹⁹⁰ Finally, privacy is less a matter of an individual’s unilateral control over the disclosure of information than it is a bidirectional process, involving control over both inputs from others (being looked at, approached, or called on the telephone) and outputs to others (staring, seeking out friends, initiating a telephone call).¹⁹¹ In short, privacy is a process of regulating the boundaries by which people make themselves more or less accessible and open to others.¹⁹²

Altman is primarily concerned with how people manage face-to-face interactions occurring in physical space and mediated by the environment in which we live.¹⁹³ Building on Altman’s work, Palen and Dourish explain how

186. *Id.* at 33–42.

187. In this stance, Altman anticipates Nissenbaum’s rethinking of the “public-private” distinction. *See id.*, NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 113–25.

188. ALTMAN, *supra* note 181, at 43–45.

189. *Id.* at 11 (noting that such balancing depends not only on the time and circumstances but also on individual character and group cultural norms).

190. Altman notes that at any given moment, individuals may achieve more privacy than they desire (resulting in boredom, loneliness, or social isolation), less privacy than they desire (resulting in feelings of crowding, intrusion, or invasion), or the optimum level, where the achieved level of interaction and contact with others matches the desired level. *Id.* at 25–27.

191. *Id.* at 27–28.

192. *Id.* at 10. Goffman offers a similar analysis of the complex behavioral decisions people engage in when deciding whether to release or withhold specific information to a given person at a given time depending on their view of themselves, the current situation, and the consequences of disclosure. *See generally* ERVING GOFFMAN, RELATIONS IN PUBLIC: MICROSTUDIES OF THE PUBLIC ORDER (1972); ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

193. Sociologist Christena Nippert-Eng has extended Altman’s work to privacy management in a variety of everyday settings and tasks such as visiting the beach; keeping

privacy as a boundary process works in a networked world mediated by information technology, which simultaneously enables social interaction with large, distant, and even unknown audiences, but also eliminates most of the familiar physical, psychological, and social cues we rely on to manage our interpersonal relationships.¹⁹⁴ Whether we know it or not, every time we “go online,” we disclose information about ourselves.¹⁹⁵ Common activities like web surfing or searching create data trails that are collected, aggregated, and analyzed, often without our knowledge or consent.¹⁹⁶ SNSs introduce new opportunities for social interaction and sharing but offer very limited means to convey demeanor and intent or otherwise establish the context of self-expression.¹⁹⁷

Privacy management in a networked world therefore involves “combinations of social and technical arrangements that reflect, reproduce, and engender social expectations, guide the interpretability of action, and evolve as both technologies and social practices change.”¹⁹⁸ These new privacy mechanisms should enable individuals to intervene in the flows of existing data about them in relation to others and to renegotiate the boundaries of disclosure, identity, and temporality.¹⁹⁹

What, then, are the tools that support both strategic concealment and revelation of data in the various contexts of our networked lives? Lederer et al. suggest improving privacy practices in technical systems through a combination of understanding and action, and offer design guidelines in the form of “five pitfalls” for designers to avoid.²⁰⁰ They are:

and revealing secrets; assembling and categorizing the contents of one’s wallet or purse; managing the receipt of email, cell phone, and other interruptions; and controlling accessibility at the “porous perimeters” of one’s home (windows, doors, yards, and curbs). CHRISTENA NIPPERT-ENG, *ISLANDS OF PRIVACY* 2–3 (2010) (defining privacy as “selective concealment and disclosure” and as a daily activity of trying to “deny or grant varying amounts of access to our private matters to specific people in specific ways”).

194. See Palen & Dourish, *supra* note 183.

195. *Id.* at 131–32.

196. *Id.*

197. *Id.* at 132 (highlighting specifically the concern of friends sharing photographs online without consent or input from the subjects).

198. *Id.* at 133.

199. *Id.*; see also danah boyd, *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications*, in *NETWORKED SELF: IDENTITY, COMMUNITY, AND CULTURE ON SOCIAL NETWORK SITES* 49 (Zizi Papacharissi ed., 2010) (describing three dynamics that play a role in shaping what she calls “networked publics”: invisible audiences, collapsed contexts, and the blurring of public and private).

200. See Lederer et al., *supra* note 183, at 445–49.

1. Designs should not obscure potential information flow (because informed use of a system requires that users understand the scope of its privacy implications);
2. Designs should not conceal actual information flow (because users need to understand what information is being disclosed to whom);
3. Designs should not require excessive configuration to manage privacy but rather should enable users to practice privacy as a natural consequence of their normal engagement with the system;
4. Designs should not forgo an obvious, coarse-grain mechanism for halting and resuming disclosure; and
5. Designs should not inhibit users from transferring established social practice to emerging technologies.²⁰¹

According to the authors, tools that combine such feedback (understanding) and control (action) mechanisms “make their consequences known and do not require great effort to use,” resulting in socially meaningful privacy practices.²⁰²

c) Nissenbaum

Nissenbaum’s theory of privacy as contextual integrity begins with the observation that norms govern the flow of information in highly specific social contexts. Familiar social contexts include health care, education, employment, religion, family, and the commercial marketplace.²⁰³ Each of these contexts may be more fully understood in terms of the roles people play within them (e.g., doctor, nurse, patient), the activities and practices they engage in within such roles (e.g., asking about symptoms, administering medicines, describing an ailment), the norms that define acceptable and unacceptable behaviors within a given context (e.g., respecting patient privacy), and the values around which activities in a context are defined (e.g., prescribing medicine for the good of the patient or applying measures that benefit the sick while avoiding overtreatment).²⁰⁴ People move from one context to another throughout the day, and they implicitly understand what norms apply and act accordingly. For example, we expect a physician treating us for hepatitis to inquire about our consumption of alcohol and drugs but not to share this information with our employer. And we share our joys and anxieties with spouses or partners but not with the clerk at the convenience

201. *Id.* at 441.

202. *Id.* at 450.

203. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 129–30.

204. *Id.* at 132–37.

store. Each of these everyday social contexts has distinctive sets of rules governing information flows. These informational norms define contextual integrity, which is preserved when informational norms are respected, and violated when they are breached.

Nissenbaum posits two fundamental types of informational norms: appropriateness and distribution.²⁰⁵ The former prescribe what personal data is (or is not) allowable, expected, or even required to be revealed in a given context.²⁰⁶ These norms vary greatly and may be more or less restrictive, explicit, or complete. But the key point is that there is no area of life not governed by some informational norms.²⁰⁷ The latter prescribe how and with whom data may be shared in a given context.²⁰⁸ Distributional norms are also highly variable and rather complex.²⁰⁹ For example, information sharing between friends is bidirectional but they expect that what they say to each other will be held in confidence and not arbitrarily spread to others. In contrast, information flows in only one direction in the doctor-patient relationship; doctors expect (and even may demand) that patients reveal their physical and/or mental condition, while patients expect that what they say is confidential, subject to exceptions when a disease poses a public health risk.²¹⁰

Nissenbaum proposes contextual integrity as a “benchmark” of privacy insofar as in any given situation, a privacy violation may be understood as a violation of informational norms.²¹¹ Her work thus sheds much light on recent privacy controversies associated with new information technologies and systems. In a nutshell, information technologies worry and alarm us—and in more extreme cases result in privacy incidents—when they “flout entrenched informational norms and hence threaten contextual integrity.”²¹² In her later work, Nissenbaum argues more generally that information norms are characterized by four parameters—context, actors, attributes, and transmission principles—which are also key parameters for determining whether a new practice resulting from the deployment of a novel technical device or system violates contextual integrity, for example, photo tagging on

205. Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 182, at 138.

206. *Id.* at 137–40.

207. *Id.*

208. *Id.* at 140–43.

209. *Id.*

210. *Id.*

211. NISSENBAUM, *PRIVACY IN CONTEXT*, *supra* note 182, at 140; *see also* Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 182, at 138 (referring specifically to violations of norms of appropriateness and distribution).

212. NISSENBAUM, *PRIVACY IN CONTEXT*, *supra* note 182, at 127.

a SNS.²¹³ She offers a “decision heuristic” for detecting such violations, which involves five steps:²¹⁴ establish the prevailing context (e.g., junior high school students sharing photos by posting them to Facebook); identify key actors (e.g., parents, minor children, friends, friends of friends, Facebook); analyze whether the novel technology (SNSs) affect the types of information transmitted (e.g., not only visual images but links to status updates, photos, tags, etc.);²¹⁵ establish whether transmission principles have changed (e.g., school children sharing a racy photograph with each other in a very guarded fashion versus one of them uploading the photo to a SNS and tagging their friends, thereby sharing and distributing the now tagged photo to a potentially large audience of classmates, teachers, parents, and all of their social networks); and “flag” violations.²¹⁶

For Nissenbaum, contextual integrity is not only a sound benchmark for describing and predicting how people respond to privacy violations but also a prescriptive guide. We will not explore the moral elements of Nissenbaum’s theory²¹⁷ but instead focus on how the framework of contextual integrity assists firms seeking to design new systems that avoid privacy incidents. For example, Heather Richter Lipford builds on Nissenbaum’s work to propose

213. *Id.* at 140–47.

214. NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 148–50.

215. As Facebook explains:

Tag people in your posts: Add tags to anything you post, including photos and updates. Tags can point to your friends or anyone else on Facebook. Adding a tag creates a link that people can follow to learn more.

Tell people about stuff they’re in: Adding tags can let people know when they’re in photos or other things you share. People you tag can receive a notification so they can see your post. The post may also go on the person’s profile and appear in their friends’ news feeds.

Help tag things other people missed: You can tag other people’s photos and posts to help them add details. Your name appears with the tag, so it’s always clear where it came from.

How Tagging Works, FACEBOOK, <https://www.facebook.com/about/tagging> (last visited Feb. 27, 2013). For further discussion of tagging on Facebook, see *supra* Section III.B.4.

216. On the topic of “red flags,” Nissenbaum says, “[i]f the new practice generates changes in actors, attributes, or transmission principles, the practice is flagged as violating entrenched informational norms and constitute[s] a prima facie violation of contextual integrity.” NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 150.

217. The moral element goes beyond assessing information flows in terms of entrenched norms and instead asks whether “new practices are demonstrably more effective at achieving contextual values, ends, and purposes.” *Id.* at 179. This addition of a moral element results in what Nissenbaum refers to as the “augmented” decision heuristic. *Id.* at 181–82.

two specific interface modifications for managing privacy issues on Facebook: Restrict Others²¹⁸ and AudienceView.²¹⁹

As discussed more fully below,²²⁰ photo sharing on Facebook reduces the photo subject's control over her image and its distribution, resulting in now-commonplace stories of embarrassment, humiliation, discrimination, and even arrest.²²¹ Restrict Others relies on the analytic frameworks of Nissenbaum (and Altman) to develop a new tool for enhancing a user's ability to control who sees photos uploaded and tagged by users other than the subject of the photo.²²² Quite simply, "[i]t works by allowing tagged users to send a request to the owner [the person who uploaded the photo] asking that a photo be hidden from certain people."²²³ When Lipford et al. first proposed AudienceView in 2008, the then-current Facebook interface offered limited visual feedback regarding a user's audience and a "poor mental model" of how changes in the privacy settings affect the sharing of profile data with different audiences.²²⁴ As a result, many users unwittingly revealed profile data more broadly than they intended.²²⁵ While Facebook enabled users to configure their profile privacy settings in advance through the usual "wall of checkboxes,"²²⁶ the default privacy settings were permissive and users rarely changed them. AudienceView offers a modified interface:

[U]sers view pages of their profiles from the point of view of different audiences, such as their different groups of friends, networks, public, etc. This interface provides a more visual and accurate mental model of what different people can view of them, allowing users to more explicitly and concretely consider the

218. See Andrew Besmer & Heather Richter Lipford, *Moving Beyond Untagging: Photo Privacy in a Tagged World*, CHI 2010: PRIVACY: PROC. SIGCHI CONF. ON HUM. FACTORS COMPUTING SYS. 1563 (2010), available at <http://dl.acm.org/citation.cfm?id=1753560&bnc=1>.

219. See Heather Richter Lipford et al., *Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites*, in PROC. 12TH IEEE INT'L CONF. ON COMPUTATIONAL SCI. & ENGINEERING 985 (2009), available at <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5283751>.

220. See *infra* notes 399–403 and accompanying text.

221. See NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 59–61 (citing various incidents).

222. Besmer & Lipford, *supra* note 218, at 1567.

223. *Id.*

224. See Heather Richter Lipford et al., *Understanding Privacy Settings in Facebook with an Audience View*, UPSEC '08: PROC. FIRST CONF. ON USABILITY, PSYCHOL., & SECURITY, art. 2 (Elizabeth Churchill & Rachna Dhamija eds., 2008), available at http://static.usenix.org/event/upsec08/tech/full_papers/lipford/lipford.pdf (describing the relationship between user privacy concerns and the shortcomings in Facebook's user interface).

225. *Id.* at 2.

226. See Nathan Good, *The Deadly Sins of Security User Interfaces*, in THE DEATH OF THE INTERNET 290, 300–02 (Markus Jakobsson ed., 2012).

context of their information and adjust that information flow as desired.²²⁷

To remind users of information flows as they view friends' profiles and post information, Lipford et al. proposed a "message box on the user's home page . . . show[ing] the most recent information access[ed by others], . . . or summariz[ing] the number of accesses in a certain time period."²²⁸ And to prevent the "flattening" of a user's social contexts and ensure that Facebook privacy settings better reflect the more nuanced and varied social contexts of offline relationships, they suggested that Facebook automatically determine a user's social spheres by analyzing every user's "social network graph" and that it make this information available to users through the AudienceView interface.²²⁹

Finally, Lipford et al. offer six design guidelines based on the contextual integrity framework for making information flows more visible in SNSs.²³⁰ They are as follows:

1. Make information flows more transparent, so that users know what information they are sharing and with whom;
2. Increase user awareness of information flows as they make decisions about sharing profile data, photos, and the like, both with other users and/or third parties;
3. Increase user awareness of how much information is archived and still available to others;
4. Make information and context concrete by providing specific examples of who will see what;
5. Provide more granular controls over information flows; and
6. Do not abruptly modify the flow of information.²³¹

This completes our brief overview of the design process, the multiple factors that influence design, and the engineering and usability principles that firms must follow in order to translate a robust understanding of FIPs into well-engineered and highly usable privacy designs. We began by distinguishing back-end implementation and security protections from front-

227. See Lipford et al., *supra* note 219, at 987.

228. *Id.* at 988.

229. *Id.* at 987–88. For a related idea, see Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1342–44 (2009) (proposing a "tool for users to express . . . privacy preferences over uploaded content . . . by tagging any uploaded content with [a visual] icon" and perhaps machine-readable metadata).

230. See Lipford et al., *supra* note 219, at 987. The guidelines are highly reminiscent of the five "pitfalls" of Lederer et al. See *supra* note 200 and accompanying text.

231. Lipford et al., *supra* note 219, at 987.

end design issues centered on users' privacy expectations and, hence, on the disciplines of Human-Computer Interactions ("HCI"), including both user-interface ("UI") and user-experience ("UX") design. Next, relying mainly on the works of Feigenbaum, et al., and Spiekermann and Cranor, we identified a short list of FIPs-based engineering principles including data avoidance and minimization, data retention limits, notice, choice, access, and accountability. Finally, relying on Grimmelmann's idea of the "social dynamics" of privacy, we fleshed out the UX approach to privacy design by discussing "five pitfalls" for designers to avoid as identified by Lederer et al., and six design principles of Lipford et al., which we traced back, respectively, to the pioneering work of Altman and Nissenbaum. With the completion of this preliminary work, we may now take up the counterfactual analysis, which applies these privacy engineering and design principles to the ten case studies.

III. CASE STUDIES AND COUNTERFACTUAL ANALYSES

A. GOOGLE

Google manages the most popular Internet search engine,²³² which generates revenue when users click or view advertising related to their searches.²³³ Advertising revenue accounted for about 95% of Google's approximately \$46 billion in annual revenues in 2012.²³⁴ The company has a long history with privacy issues, and we review four major Google services—Gmail, Search, Street View, Buzz (and its successor, Google+)—as well as its controversial new revisions to the company's privacy policies.

1. Gmail

Gmail is Google's free, web-based and advertising-supported email service.²³⁵ When launched in early 2004 as an invitation-only beta release, it was an immediate success, offering users unprecedented storage capacity in exchange for receiving contextual ads.²³⁶ Gmail's ad engine automatically scans header information and the content of incoming and outgoing

232. See Press Release, comScore, comScore Releases January 2013 U.S. Search Engine Rankings (Feb. 13, 2013), http://www.comscore.com/Insights/Press_Releases/2013/2/comScore_Releases_January_2013_U.S._Search_Engine_Rankings (showing Google accounts for two-thirds of U.S. web searches).

233. See *Investor Relations: 2012 Financial Tables*, GOOGLE, <http://investor.google.com/financial/tables.html> (last visited Mar. 8, 2013).

234. *Id.*

235. See *Google Gets the Message, Launches Gmail*, NEWS FROM GOOGLE (Apr. 1, 2004), <http://googlepress.blogspot.com/2004/04/google-gets-message-launches-gmail.html>.

236. *Id.*

messages for key words provided by advertisers in advance.²³⁷ Despite this privacy-sensitive design, Google's decision to fund free storage by serving contextual ads proved quite controversial: users and consumer advocacy groups raised concerns over the lack of consent by non-subscribers, the impact of storage capacity on data retention (and hence government requests for data), and the prospect of Google someday modifying its approach and creating highly detailed user profiles based on the correlation of users' Gmail identities with their Google search behavior.²³⁸ Despite numerous government investigations, no adverse actions were taken, and the controversy gradually faded without forcing any major change in Gmail's handling of ads.²³⁹ Gmail's success allowed Google to branch out into new products and create a more individualized relationship with hundreds of million users, managing their email accounts and contact lists, and laying the foundation for its later foray into social networking.²⁴⁰

Gmail is a design success: it offered users a very clear value proposition, served ads while avoiding both profiling and disclosure of PII to advertisers, and did a reasonably thorough job of ensuring informed consent.²⁴¹ And yet many greeted Gmail with anxiety and suspicion, which persisted notwithstanding its design strengths.²⁴² Prior to Gmail, email was conceived of as a personal and inviolate form of communication between a sender and

237. See *Gmail Privacy FAQ: How Does Google's "Content Extraction" Work?*, EPIC, <http://epic.org/privacy/gmail/faq.html> (last visited Mar. 8, 2013).

238. See Stefanie Olsen, *Google's Web Mail No Joke*, CNET (Apr. 2, 2004), <http://news.cnet.com/2100-1032-5184090.html> (describing how government could subpoena archived information or how Google could mine the data); Donna Wentworth, *Gmail: What's the Deal?*, ELEC. FRONTIER FOUND. (Apr. 5, 2004), <https://www.eff.org/deeplinks/2004/04/Gmail-whats-deal> (listing various news stories regarding concerns about Gmail).

239. See Jane Perrone, *Google Free Email Faces Legal Challenge*, THE GUARDIAN (Apr. 12, 2004), <http://www.guardian.co.uk/technology/2004/apr/13/internationalnews.onlinesupplement>.

240. See Dante D'Orazio, *Gmail Now Has 425 Million Total Users*, THE VERGE (June 28, 2012), <http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users>; Robert Charette, *Google Expands In Two More Directions: Social Media and Broadband Service*, IEEE SPECTRUM: RISK FACTOR BLOG (Feb. 11, 2010), <http://spectrum.ieee.org/riskfactor/telecom/internet/google-expands-in-two-more-directions-social-media-and-broadband-service>.

241. See Friedman et al., *Informed Consent by Design*, *supra* note 155, at 521–26. Friedman et al., however, also raised two related privacy concerns regarding Gmail: (1) whether using a machine to read email violates a person's privacy expectations, and (2) whether email senders actually consent to automatic scanning. *Id.* at 524.

242. See Perrone, *supra* note 239.

a receiver; contextual ads disrupted these informational norms by treating a private communication as the basis for a commercial offer.²⁴³

Are there additional design steps that Google might have taken to allay users' privacy concerns? First, Google might have been more transparent about whether Gmail served ads related to the content of one's emails and also tracked users in other ways or shared information with other services for advertising or other purposes.²⁴⁴ Second, Google might have translated these assurances into architectural choices by designing a web mail service that segregated and separated any personal data about subscribers or their message content from any data collected by other Google services.²⁴⁵ Third, and more radically, Google might have considered a simultaneous release of both an ad-supported free web mail service and an ad-free paid version.²⁴⁶ By providing consumers with a range of choices from the outset, Google could have facilitated "privacy by experimentation" and set a sound precedent for designing future services with privacy in mind.²⁴⁷

2. Search

Unlike Gmail, Google Search attracted more sustained interest from privacy officials. Beginning in the final months of 2006, European and U.S. regulators challenged Google and its search engine competitors regarding the amount, sensitivity, and retention periods of the data collected for search ads and other purposes.²⁴⁸ Both consumer and regulatory concerns were spurred in part by two widely read news stories alerting the public to the data processing practices of their favorite search engines.²⁴⁹ Over the next several

243. *See id.* ("[I]t's an absolute invasion of privacy. It's like having a massive billboard in the middle of your home." (quoting former California State Senator Liz Figueroa)).

244. The original Gmail privacy policy stated, "Google may send you information related to your Gmail account or other Google services." *Google Gmail Privacy Policy*, TOSBACK (Sep. 12, 2008), <http://www.tosback.org/version.php?vid=1030>.

245. *See supra* notes 116, 137 and accompanying text.

246. Google later provided options for paying customers of Google Apps for Business or Education to turn off ads for a given domain. *See Disable Advertisements*, GOOGLE, <http://support.google.com/a/bin/answer.py?hl=en&answer=60758> (last visited July 23, 2012).

247. *See* Betsy Masiello, @betsymas, TWITTER (Aug. 19, 2010), <https://twitter.com/betsymas/status/21615739700> ("two concepts from today: privacy by experimentation in contrast to privacy by design; data driven policy by design as a way fwd").

248. *See* Verne Kopytoff, *Google Comes Under Scrutiny*, SFGATE (May 30, 2007), <http://www.sfgate.com/business/article/Google-comes-under-scrutiny-FTC-European-2590461.php>.

249. In one, the DOJ subpoenaed millions of search records from leading firms and Google challenged the request in court, winning concessions on the scope of the final order. *See* Verne Kopytoff, *Google Says No to Data Demand*, SFGATE (Jan. 20, 2006), <http://www.sfgate.com/news/article/Google-says-no-to-data-demand-Government-wants->

years, regulators and advocates called upon all search firms to offer greater transparency regarding their data practices, shorter data retention periods, and improved methods for anonymizing data after the retention period expired.²⁵⁰ In response, Google, Yahoo!, and Microsoft shortened data retention periods, sought to improve anonymization techniques, and began developing new compliance mechanisms.²⁵¹ Soon, all of the major search firms were competing on privacy features for their search engine and browser offerings.²⁵² Despite this heated competition, Google remained the leading search engine and moved ahead with a \$3.1 billion acquisition of DoubleClick, overcoming objections on both antitrust and privacy grounds.²⁵³

With Search, the public grew alarmed when it learned that leading search engines were tracking their searches and collecting and storing sufficient information to attract the attention of law enforcement agencies and to permit inquisitive journalists to discover their “real-life” identities.²⁵⁴ Two interrelated design issues emerged: (1) how long search data should be retained before being deleted; and, (2) if it was anonymized instead of deleted, the proper method of anonymization. Google sought to achieve what it deemed the “right balance” between “privacy and other goals (like security, fraud prevention, and search improvements)” by retaining search logs for eighteen months and then “anonymizing” any data linking search terms to IP addresses by erasing the last octet of the IP address.²⁵⁵ To be

2523692.php. In the other, AOL shared “anonymized” search logs with researchers but the released data enabled curious journalists to identify a sixty-two-year-old woman in Georgia. See Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1.

250. See, e.g., E.U. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 1/2008 ON DATA PROTECTION ISSUES RELATED TO SEARCH ENGINES (WP 148) (Apr. 2008) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf; FED. TRADE COMM’N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: TRACKING, TARGETING, AND TECHNOLOGY (Feb. 2009), <http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

251. See, e.g., Peter Fleischer, *Data Retention: The Right Balance Between Privacy and Security*, GOOGLE PUB. POL’Y BLOG (July 11, 2007), <http://googlepublicpolicy.blogspot.com/2007/07/data-retention-right-balance-between.html>.

252. See Gregg Keizer, *Mozilla Adds Privacy Mode to Firefox 3.1 Plans*, MACWORLD (Sept. 12, 2008), <http://www.macworld.co.uk/macsoftware/news/?newsid=22767> (describing Mozilla’s efforts to compete with Microsoft and Google by adding a private search mode to browser).

253. See Louise Story & Miguel Helft, *Google Buys an Online Ad Firm for \$3.1 Billion*, N.Y. TIMES, Apr. 14, 2007, at C1.

254. See Barbaro & Zeller Jr., *supra* note 249.

255. See Fleischer, *supra* note 251. For criticisms of Google’s anonymization method, see Soghoian, *supra* note 133. Other search engines have experimented with shorter periods. See

sure, there is a trade-off between retaining data to improve search results and maintain security, and deleting or anonymizing search data to protect user privacy. That being said, are there other steps Google might have taken to address privacy concerns? First, it might have assisted users in conducting searches or browsing the web anonymously, either by partnering with a proxy server or by integrating search with an onion-router proxy like Tor.²⁵⁶ Alternatively, Google might have pursued a data minimization approach by managing internal access to users' IP addresses for uses beyond search quality and anti-fraud issues. Third, Google might have stepped up its transparency efforts with respect to its search practices. While Google's disclosures met or exceeded industry standards,²⁵⁷ it neither explained the potential privacy harms of monitoring and tracking search queries nor stated explicitly whether it combined search query data with any other information it collected from Gmail and other services requiring account registration.²⁵⁸ Finally, Google might have facilitated multiple online accounts early on, thereby allowing users to segment their lives and adjust their public personas in accordance with the social insights of Altman and Goffman.²⁵⁹

Chloe Albanesius, *Yahoo to Keep Your Search Data for 18 Months, Not Three*, PCMAG (Apr. 18, 2011), <http://www.pcmag.com/article2/0,2817,2383711,00.asp> (describing Yahoo!'s attempt at a three-month retention period before it was forced to retreat to 18 months due to search quality issues); Michael Zimmer, *Microsoft to Delete IP Addresses from Bing Search Logs after 6 Months*, MICHAELZIMMER.ORG (Jan. 19, 2010), <http://www.michaelzimmer.org/2010/01/19/microsoft-to-delete-ip-addresses-from-bing-search-logs-after-6-months>.

256. An onion router repeatedly encrypts and forwards requests through a chain of proxies and, like a layer of an onion, removes a layer of the encryption to determine the next destination. The end effect is that the traffic cannot be traced back to its original source, unlike common network connections. *See* TOR, <https://www.torproject.org> (last visited Mar. 8, 2013); *see also supra* note 108 and accompanying text.

257. For example, in 2007, Google launched an innovative series of short videos to explain basic privacy concepts including search privacy. *See* Peter Fleischer, *Google Search Privacy: Plain and Simple*, GOOGLE OFFICIAL BLOG (Aug. 8, 2007), <http://googleblog.blogspot.com/2007/08/google-search-privacy-plain-and-simple.html>.

258. In 2010, Google launched a tool for reporting on government requests for user data. Dorothy Chou, *Transparency Report: Government Requests on the Rise*, GOOGLE OFFICIAL BLOG (Nov. 13, 2012), <http://googleblog.blogspot.com/2012/11/transparency-report-government-requests.html>; *see Google Transparency Report*, GOOGLE, <http://www.google.com/transparencyreport/> (last visited July 23, 2012).

259. *See supra* Section II.B.3.b; *supra* note 192. Privacy advocates maintain that allowing users multiple accounts and identities allows users to engage in more natural online interactions and to adjust their privacy requirements as needed. *See, e.g.,* danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, in YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 131–34 (David Buckingham ed., 2008) (describing teenagers' use of multiple accounts on MySpace, each tailored for different audiences); *Anonymity*, ELEC. FRONTIER FOUND., <https://www.eff.org/issues/anonymity> (last visited Apr. 11, 2013) (describing the importance and need for protection of anonymous speech on

3. *Google Street View*

Street View presents a more complex privacy scenario than either Gmail or Search. Launched initially in the United States in May 2007, Street View is an adjunct to Google Maps.²⁶⁰ It displays panoramic images of many cities, which are photographed from cars equipped with specially adapted digital cameras and antennas.²⁶¹ Advocates and regulators objected early on to Google's collection and display of identifiable faces and license plates in conjunction with buildings or street scenes that might associate individuals with embarrassing or sensitive activities or locations (e.g., sunbathing in the nude or leaving a strip club).²⁶²

At first, Google defended its actions in the United States by arguing that all of the images were taken on public streets, where expectations of privacy are minimal.²⁶³ Over time, Google improved its procedures for removing objectionable images and adopted digital "pixelation" technology (i.e., facial blurring) on a worldwide basis.²⁶⁴ And yet Street View continued to be closely scrutinized in many jurisdictions where privacy laws prohibited the publication of images of people without their explicit consent, or local norms treated residential streets as part of one's private space.²⁶⁵ Although privacy officials in several countries opened Street View investigations and ordered Google to stop taking pictures until these were completed, Google seemed on a path to resolve most of these matters.²⁶⁶ Then, in late April 2010, Google revealed that its Street View cars had been inadvertently collecting "payload data" from Wi-Fi networks ("payload data" refers to information

the Internet). While consumers have regularly used multiple online identities to segment their lives, Google has recently made it easier for consumers to do so. *See Manage Multiple Users on Chrome*, CHROME HELP, <https://support.google.com/chrome/bin/answer.py?hl=en&answer=2364824> (last visited July 23, 2012).

260. *See* Josh Lowensohn, *Google Launches Street View, Maplets*, CNET (May 29, 2007), http://news.cnet.com/8301-17939_109-9723263-2.html.

261. SIVA VAIDHYANATHAN, *THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY)* 98 (2011).

262. *See* Elinor Mills, *Cameras Everywhere, Even in Online Maps*, CNET (May 30, 2007), http://news.cnet.com/Cameras-everywhere,-even-in-online-maps/2100-1038_3-6187556.html.

263. Peter Fleischer, *Street View and Privacy*, GOOGLE MAPS BLOG (Sept. 24, 2007), <http://google-latlong.blogspot.com/2007/09/street-view-and-privacy.html> ("There's an important public policy debate in every country around what privacy means in public spaces. That balance will vary from country to country, and Street View will respect it.").

264. *See* VAIDHYANATHAN, *supra* note 261, at 98–107.

265. *Id.* at 102–03 (noting that Google was forced to reshoot its Street View photos in Japan with cameras mounted lower to avoid peering over hedges and fences).

266. *See id.* at 111 ("The vast majority of those who use Google find Street View more beneficial . . . than harmful. . . . For every person who complains about Street View, millions more find it useful.").

sent over unprotected networks that includes locational data, passwords, email address, and contents of communications).²⁶⁷ Public censure, private lawsuits, and dozens of new investigations quickly followed.²⁶⁸ Google responded by intensifying its efforts to address these new (and old) concerns but with mixed results.²⁶⁹ Additionally, the Federal Communications Commission (“FCC”) fined Google for obstructing its inquiry into the company’s collection of Wi-Fi payload data.²⁷⁰ According to new details that emerged upon publication of a full version of the FCC report, data collection “was neither a mistake nor the work of a rogue engineer, as the company long maintained, but a program that supervisors knew about.”²⁷¹ As a result, a number of regulators are considering whether to reopen their investigations.²⁷² Meanwhile, in Switzerland, an appeals court issued a mixed ruling, concluding that a ninety-nine percent accuracy rate in Google’s blurring technology was acceptable, yet still upholding several conditions demanded by the privacy commissioner.²⁷³

Although many commentators take it for granted that it was highly invasive for Street View to publish images of people at specific geographical

267. See Alan Eustace, *Wifi Data Collection: An Update*, GOOGLE OFFICIAL BLOG (May 14, 2010) (updated June 9, 2010), <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>.

268. See Joshua Keating, *Google’s Most Controversial Feature*, FOREIGN POLICY (Aug. 10, 2010), http://blog.foreignpolicy.com/posts/2010/08/10/googles_most_controversial_feature (noting that “nearly half of the 60 legal or criminal investigations being faced by Google are related to Street View”).

269. In a 2009 agreement with Germany, Google agreed to let property owners opt out of Street View before it was activated. See Kevin J. O’Brien, *Many Germans Opt Out of Google’s Street View*, N.Y. TIMES, Oct. 15, 2010, <http://www.nytimes.com/2010/10/16/technology/16streetview.html>. In contrast, Google failed to reach an agreement with Switzerland—which insisted that Google’s pixelation technology achieve a 100 percent success rate—forcing Google to litigate. See Kevin J. O’Brien & David Streitfeld, *Swiss Court Allows Google Street View*, N.Y. TIMES, June 9, 2012, at B2.

270. See David Streitfeld, *Google Engineer Told Others of Data Collection, Full Version of F.C.C. Report Reveals*, N.Y. TIMES, Apr. 29, 2012, at A22.

271. *Id.* A Google privacy official later stated that the documents Google released in connection with the investigation “show some isolated references to payload collection early in the project that could have been seen as red flags by the recipients with the benefit of hindsight. But in context, at the time, the red flags were missed or not understood.” See Letter from Peter Fleischer, Global Privacy Counsel, Google, to Steve Eckersley, Head of Enforcement, UK ICO (June 18, 2012), *available at* <http://www.telegraph.co.uk/technology/google/9339113/Google-snooping-investigation-response-in-full.html>.

272. See Kevin J. O’Brien, *Rethinking an Inquiry of Google*, N.Y. TIMES, May 3, 2012, at B1.

273. See O’Brien & Streitfeld, *supra* note 269 (explaining that the conditions require Google “to lower the height of its Street View cameras so they would not peer over garden walls and hedges, to completely blur out sensitive facilities like women’s shelters, prisons, retirement homes and schools, and to advise communities in advance of scheduled tapings”).

locations, the social norms governing public images differ cross-culturally and remain somewhat unsettled.²⁷⁴ This is especially true in the United States, where people became accustomed to Street View with little difficulty.²⁷⁵ Google acknowledged these cultural differences when it released Street View overseas with additional privacy protections (blurring faces and license plates) and made local adjustments in Japan²⁷⁶ and Germany.²⁷⁷ Despite these efforts, many users and foreign governments strongly objected to Google's failure to provide advance notice or obtain explicit consent prior to recording and distributing personal images via Street View.²⁷⁸ Granted, Google provided an ex post mechanism for removing objectionable images from Street View but did not provide tools for residents of city streets to signal, ex ante, that they did not want Google to photograph them or their residences.²⁷⁹ Google might object that an ex ante mechanism was impractical at the massive scale of Street View, but obviously this begs the question of whether the service violates norms of appropriateness and what should be done about it.²⁸⁰ Additionally, Google might have included blurring technology in the initial U.S. roll out.²⁸¹ Instead, it assumed that the attitudes of American city dwellers would perfectly mirror U.S. legal doctrine, which offers weaker protection of public streets than of the interior of the home.²⁸² When Google later added blurring technology to Street View, however, it did so on a worldwide basis, something it might have done from the outset. In sum, Street View combines design successes—such as digital pixelation and

274. For a discussion of the disruptive nature of technologies that capture visual information and enable visual recognition and analysis on a massive scale, see generally Ryan Shaw, Recognition Markets and Visual Privacy (Nov. 2006) (unpublished paper), www.law.berkeley.edu/files/bclt_unblinking_shaw.pdf.

275. See VAIDHYANATHAN, *supra* note 261, at 99 (“Over time, as no horror stories emerged, American Google users became accustomed to the new function [of Street View] . . .”).

276. See Chris Matyszczyk, *Google Street View Has to Reshoot in Japan*, CNET (May 13, 2009), http://news.cnet.com/8301-17852_3-10240459-71.html.

277. See Frederic Lardinois, *Several Hundred Thousands Germans Opt out of Google Street View*, READWRITEWEB (Sept. 20, 2010), http://readwrite.com/2010/09/20/hundreds_of_thousands_of_germans_opt_out_of_google.

278. See VAIDHYANATHAN, *supra* note 261, at 100–07.

279. See *id.* at 102–05 (describing how residents of Kiel, Germany, put stickers on their front doors demanding that Google not photograph their homes, and how residents of Broughton, England formed a human chain to prevent the “Googlemobile” from entering their streets).

280. See NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 192–93; see also VAIDHYANATHAN, *supra* note 261, at 102–03.

281. Pixelation may be thought of as a form of data minimization. See *supra* note 137 and accompanying text.

282. See Fleischer, *supra* note 263.

opt-out—with design failures—such as delayed introduction of privacy-protective features and a still unexplained breakdown of its privacy process resulting in the Wi-Fi payload data scandal.²⁸³

In 2009, the year preceding the launch of Buzz, Google released Latitude, a location-tracking service that shares a user's position on a map with her friends and included a large number of privacy-protective features.²⁸⁴ It also announced several major privacy initiatives such as the Data Liberation Front, which sought to ensure that data from any Google property was easily exportable for use with other applications and services;²⁸⁵ a “Data Dashboard,” which provided users with a single location to control and view their settings for every services they subscribed to or otherwise utilized,²⁸⁶ and, just two weeks before launching Buzz, a new set of privacy principles.²⁸⁷

4. *Buzz and Google+*

On February 9, 2010, Google launched Buzz, with great hopes for competing directly with Facebook in the SNS space.²⁸⁸ Towards that goal,

283. For the details of collection of Wi-Fi payload data, see Notice of Apparent Liability for Forfeiture, Google, Inc., 27 FCC Rcd. 4012 (Apr. 13, 2012), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-12-592A1.pdf. While Google maintained that it only collected fragments of payload data, the FCC was unable to determine what use, if any, Google made of certain data due to its inability to compel testimony from key witnesses. Additionally, in March 2013, Google reached a settlement with the attorneys general of thirty-eight states and the District of Columbia to resolve state claims concerning the Wi-Fi payload data controversy. See Alexei Oreskovic, *Google Pays \$7 Million to Settle 38-State WiFi Investigation*, REUTERS (Mar. 12, 2013), <http://www.reuters.com/article/2013/03/12/us-google-wifi-fine-idUSBRE92B0VX20130312>.

284. See Michael Zimmer, *With Latitude, Google Actually Got It (Mostly) Right*, MICHAELZIMMER.ORG (Feb. 6, 2009), <http://michaelzimmer.org/2009/02/06/with-latitude-google-actually-got-it-mostly-right>.

285. See DATA LIBERATION, <http://www.dataliberation.org> (last visited Apr. 11, 2012).

286. *About the Dashboard*, GOOGLE, <http://support.google.com/accounts/bin/answer.py?hl=en&answer=162744> (last visited Mar. 18, 2013).

287. See Alan Eustace, *Google's Privacy Principles*, THE OFFICIAL GOOGLE BLOG (Jan. 27, 2010), <http://googleblog.blogspot.com/2010/01/googles-privacy-principles.html>. These anodyne principles obligate Google to:

- Use information to provide [its] users with valuable products and services.
- Develop products that reflect strong privacy standards and practices.
- Make the collection of personal information transparent.
- Give users meaningful choices to protect their privacy.
- Be a responsible steward of the information [it holds].

Id.

288. Todd Jackson, *Introducing Google Buzz*, THE OFFICIAL GOOGLE BLOG (Feb. 9, 2010), <http://googleblog.blogspot.com/2010/02/introducing-google-buzz.html>.

Buzz included a feature that, “without prior notice or the opportunity to consent, Gmail users were, in many instances, automatically set up with ‘followers’ (people following the user).”²⁸⁹ In addition, after enrolling in Buzz, Gmail users were automatically set up to “follow” other users.²⁹⁰ Moreover, Google made this information publicly accessible to anyone viewing a user’s profile.²⁹¹ This decision to jump-start the Buzz social network by exploiting existing Gmail contact lists backfired, turning Buzz into a “danger zone” for investigative reporters, human rights activists, abuse victims, or anyone whose most frequent contacts were—and needed to remain—confidential.²⁹² Google immediately created a war room and sought to resolve problems without delay; two days later, it adjusted Buzz’s user interface by making it easier to opt-out of disclosing the lists of followers and people one follows, although the disclosure option was still pre-selected.²⁹³ In a blog post announcing further changes, Google sought to justify its decision to implement “auto-following” by noting, “we wanted to make the getting started experience as quick and easy as possible.”²⁹⁴ But in response to customer concerns, Google introduced a new “auto-suggest” feature, which allowed users to review and approve follower suggestions based on their most frequent contacts.²⁹⁵

These changes failed to satisfy the Electronic Privacy Information Center (“EPIC”), which soon filed a complaint with the FTC.²⁹⁶ In a blog post, the Electronic Frontier Foundation (“EFF”) blamed Google’s privacy problems on its attempt “to overcome its market disadvantage in competing with

289. See Complaint at *2–5, Google, Inc., F.T.C. No. 102-3136, 2011 WL 5089551 (Mar. 30, 2011), available at <http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf>.

290. See *id.* These lists of “followers” and people being “followed” were based on the individuals to or with whom Gmail users most frequently emailed and/or chatted. *Id.*

291. See *id.* at *3.

292. See James Grimmelman, *Privacy as Product Safety*, 19 WIDENER L.J. 793, 823–26 (2010) (quoting Nicholas Carlson). For more user complaints about Google Buzz, see EPIC’s complaint filed with the FTC. Complaint, Request for Investigation, Injunction, and Other Relief ¶¶ 25–30, 37–40, Google, Inc., EPIC (Feb. 16, 2009), available at http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf [hereinafter EPIC Buzz Complaint].

293. See Nicholas Carlson, *How Google Went into “Code Red” and Saved Google Buzz*, BUSINESS INSIDER (Feb. 16, 2010), http://articles.businessinsider.com/2010-02-16/tech/30071123_1_google-buzz-google-employees-googleplex. Google’s blog posts chronicled the implementation of the changes. See Todd Jackson, *Millions of Buzz Users, and Improvements Based on Your Feedback*, OFFICIAL GMAIL BLOG (Feb. 11, 2010), <http://gmailblog.blogspot.com/2010/02/millions-of-buzz-users-and-improvements.html>.

294. Jackson, *supra* note 288.

295. *Id.*

296. See EPIC Buzz Complaint, *supra* note 292.

Twitter and Facebook by making a secondary use of [users'] information.”²⁹⁷ An op-ed posted the next day by Leslie Harris of the Center for Democracy and Technology (“CDT”) called Buzz “a textbook example of how to violate the principles of Privacy by Design.”²⁹⁸ Google was also hit with a class-action lawsuit, which it eventually settled for \$8.5 million.²⁹⁹

Buzz raised multiple privacy concerns that brought about its untimely demise. Buzz violated several FIPs and related privacy engineering requirements, including inadequate and misleading notice and lack of informed consent, and these deficiencies eventually forced Google to settle both a class action lawsuit and an FTC complaint.³⁰⁰ Buzz also disregarded several design guidelines, including all five pitfalls of Lederer et al.³⁰¹ and many of the design guidelines of Lipford et al. as well.³⁰² Google might have done things very differently with Buzz. First, it might have more clearly disclosed that users’ frequent Gmail contacts would be made public by default. Second, it might have released the service not with an auto-following feature, but rather with the auto-suggest feature that it was forced to hurriedly develop under pressure. Finally, it might have provided easier and more effective options for users to exit the new service. In short, it might have made Buzz more configurable (per Feigenbaum et al.)³⁰³ from the outset.

Because Buzz was such a spectacular defeat for an otherwise successful and savvy company, it is worth pausing for a moment to ask a slightly different question: why did Google get Buzz so wrong? danah boyd suggests two reasons: first, Google launched Buzz as a “public-facing service inside a service that people understand as extremely private.”³⁰⁴ But this disrupted social expectations, or as Nissenbaum would say, violated contextual integrity.³⁰⁵ Second, “Google assumed that people would opt-out of Buzz if

297. Kurt Opsahl, *Google Buzz Privacy Update*, ELEC. FRONTIER FOUND. (Feb. 16, 2010), <https://www.eff.org/deeplinks/2010/02/google-buzz-privacy-update>.

298. Leslie Harris, *Buzz or Bust*, THE HUFFINGTON POST (Feb. 17, 2010), www.huffingtonpost.com/leslie-harris/buzz-or-bust_b_466133.html.

299. Nick Saint, *Google Settles Over Buzz, Will Establish \$8.5 Million Fund to Promote Privacy Education*, BUSINESS INSIDER (Nov. 2, 2010), <http://www.businessinsider.com/google-settles-over-buzz-will-establish-85-million-fund-to-promote-privacy-education-2010-11>.

300. *See id.*; Google Settlement, *supra* note 25.

301. *See supra* note 200 and accompanying text.

302. *See supra* note 230 and accompanying text.

303. *See supra* note 114 and accompanying text.

304. danah boyd, Remarks at SXSW, Making Sense of Privacy and Publicity (Mar. 13, 2010), <http://www.danah.org/papers/talks/2010/SXSW2010.html>.

305. *See* Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 182.

they did not want to participate.”³⁰⁶ But this premise was flawed, as many unsuspecting users jumped into Buzz without understanding its information flows, became confused, and found it hard to exit, which only intensified their anxiety.³⁰⁷

During the remainder of 2010 and through the first quarter of 2011, Google also made a number of significant policy announcements regarding its commitment to end-user privacy. To begin with, Google apologized for Buzz.³⁰⁸ Eight months later, it named Alma Whitten as its director of privacy, with responsibility for ensuring that Google “build[s] effective privacy controls into [its] products and internal practices.”³⁰⁹ At the same time, Google committed to educating new employees on its privacy principles with an enhanced curriculum for engineers, product managers, and legal teams, and announced a new compliance process,

in which every engineering project leader will be required to maintain a privacy design document for each initiative they are working on. This document will record how user data is handled and will be reviewed regularly by managers, as well as by an independent internal audit team.³¹⁰

About five months later, Google agreed to a consent decree regarding Buzz, which “bar[red] the company from future privacy misrepresentations, require[d] it to implement a comprehensive privacy program, and call[ed] for regular, independent privacy audits for the next 20 years.”³¹¹ That same day, Whitten posted a blog response reaffirming Google’s commitment to privacy and apologizing again for Buzz’s privacy concerns.³¹² The saga ended when

306. See Boyd, *supra* note 304.

307. *Id.* (noting that she gave Google “the benefit of the doubt on this one because a more insidious framing would be to say that they wanted to force people into opting-in because this makes the service more viral and more monetizable.”).

308. See Miguel Helft, *Anger Leads to Apology from Google About Buzz*, N.Y. TIMES, Feb. 14, 2010, at B3.

309. Alan Eustace, *Creating Stronger Privacy Controls Inside Google*, GOOGLE OFFICIAL BLOG (Oct. 22, 2010), <http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html>.

310. *Id.*

311. Press Release, Fed. Trade Comm’n, FTC Charges Deceptive Privacy Practices in Google’s Rollout of Its Buzz Social Network (Mar. 30, 2011), <http://www.ftc.gov/opa/2011/03/google.shtm>.

312. Alma Whitten, *An Update on Buzz*, GOOGLE OFFICIAL BLOG (Mar. 30, 2011), <http://googleblog.blogspot.com/2011/03/update-on-buzz.html>.

Google officially announced on October 14, 2011, that it was discontinuing Buzz.³¹³

In releasing Google+ in the summer of 2011, Google sought to take a major step to recover from the Buzz debacle.³¹⁴ Built from the ground up around notions of privacy and user control, Google+ was the first SNS to rely explicitly on the idea of dividing users into “circles” (e.g., family, friends, co-workers) and to organize controls for both individual posts and one’s profile information with these customized groups in mind.³¹⁵ Google’s new approach was widely applauded and even cited for exemplifying privacy by design.³¹⁶ Although Google+ encountered a few privacy-related objections, they were fairly minor and did not tarnish Google’s newly restored reputation.³¹⁷ Indeed, it seemed as if Google had learned its lessons from Buzz and was now making a concerted effort not only to move into the social space in a responsible way that respected users’ privacy, but also to outdo its competitors in providing innovative privacy tools.³¹⁸ But was Google’s new, privacy-centric SNS the first fruit of Whitten’s new focus on building effective privacy controls into Google’s products and internal practices³¹⁹ or just a very successful instance of Google turning lemons into lemonade?

5. *Google’s New Privacy Policy*

On January 24, 2012, Google announced that it would soon combine almost sixty different privacy policies into one document covering virtually

313. Bradley Horowitz, *A Fall Sweep*, THE OFFICIAL GOOGLE BLOG (Oct. 14, 2011), <http://googleblog.blogspot.com/2011/10/fall-sweep.html>.

314. See Bradley Horowitz, *Buzzkiller*, GOOGLE+ (Oct. 14, 2011), <https://plus.google.com/+BradleyHorowitz/posts/WjNHWiZtYR> (explaining that Google had learned from the Buzz’s failures and would use the experience to improve).

315. See Adams, *supra* note 172.

316. Kashmir Hill, *Why ‘Privacy by Design’ Is the New Corporate Hotness*, FORBES (July 28, 2011), <http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness> (“After flunking Privacy 101 with Buzz, . . . Google has designed a social network with privacy as its building block.”).

317. Users initially criticized Google+ for requiring them to publicize their gender and refusing to allow anonymous names or pseudonyms. See Susana Polo, *Google+ Won’t Let You Keep Your Gender Private, and Why That’s Interesting*, THE MARY SUE (July 8, 2011), <http://www.themarysue.com/google-plus-gender-private>; Bradley Horowitz, *Toward a More Inclusive Naming Policy for Google+*, GOOGLE+ (June 11, 2012), <https://plus.google.com/u/0/113116318008017777871/posts/SM5RjubMmV>.

318. See generally *Know Your Google Security and Privacy Tools*, GOOGLE, <http://www.google.com/goodtoknow/online-safety/security-tools> (last visited Feb. 27, 2012).

319. See Whitten, *supra* note 312.

all of its online services.³²⁰ To ensure that users had sufficient notice of these changes prior to the March 1, 2012 implementation, the company emailed hundreds of millions of users and prominently displayed a notice on its homepage.³²¹ Google justified the new policy as a response to regulatory demands for shorter, simpler privacy terms and explained that the main change would be for registered users, that is, consumers with Google Accounts.³²²

Commentators and politicians alike expressed alarm over the proposed changes, mainly due to Google's decision to combine information across diverse services (some of which were previously separate).³²³ They worried that these changes would create a single, large repository of user data without an easy way for the average user to opt out.³²⁴ EPIC claimed that the proposed changes violated the Buzz consent decree and unsuccessfully sought to compel the FTC to enforce the order against Google.³²⁵ Then, in rapid succession, Members of Congress,³²⁶ state Attorneys General,³²⁷ and

320. See Cecilia Kang, *Google Announces Privacy Changes Across Products; Users Can't Opt Out*, WASH. POST (Jan. 24, 2012), http://articles.washingtonpost.com/2012-01-24/business/35440035_1_google-web-sites-privacy-policies; Alma Whitten, *Google's New Privacy Policy*, GOOGLE OFFICIAL BLOG (Feb. 29, 2012), <http://googleblog.blogspot.com/2012/02/googles-new-privacy-policy.html>.

321. See Eyder Peralta, *Google's New Privacy Policy Will Allow Tracking Across Services*, NPR (Jan. 25, 2012), <http://www.npr.org/blogs/thetwo-way/2012/01/25/145830858/googles-new-privacy-policy-will-allow-tracking-across-services>.

322. Alma Whitten, *Updating our Privacy Policies and Terms of Service*, GOOGLE OFFICIAL BLOG (Jan. 24, 2012), <http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html> (“[Google+’s] new Privacy Policy makes clear that, if you’re signed in, we may combine information you’ve provided from one service with information from other services. In short, we’ll treat you as a single user across all our products, which will mean a simpler, more intuitive Google experience.”).

323. See Hayley Tsukayama, *Google Faces Backlash over Privacy Changes*, WASH. POST (Jan. 25, 2012), http://articles.washingtonpost.com/2012-01-25/business/35439034_1_google-account-google-services-rachel-whetstone.

324. See Samantha Grossman, *Google's New Privacy Policy: Five Ways to Minimize Your Online Exposure*, TIME (Mar. 1, 2012), <http://techland.time.com/2012/03/01/googles-new-privacy-policy-six-tips-for-minimizing-your-online-exposure>.

325. Brenda Sasso, *Judge Dismisses Lawsuit Over Google Privacy Changes*, THE HILL (Feb. 24, 2012), <http://thehill.com/blogs/hillicon-valley/technology/212509-judge-dismisses-lawsuit-over-google-privacy-changes>.

326. Declan McCullagh, *Politicians Aim Some Pointed Privacy Questions at Google*, CNET (Jan. 26, 2012), http://news.cnet.com/8301-31921_3-57367059-281/politicians-aim-some-pointed-privacy-questions-at-google.

327. Letter from Nat'l Assoc. of Attys. Gen. (NAAG) to Larry Page, CEO, Google (Feb. 22, 2012) [hereinafter NAAG Letter], available at <http://www.naag.org/assets/files/pdf/signons/20120222.Google%20Privacy%20Policy%20Final.pdf>.

E.U. privacy officials³²⁸ fired off letters to Google expressing concern and seeking additional information as well as a delay in the proposed changes. In its lengthy reply to Congress, Google reiterated that its intentions were to simplify its privacy policy and enhance user services, and that any newly combined information would not be provided to third parties.³²⁹ Despite a preliminary assessment by the CNIL that the proposed changes violated the European privacy law,³³⁰ they took effect as scheduled on March 1, 2012.³³¹

Google's revision of its privacy policy reinforced its preexisting policy of combining data from services requiring users to sign in (e.g., Gmail but now also Web History, YouTube, and Google+) with data from many other services (including Search). While Google did an admirable job of notifying users of the pending change, critics objected to the all-or-nothing nature of the choice.³³² Far worse, multiple regulators accused Google of misleading consumers by changing its existing privacy policy without consent, failing to provide an adequate opt-out mechanism, and failing to adequately disclose "exactly which data is combined between which services for which purposes."³³³ It is too soon to say what Google might have done differently until all the facts have emerged, but a few preliminary observations are in order. First, Google might have used a multilayered notice to simplify its privacy policy, given that regulators already endorsed this approach.³³⁴ Second, Google might have permitted users to opt out of data sharing, although this would have been inconsistent both with its own model of what it means to give all users "a simpler, more intuitive Google experience"³³⁵ and with the competitive reasons driving its shift to an integrated privacy policy.³³⁶ Third, Google might have been more "forthcoming" in responding

328. See Letter from Commission Nationale de l'Informatique et des Libertés ("CNIL") to Larry Page, CEO, Google Inc. (Feb. 27, 2012) [hereinafter CNIL Letter], available at http://www.cnil.fr/fileadmin/documents/en/Courrier_Google_CE121115_27-02-2012.pdf.

329. Letter from Pablo Chavez, Dir. of Pub. Policy, Google Inc., to Members of Cong. Regarding Privacy Policy (Jan. 30, 2012) [hereinafter Chavez Letter], available at https://docs.google.com/file/d/0BwxyRPFduTN2NTZhNDlkZDgtMmM3MC00Yjc0LTg4YTMtYTM3NDkxZTE2OWRi/edit?hl=en_US.

330. Eric Pfanner, *France Says Google Plan Violates Law*, N.Y. TIMES, Feb 29, 2012, at B9.

331. See Sam Grobart, *Google's New Privacy Policy: What to Do*, N.Y. TIMES: GADGETWISE BLOG (Mar. 1, 2012), <http://gadgetwise.blogs.nytimes.com/2012/03/01/googles-new-privacy-policy-what-to-do>.

332. See NAAG Letter, *supra* note 327.

333. See CNIL Letter, *supra* note 328.

334. *Id.* The Microsoft Privacy Guidelines also recommend layered notices. See *Microsoft Privacy Guidelines*, *supra* note 141.

335. See Chavez Letter, *supra* note 329.

336. See Complaint, *DeMars v. Google*, No. CV12-01382, 2012 WL 4811194 at 5 (N.D. Cal. Mar. 20, 2012), *dismissed sub nom. In re Google, Inc. Privacy Policy Litig.*, 2012 WL

to government inquiries.³³⁷ Whether regulators penalize Google or eventually force it to modify any of these decision remains to be seen. What already seems clear is that Google's decisions were driven neither by the privacy by design principles discussed in Section II.B nor by its new commitment to stronger privacy controls as Whitten previously announced but rather largely by business considerations.

B. FACEBOOK

Facebook is a free, ad-supported SNS with just over 1 billion active users.³³⁸ On May 7, 2012, the company completed an initial public offering with an estimated market value of almost \$100 billion, based on approximately \$4 billion in annual revenues, almost all of which derives from its online advertising business.³³⁹ During its eight years in business, Facebook has suffered numerous privacy controversies, partly as a result of how the service works: users of Facebook create online profiles, which contain a great deal of personal and sensitive information including their name, their interests, the names of their friends, photos and videos they upload, and content they add to their friends' profiles by sending comments and sharing photos.³⁴⁰ Users may also "tag" their friends' images (i.e., identify them by name) without prior consent from those friends³⁴¹ and install games and other applications developed by third parties that obtain access to the profile information of both the users and their friends.³⁴² In short, Facebook, by its

6738343 (2012). DeMars claimed that "Google previously targeted its advertising using bits and pieces of anonymous information garnered from each, discrete Google service," as compared with Facebook's more "holistic view of each consumer." *Id.* ¶ 18. He concluded that "Google's new privacy policy is nothing more than Google's effort to garner a larger market share of advertising revenue by offering targeted advertising capabilities that compete with or surpass those offered by social networks, such as Facebook." *Id.* ¶ 19.

337. See Brendan Sasso, *Google Isn't Being 'Forthcoming' with Congress on Privacy*, THE HILL (Feb. 2, 2012), <http://thehill.com/blogs/hillicon-valley/technology/208385-google-not-forthcoming-during-congressional-questioning> ("I don't think their answers to us were very forthcoming necessarily in what this really means for the safety of our families and our children." (quoting Representative Mary Bono Mack)).

338. See *Key Facts*, FACEBOOK, <http://newsroom.fb.com/Key-Facts> (last visited Mar. 8, 2013).

339. See Shayndi Raice, Anupreeta Das & John Letzing, *Facebook Targets \$96 Billion Value*, WALL ST. J. ONLINE (May 3, 2012), <http://online.wsj.com/article/SB10001424052702304746604577382210530114498.html>.

340. See Samuel W. Lessin, *Tell Your Story with Timeline*, THE FACEBOOK BLOG (Sept. 22, 2011), <http://www.facebook.com/blog/blog.php?post=10150289612087131>.

341. See *What Is Tagging and How Does It Work?*, FACEBOOK, <https://www.facebook.com/help/124970597582337/?q=tagging> (last visited Feb. 27, 2013).

342. See Angwin & Singer-Vine, *supra* note 16 ("[D]on't be surprised if details about your religious, political and even sexual preferences start popping up in unexpected places.").

very nature, raises fundamental privacy challenges because it enables users to disclose unprecedented volumes of highly personal information, not only to friends and friends of friends, but, depending on one's privacy settings, to very large and unfamiliar audiences as well. We review four major Facebook features: News Feed, Beacon, Facebook Apps, and Photo Sharing; as well as a related controversy over ongoing revisions to the company's privacy policies and practices.

1. *News Feed*

Facebook's first major privacy incident occurred in 2006 with the launch of News Feed, a new feature that created a stream of headlines sent to all users based on the activities of their friends throughout the day including newly uploaded pictures, changes in relationships, and so on.³⁴³ News Feed automatically enrolled all Facebook users on an opt-out basis and the feature lacked any controls over what information was shared or with which friends.³⁴⁴ Users reacted with alarm over the unintended consequences of Facebook broadcasting their activities to their entire list of friends.³⁴⁵ Within days, Facebook CEO Mark Zuckerberg released an open letter apologizing to users for “[messing] this one up” by failing to build in privacy controls from the outset, which Facebook promptly corrected by introducing new controls.³⁴⁶ Interestingly, the controversy soon faded as users adjusted to this sudden shift from a “pull” model of sharing updates to a “push” model which, given enough time, they came to appreciate and even depend on.³⁴⁷

What went wrong with News Feed is easily seen. As Grimmelmann points out, News Feed amounted to a “privacy lurch”—that is, “an overnight change that instantly made highly salient what had previously been practically obscure.”³⁴⁸ Similarly, boyd—relying on Altman's work—compares

343. Ruchi Sanghvi, *Facebook Gets a Facelift*, THE FACEBOOK BLOG (Sept. 5, 2006), <http://blog.facebook.com/blog.php?post=2207967130>.

344. See Mark Zuckerberg, *An Open Letter from Mark Zuckerberg*, THE FACEBOOK BLOG (Sept. 8, 2006), <http://blog.facebook.com/blog.php?post=2208562130>.

345. *Id.*; see also Mark Zuckerberg, *Calm Down. Breathe. We Hear You.*, THE FACEBOOK BLOG (Sept. 5, 2006), <http://blog.facebook.com/blog.php?post=2208197130>.

346. Zuckerberg, *supra* note 344.

347. These models are drawn from logistic and supply chain management. See Janet Hunt, *Push System vs. Pull System Inventory Control*, CHRON, <http://smallbusiness.chron.com/push-system-vs-pull-system-inventory-control-12650.html> (last visited Mar. 8, 2013). In a “pull” model, users request information explicitly to be viewed. In a “push” model, information is automatically fed to a user interface that is updated without a user's explicit request, similar to a “ticker” feed in the newsroom, or a news broadcast, where information is flowing to the user in a stream rather than on demand.

348. See Grimmelmann, *supra* note 59, at 1201.

Facebook users to partygoers who felt “protected by the acoustics” of the loud music at a party as they exchanged intimacies with a friend only to find themselves exposed in mid-sentence when the music abruptly stopped.³⁴⁹ Finally, Hull et al. describe the sudden switch to News Feed as “do[ing] violence to users’ norms of distribution.”³⁵⁰ What might Facebook have done differently? At the very least, and consistent with the design guidelines described above, it might have given users more granular controls over information sharing as well as more time to adjust to this new model.³⁵¹

2. Beacon

A year later, Facebook released Beacon, an addition to their developing ad platform.³⁵² Beacon provided targeted ads based on items a user purchased or browsed on the websites of some forty-four partner sites and shared this information with a user’s friends via the News Feed.³⁵³ Although early versions of Beacon apparently included a global opt-out capability, Facebook removed this feature prior to release in favor of more limited privacy controls.³⁵⁴ Moreover, even if a Facebook user decided not to share

349. danah boyd, *Facebook’s “Privacy Trainwreck”: Exposure, Invasion and Drama*, APOPHENIA BLOG (Sept. 8, 2006), <http://www.danah.org/papers/FacebookAndPrivacy.html>.

350. See Gordon Hull et al., *Contextual Gaps: Privacy Issues on Facebook*, 13 ETHICS & INFO. TECH. 289, 297 (2010) (following boyd in chastising News Feed for taking somewhat obscure snippets of social action and making them highly visible); see also *id.*

351. See *supra* notes 200–02, 230 and accompanying text. Does the eventual adaptation of users to News Feed support the view that privacy concerns should not be allowed to hamper the rapid deployment of newer and better technologies, especially where a company believes that “overnight changes” are vital to its success in attracting new customers and achieving network effects? This is a difficult question requiring careful analysis of competing values. See, e.g., NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 229–30. Nissenbaum argues that the adjustments people make to new technologies such as News Feed “will be tempered by explicit and implicit respect for those entrenched context-relative informational norms that have been finely calibrated to support goals, purposes, and values of the context of social life and kinship, such as trust, accommodation, unconditional regard and loyalty.” *Id.* Thus, adaptive patterns may include people seeking out alternative SNSs that are more sensitive to the informational norms of the relevant contexts or adjusting their behavior by finding “workarounds that mimic the constraints of the informational norms they seek.” *Id.*

352. Press Release, Facebook, *Leading Websites Offer Facebook Beacon for Social Distribution* (Nov. 6, 2007), <http://newsroom.fb.com/News/234/Leading-Websites-Offer-Facebook-Beacon-for-Social-Distribution>.

353. Om Malik, *Is Facebook Beacon a Privacy Nightmare?*, GIGAOM (Nov. 6, 2007) <http://gigaom.com/2007/11/06/facebook-beacon-privacy-issues> (“Fandango users could now publish information about the movies they saw [on Facebook].”).

354. See Michael Arrington, *Ok Here’s at Least Part of What Facebook Is Announcing on Tuesday: Project Beacon*, TECHCRUNCH (Nov. 2, 2007), <http://techcrunch.com/2007/11/02/ok-heres-at-least-part-of-what-facebook-is-announcing-on-tuesday> (describing the “number of privacy options” likely to be available to Facebook users, prior to Beacon’s release).

such information with a friend, Facebook still received it.³⁵⁵ Although commentators quickly labeled Beacon “a privacy disaster waiting to happen,”³⁵⁶ Facebook decided to ride out the controversy, hoping that consumers might still “fall in love” with Beacon once they understood it better.³⁵⁷ Instead, Facebook users revolted, voicing concerns over the risk of embarrassment or the ruining of a surprise if activity at a partner website was shared with the wrong friend or at the wrong time.³⁵⁸ As the controversy heated up, Facebook tweaked Beacon’s privacy notice and eventually converted Beacon to an opt-in model, with a global opt-out feature that turned it off entirely.³⁵⁹ But the damage was already done: Facebook discontinued Beacon in 2009 but not before settling a class action lawsuit for \$9.5 million.³⁶⁰

All of the earlier observations concerning News Feed apply, *mutatis mutandis*, to Beacon. As both Grimmelmann and Nissenbaum correctly observe, Facebook’s attempt to fix Beacon by making it easier to opt out was doomed to fail as it should have been opt-in from the start.³⁶¹ Of course, good design practices might have made a difference here, but only if Facebook stepped up to the plate before releasing the new feature. This is a case where a company’s preference for innovation over privacy had predictably unfortunate results.³⁶² Firms already have weak incentives to invest in privacy by design, and giving a pass to any firm for innovative products would only further tip the scales in favor of business goals to the detriment of sound privacy practices.

3. *Facebook Apps*

In 2007, Facebook launched the Facebook Platform, a set of Application programming interfaces (“APIs”) and tools enabling developers to create

355. See Malik, *supra* note 353.

356. *Id.*

357. Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, http://www.nytimes.com/2007/11/30/technology/30face.html?_r=0.

358. See Jim Tobin, *The Problem with Facebook’s “Beacon,”* WEBPRONNEWS (Nov. 27, 2007), <http://www.webpronews.com/backlash-against-facebooks-beacon-2007-11>.

359. See Mark Zuckerberg, *Thoughts on Beacon*, THE FACEBOOK BLOG (Dec. 5, 2007), <http://blog.facebook.com/blog.php?post=7584397130>.

360. Jon Brodtkin, *Facebook Halts Beacon, Gives \$9.5M to Settle Lawsuit*, PCWORLD (Dec. 8, 2009), http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_9_5_million_to_settle_lawsuit.html.

361. See Grimmelmann, *supra* note 59, at 1201–02; NISSENBAUM, PRIVACY IN CONTEXT, *supra* note 182, at 223.

362. See Rubinstein, *supra* note 1, at 1436–40 (discussing the economic reasons why firms underinvest in privacy and security).

hundreds of thousands of third-party applications (“apps”) for Facebook users.³⁶³ Popular apps include games, instant messaging, and a forum for social activists to share their ideas.³⁶⁴ Once approved by Facebook, apps may retrieve or post information to member profiles and request information about users and their friends.³⁶⁵ Users are required to grant access privileges to apps as a condition of installing them.³⁶⁶ However, most applications were given access to far more private information than they needed.³⁶⁷ Moreover, many users lacked understanding of what data they were sharing when they installed an app, either because they hurried through the installation process and ignored notices or relied on the fact that applications ran within the boundary of Facebook, wrongly inferring that their data would remain within the Facebook network.³⁶⁸ These issues led Canadian privacy regulators to investigate such complaints. They found that Facebook lacked adequate safeguards effectively restricting outside developers from accessing a user’s profile information,³⁶⁹ and called for technological measures restricting access to the information that was actually required to run a specific application.³⁷⁰

Facebook responded by restricting third-party app access to only the public parts of a user’s profile unless the user granted additional permission.³⁷¹ It then announced a new permissions model for third-party applications,³⁷² which eventually satisfied the Canadian regulators.³⁷³ A year later, Facebook took additional steps to address privacy issues in third-party apps by releasing a new dashboard allowing users to see exactly how and

363. See Jonathan Strickland, *How Facebook Works*, HOWSTUFFWORKS.COM, <http://computer.howstuffworks.com/internet/social-networking/networks/facebook3.htm> (last visited Mar. 25, 2013).

364. See Jennifer King et al., *Privacy: Is There an App for That?*, in PROCEEDINGS OF THE SYMPOSIUM ON USABLE PRIVACY AND SECURITY (SOUPS) art. 12 (2011), available at http://cups.cs.cmu.edu/soups/2011/proceedings/a12_King.pdf.

365. See Strickland, *supra* note 363.

366. See Lipford et al., *supra* note 219, at 987.

367. See Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs*, U. VA., <http://www.cs.virginia.edu/felt/privacy> (last visited Feb. 27, 2013) (noting that over ninety percent of the top 150 apps received more privileges than they actually needed).

368. See Lipford et al., *supra* note 219.

369. See DENHAM, *supra* note 70, at 37–47.

370. *Id.*

371. Emily Steel & Geoffrey A. Fowler, *Facebook in Privacy Breach*, WALL ST. J. (Oct. 17, 2010), <http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html>.

372. InsideFacebook.com, *Facebook Announces Significant Changes to the Way Applications Can Access User Data*, FACEBOOK (Aug. 27, 2009), http://www.facebook.com/note.php?note_id=123271997739.

373. *Background: Facebook Investigation Follow-up Complete*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (Sept. 22, 2010), http://www.priv.gc.ca/media/nr-c/2010/bg_100922_e.cfm.

when their data has been accessed through the Facebook Platform, and giving users the option to remove unwanted apps, games, or sites, or to revoke persistent permissions.³⁷⁴

Despite laboring to address these longstanding privacy issues, Facebook encountered new problems with third-party apps. For example, a Wall Street Journal investigation revealed that many Facebook apps were not only providing data to advertisers but also linking it directly to users' names and their friends' names.³⁷⁵ Then, in November 2011, Facebook agreed to a consent decree with the FTC based on an eight-count complaint including allegations concerning the consent model of Facebook Apps; it was ordered not to misrepresent "the extent to which it makes or has made covered information accessible to third parties."³⁷⁶ In December 2011, the Data Protection Commissioner of Ireland completed a very extensive audit of Facebook and asked it, *inter alia*, to create a system to allow users to control how their data is shared with third-party apps.³⁷⁷ More recently, a new Wall Street Journal investigation found that even though apps must ask permission before accessing a user's personal details, "a user's friends aren't notified if information about them is used by a friend's app. An examination of the apps' activities also suggests that Facebook occasionally isn't enforcing its own rules on data privacy."³⁷⁸

Facebook Apps is more complex than News Feed or Beacon and raises multiple issues. To begin with, Facebook introduced its apps platform with permissive defaults for developers and overly broad access to profile information, while limiting users to an all-or-nothing choice over what information they had to share as a condition of installing the app. Moreover, Facebook Apps violated norms of distribution by forcing users to share their own and their friends' information in unexpected ways with unknown third parties who were not vetted by Facebook and remained largely invisible to ordinary users, who were in no position to conduct their own evaluations.³⁷⁹

Facebook might have done several things differently and still have succeeded in launching a successful apps platform. First, it might have followed a data minimization approach by restricting what information apps

374. Josh Constine, *How to Use Facebook's Application Settings Dashboard*, INSIDE FACEBOOK (Oct. 7, 2010), <http://www.insidefacebook.com/2010/10/07/how-to-application-settings-dashboard>.

375. Steel & Fowler, *supra* note 371.

376. Facebook Settlement, *supra* note 25.

377. See IRISH AUDIT, *supra* note 70.

378. Angwin & Singer-Vine, *supra* note 16.

379. See Lipford et al., *supra* note 219.

could access from the outset.³⁸⁰ Second, it could have shipped the API with a permissions model and a Dashboard, rather than waiting several years to implement these features—and only then under regulatory pressure. Finally, it might have designed better user interfaces with the goal of disclosing and emphasizing the information flows that occur when users install various apps.³⁸¹

4. *Photo Sharing*

Facebook allows users to share photos with their friends in multiple ways. Users can upload photos to an album, post photos directly to their profile, or post directly to someone else's profile.³⁸² Once a photo has been posted, users may tag it, which creates a link between the tagged photo and a person, page, or place, thereby revealing additional information about the identity and associations of the people depicted in the photo.³⁸³ Users may tag themselves or their friends, who will be notified of the tag.³⁸⁴ Tagging people also alters the potential audience who can view a photo.³⁸⁵ Users can remove the tag from the photo, which removes the explicit reference to the user (by eliminating the link to the user's profile), but the photo remains on Facebook, accessible from any friends' profiles to which it is cross-linked.³⁸⁶

As Facebook tagging has taken off, so has the desire of individuals to retain control over unflattering images.³⁸⁷ Individuals are especially concerned about the unintended results of tagged photos, which may cause embarrassment or humiliation if family, employers, school officials, or law enforcement officials see photos meant for different eyes.³⁸⁸ These tagging

380. See *supra* notes 115–16 and accompanying text.

381. See *supra* notes 200, 230 and accompanying text; see also ANDREW BESMER ET AL., *SOCIAL APPLICATIONS: EXPLORING A MORE SECURE FRAMEWORK* 5 (2009), available at <http://www.andrewbesmer.com/wordpress/wp-content/uploads/2009/08/socialapplications.pdf> (describing an interface prototype for Facebook Apps that “provides a more accurate mental model” of sharing and “serves to catch the user’s attention”).

382. See *Uploading Photos & Profile Pictures*, FACEBOOK HELP CENTER <https://www.facebook.com/help/photos/upload-photos-and-profile-pictures> (last visited July 23, 2012).

383. See *What Is Tagging and How Does It Work?*, FACEBOOK, <https://www.facebook.com/help/124970597582337/?q=tagging&sid=0GzpxRPeunNeIBXiI> (last visited Feb. 27, 2013) (“[I]f you or a friend tags someone in your post and the post is set to Friends or more, the post could be visible to the audience you selected plus friends of the tagged person.”).

384. See *How Tagging Works*, *supra* note 215.

385. *Id.*

386. *Id.*

387. See Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, <http://www.nytimes.com/2008/07/27/education/edlife/27facebook-innovation.html>.

388. See *supra* note 221 and accompanying text; see also Besmer & Lipford, *supra* note 218.

disputes are exacerbated by the fact that the tagging process often involves three distinct individuals—the photographer, the tagger, and the tagged subject—who may disagree over the propriety of tagging a given photo.³⁸⁹ These issues will likely become even more prevalent given Facebook’s creation of the Photo Tag Suggest feature, which uses facial recognition technology to help users tag even more photos.³⁹⁰ Users can opt out of this feature and provide direct feedback about any items that friends post or share.³⁹¹

After the rollout of Photo Tag Suggest, Facebook announced changes in August 2011 to enhance users’ control over who could see photos, tags, and other content.³⁹² The main change was moving the privacy controls from a settings page to an inline control adjacent to the affected photos.³⁹³ Each photo or album now has a drop down menu that allows a user to control exactly who can access it.³⁹⁴ Facebook also added a new Profile Tag Review feature that allowed users to approve or reject any photo in which they were tagged before it became visible on their profile.³⁹⁵ Finally, Facebook changed the way the options for removing tags or content on Facebook are presented to users.³⁹⁶ They now have options to remove a photo from their profile, remove the tag itself, send a message to the owner or tagger, or request that the content be taken down.³⁹⁷ The Irish regulators raised some initial concerns about photo tagging but were generally satisfied by these new controls.³⁹⁸

Photo Sharing introduces a new set of issues involving two kinds of peer-produced privacy violations. The first arises due to the “shrinking perceived audience” problem, in which users indiscriminately disclose potentially embarrassing photos because they forget just how many people can view them notwithstanding their intentions to share them with a much smaller

389. See Grimmelmann, *supra* note 59, at 1137, 1172.

390. See Justin Mitchell, *Making Photo Tagging Easier*, THE FACEBOOK BLOG (June 30, 2011), <https://www.facebook.com/blog/blog.php?post=467145887130>.

391. *Id.*

392. See Chris Cox, *Making It Easier to Share with Who You Want*, THE FACEBOOK BLOG (Aug. 23, 2011), <https://blog.facebook.com/blog.php?post=10150251867797131>.

393. *Id.*

394. *Id.*

395. *Id.*

396. *Id.*

397. *Id.*

398. IRISH AUDIT, *supra* note 70. Section 3.12 of the audit suggests that users be given the option to prevent themselves from being tagged and Facebook has agreed to look into this option. *Id.* § 3.12.

audience.³⁹⁹ The second implicates the social fallout from tagging disputes, where the photographer, the tagger, and the subject disagree over whether the photo should be untagged, made private, or even removed.⁴⁰⁰ As Grimmelmann notes, Facebook is the catalyst of these privacy violations, not the perpetrator.⁴⁰¹

Might Facebook have taken steps to assist users in avoiding or limiting these peer-produced privacy harms? Yes. First, it might have done much more to avoid the “five pitfalls for designers” identified by Lederer et al.—for example, by ensuring that users understood the potential and actual information flows when they posted photos and making it easier for them to configure the relevant privacy settings as part of their ordinary use of the photo-posting feature.⁴⁰² Second, it might have developed innovative privacy tools along the lines of Restrict Others when it released new features such as photo tagging.⁴⁰³ Granted, Facebook did just that in August 2011 with Photo Tag Suggest, but this was already late in the game and in response to regulatory pressure.⁴⁰⁴

5. *Changes in Privacy Settings and Policies*

Over the years, Facebook has modified both its privacy settings and policies many times. Here we focus on the period from late June 2009 to December 2011. On June 24, 2009, Facebook launched a beta version of a “publisher privacy control” that allowed users to decide who can see their published content (status updates, photos, etc.) on a per-post basis using a standardized drop-down menu.⁴⁰⁵ A week later, Facebook moved to simplify its privacy settings by putting them all on the same page and creating a transition tool.⁴⁰⁶ These changes were at least partly motivated by Canada’s far-ranging investigation of Facebook’s privacy practices and policies.⁴⁰⁷ One of the issues that Facebook resolved related to default privacy settings.⁴⁰⁸

399. See Hull et al., *supra* note 350, at 227.

400. See Grimmelmann, *supra* note 59, at 1172.

401. *Id.* at 1164.

402. See *supra* note 200 and accompanying text.

403. See *supra* note 223 and accompanying text.

404. See IRISH AUDIT, *supra* note 70, § 3.12.

405. See *supra* notes 390–97 and accompanying text.

406. Chris Kelly, *Improving Sharing Through Control, Simplicity and Connection*, THE FACEBOOK BLOG (July 1, 2009), <http://blog.facebook.com/blog.php?post=101470352130> (stating that “the compounding effect of more and more settings has made controlling privacy on Facebook too complicated” and noting that the transition tool was designed to respect users’ previous decisions to limit access to information).

407. See DENHAM, *supra* note 70.

408. See *id.*

Although the Commissioner's Office was especially concerned with the default settings for photo sharing (specifically, that "Everyone"—all Internet users—could view the photos) and for public search listings (pre-checked to make name, networks, thumbnail picture, and friends available to search engines for indexing), it concluded that Facebook's plans to introduce a privacy wizard and implement a per-object privacy tool resolved its concerns.⁴⁰⁹

As a result of the Canadian investigation, Facebook modified its privacy policy and settings in August⁴¹⁰ and again in late October.⁴¹¹ Privacy advocates praised Facebook's efforts to simplify privacy settings and liked the transition tool, at least in principle.⁴¹² At the same time, they took issue with several changes, most notably Facebook's expansion of profile information classified as publicly available: from name and network, to profile picture, current city, friends list, gender, and fan pages.⁴¹³ Although Facebook soon backtracked on making friends lists publicly available,⁴¹⁴ EPIC filed a complaint with the FTC urging it to open an investigation into Facebook's revised privacy settings,⁴¹⁵ while Canadian privacy regulators opened a new investigation that was not resolved until September 2010.⁴¹⁶

The next major chapter in this saga occurred in Spring 2010. In April, Facebook made a significant change to how it classified and disclosed users' profiles by requiring all users to designate personal information as publically available "Links," "Pages," or "Connections"; if they declined, Facebook would delete this previously restricted information from their profiles.⁴¹⁷ At

409. *See id.* ¶¶ 88–95.

410. InsideFacebook.com, *supra* note 372 (adopting a "permissions model" for application developers, improving explanations of collection of date of birth and of account deactivation versus deletion, and explaining privacy settings during signup).

411. Elliot Schrage, *Improving Transparency Around Privacy*, THE FACEBOOK BLOG (Oct. 29, 2009), <http://blog.facebook.com/blog.php?post=167389372130>.

412. *See* Nicole Ozer, *Facebook Privacy in Transition—But Where Is It Heading?*, ACLU OF N. CAL. (Dec. 9, 2009), http://www.aclunc.org/issues/technology/blog/facebook_privacy_in_transition_-_but_where_is_it_heading.shtml.

413. *Id.*

414. Caroline McCarthy, *Facebook Backtracks on Public Friend Lists*, CNET (Dec. 11, 2009), http://news.cnet.com/8301-13577_3-10413835-36.html.

415. Brad Stone, *Privacy Group Files Complaint on Facebook Changes*, N.Y. TIMES: BITS BLOG (Dec. 17, 2009), <http://bits.blogs.nytimes.com/2009/12/17/privacy-group-files-complaint-on-facebook-privacy-changes>.

416. DENHAM, *supra* note 70.

417. This profile data included a user's friends list, music preferences, affiliated organizations, employment information, educational institutions, film preferences, reading preferences, and other information. Facebook did not permit users to opt-out of linking their profiles to publicly available "Links," "Pages," or "Connections"; rather, it stated, "if

the same time, Facebook announced two new features: social plug-ins (which added “like” and “recommend” buttons to third-party websites without clearly indicating to users when their profile information might be shared with these websites), and “instant personalization” (which allowed a few select partners to personalize their web pages by using personal information that Facebook disclosed without a user’s explicit consent).⁴¹⁸ These changes were immediately and widely criticized by privacy advocates, bloggers, and Members of Congress, and led EPIC to file a second complaint with the FTC.⁴¹⁹ The bad press continued into the month of May with the *New York Times* publishing, in graphic detail, the complexity of Facebook privacy settings,⁴²⁰ and the *Wall Street Journal* exposing a serious privacy loophole.⁴²¹

Responding to the growing controversy, Facebook announced, in late May, a complete overhaul of its privacy settings.⁴²² The new controls, which were based on extensive consultations with consumers and critics alike, promised to give users “control over how their information is shared” and to avoid sharing personal information “with people or services users don’t want.”⁴²³ This was followed three months later by several more improvements in its privacy controls addressing many of the issues previously identified in complaints filed with the FTC. The major changes

you don’t link to any pages, these sections on your profile will be empty. By linking your profile to pages, you will be making these connections public.” See Complaint, Request for Investigation, Injunction, and Other Relief ¶ 53, Facebook, Inc., EPIC, F.T.C. No. 092-3184 (May 5, 2010), available at http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC Facebook Complaint]. For Facebook’s explanation of these new features, see Alex Li, *Connecting to Everything You Care About*, THE FACEBOOK BLOG (Apr. 19, 2010), <http://blog.facebook.com/blog.php?post=382978412130>.

418. See Austin Haugen, *Answers to Your Questions on Personalized Web Tools*, THE FACEBOOK BLOG (Apr. 26, 2010), <http://blog.facebook.com/blog.php?post=384733792130>.

419. EPIC Facebook Complaint, *supra* note 417.

420. Guilbert Gates, *Facebook Privacy: A Bewildering Tangle of Options*, N.Y. TIMES, May 12, 2010, <http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html> (noting that managing privacy on Facebook means navigating “through 50 settings with more than 170 options”).

421. Emily Steel & Jessica E. Vascellaro, *Facebook, MySpace Confront Privacy Loophole*, WALL ST. J. ONLINE, May 21, 2010, http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html?mod=WSJ_hps_LEFTWhatsNews (describing how Facebook and others gave online ad firms data that could be used to look up individual profiles).

422. See Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, WASH. POST, May 24, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html>.

423. *Id.*

included new inline profile and posting controls, profile and content tag reviews, and the ability to remove tags or content from Facebook.⁴²⁴

In parallel with these changes, Facebook continued to press the boundaries of privacy through the remainder of 2011. In September 2011, Facebook announced several key design changes as well as new opportunities for advertisers.⁴²⁵ The first was a new user interface known as “Timeline,” which included all of a user’s former posts, apps, and Facebook-related information organized into a graphic timeline of the user’s life.⁴²⁶ The second was the concept of “Frictionless Sharing,” a means for users to share their interactions with websites and advertiser’s products automatically with their friends via News Feed.⁴²⁷ The third, what Facebook dubbed “Open Graph,” was a platform that expanded on the notion of frictionless sharing by allowing apps to insert interactions into a user’s News Feed.⁴²⁸ Open Graph also allowed apps to post ads via News Feed.⁴²⁹ Within days, privacy advocates were asking the FTC to ban several of these new features.⁴³⁰ They voiced concerns about the automatic sharing of news articles and other information if users choose to enable “social readers,” and about Facebook’s use of the “Like” button, which continued to track users even after they logged out of Facebook.⁴³¹

At the end of November, Facebook settled with the FTC.⁴³² In the aftermath of the settlement, Zuckerberg publicly conceded that although Facebook had made mistakes in the past, it was now committed to becoming

424. See *Facebook to Allow Users to Pre-Approve Photo Tags*, BILLBOARD BIZ (Aug. 24, 2011), <http://www.billboard.com/biz/articles/news/1173330/facebook-to-allow-users-to-pre-approve-photo-tags>.

425. See Daniel Terdiman, *What Facebook Announced at F8 Today*, CNET (Sept. 22, 2011), http://news.cnet.com/8301-1023_3-20110181-93/what-facebook-announced-at-f8-today.

426. See Samuel W. Lessin, *Tell Your Story with Timeline*, THE FACEBOOK BLOG (Sept. 22, 2011), <https://www.facebook.com/blog/blog.php?post=10150289612087131>.

427. See Mathew Ingram, *Why Facebook’s Frictionless Sharing Is the Future*, GIGAOM (Oct. 3, 2011) <http://www.businessweek.com/technology/why-facebooks-frictionless-sharing-is-the-future-10032011.html>.

428. See Terdiman, *supra* note 425.

429. *Open Graph Concepts*, FACEBOOK DEVELOPERS, <https://developers.facebook.com/docs/opengraph> (last visited Mar. 23, 2012). For example, an auto company could create an app for users to comment on test drives and post this information to their News Feed.

430. See Declan McCullagh, *Groups Ask Feds to Ban Facebook’s ‘Frictionless Sharing’*, CNET (Sept. 29, 2011), http://news.cnet.com/8301-31921_3-20113457-281/groups-ask-feds-to-ban-facebooks-frictionless-sharing.

431. See *id.*

432. See Facebook Settlement, *supra* note 25.

a leader in transparency and user control.⁴³³ According to his blog post, Facebook would begin to formalize privacy reviews by making them part of the company's design and development process.⁴³⁴

European regulators were also concerned with Facebook's privacy practices. On December 12, 2011 the Irish Data Protection Commissioner released a 150-page audit report, by far the most extensive government audit of a major Internet firm to date.⁴³⁵ The report describes numerous changes in policies and practices that Facebook had agreed to, including a new mechanism for users to convey an informed choice for how their information is used and shared on the site and in relation to Third Party Apps, as well as increased transparency and controls for the use of personal data for advertising purposes.⁴³⁶ A few days later, however, Facebook announced that it would post archived user information on Timeline without user consent.⁴³⁷ With this feature scheduled to go live on December 22, 2011, users had just one week to clean up their entire history of Facebook activities.⁴³⁸ This was particularly troubling given Facebook's later announcement that Timeline would ultimately become mandatory for all Facebook users.⁴³⁹

As the year ended, EPIC filed comments with the FTC regarding the November consent decree in which it elaborated on its concerns with Timeline, not only labeling it a privacy risk but pointing out that security experts deemed it a "treasure trove" of personal information that easily could

433. See Mark Zuckerberg, *Our Commitment to the Facebook Community*, THE FACEBOOK BLOG (Nov. 29, 2011, 9:39 AM), <http://blog.Facebook.com/blog.php?post=10150378701937131>.

434. *Id.*

435. See IRISH AUDIT, *supra* note 70.

436. *Id.*

437. Kristin Burnham, *Facebook's New Timeline: Important Privacy Settings to Adjust Now*, CIO (Dec. 21, 2011), http://www.cio.com/article/690742/Facebook_s_New_Timeline_Important_Privacy_Settings_to_Adjust_Now.

438. *Id.*

439. Paul McDonald, *Timeline: Now Available Worldwide*, THE OFFICIAL FACEBOOK BLOG (Dec. 15, 2011) (updated Jan. 24, 2012) (noting that "[o]ver the next few weeks, everyone will get timeline"). Facebook started the migration with "Pages," which automatically switched over to Timeline on March 29, 2012. See Josh Constone, *Don't Dread Today's Mandatory Switch to Timeline, Studies Show It's Good for 95% of Facebook Pages*, TECHCRUNCH (Mar. 29, 2012), <http://techcrunch.com/2012/03/29/mandatory-switch-to-timeline>. Facebook initiated the mandatory transition for users later in August 2012. See Mike Flacy, *Facebook Finally Starts Forcing Timeline on All Users*, DIGITAL TRENDS (Aug. 2, 2012), <http://www.digitaltrends.com/social-media/facebook-finally-starts-forcing-timeline-out-to-users>.

be used to compromise a user's identity.⁴⁴⁰ Users also complained that Timeline revealed too much information, essentially opening up their entire history to anyone they had ever added as a friend.⁴⁴¹ Facebook responded with a blog entry describing several new, privacy-enhancing measures including a seven-day review period before a user's Timeline went live, an activity log, a more easily accessible "view as" feature, the ability to easily control who could view posts (including an "only me" feature), and the ability to limit the audience for past posts.⁴⁴²

Despite years of negative press, user revolts, the exacting scrutiny of privacy advocates, foreign and domestic investigations, audits, settlements, and other concessions, Facebook users still migrated to Timeline as scheduled.⁴⁴³ Moreover, in anticipation of going public, the company continued to experiment with new ways to increase ad revenues by targeting users based not only on their profile information and on-site social activities, but also on their purchasing plans as expressed by their so-called "in-app" activity.⁴⁴⁴ In short, privacy incidents seem to have had limited impact on the company's rapid and relentless pace of product development.

News Feed and Beacon were discrete events that flared up quickly, drew an immediate company response, and then died down or led to the new feature's modification or demise. Along similar lines, Facebook Apps and Photo Sharing, even if more protracted, eventually led to design modifications and/or new privacy settings. However, the controversies surrounding Facebook's frequent changes in privacy policies and settings exhibit a far more complex pattern. Over time, advocacy groups filed

440. EPIC, Comments to the FTC at 27; Facebook, Inc., F.T.C. No. 092-3184 (Dec. 27, 2011), <http://epic.org/privacy/facebook/Facebook-FTC-Settlement-Comments-FINAL.pdf>.

441. See Anthony Bond, *Facebook's Controversial 'Timeline' Feature Is Supported by Just One in Ten Users*, MAIL ONLINE (Jan. 30, 2012), <http://www.dailymail.co.uk/sciencetech/article-2093811/Facebooks-controversial-timeline-feature-supported-just-users.html>.

442. See *Controlling What You Share on Timeline*, FACEBOOK PRIVACY (Dec. 20, 2011), <https://www.facebook.com/notes/facebook-and-privacy/controlling-what-you-share-on-timeline/271872722862617>.

443. See *supra* note 439.

444. See Josh Constine, *Facebook's Revenue Growth Strategy: Ad Targeting by In-App Behavior*, TECHCRUNCH (Feb. 1, 2012), <http://techcrunch.com/2012/02/01/action-spec-ad-targeting/> (describing how "Facebook has been quietly rolling out the beta of 'Open Graph action spec targeting' which allows advertisers to target users by what they listen to, where they travel, what they buy, and other in-app activity"); see also Tanzina Vega, *Substantial Growth in Ads Is on the Way to Facebook*, N.Y. TIMES, Mar. 1, 2012, at B2 (noting that "Facebook is moving all marketers' pages to its new Timeline format that allows advertisers to have more dynamic pages for their own brands" and that "anything posted on an advertiser's own page—status updates, photos and videos—can be made into an ad that can be pushed out to users' newsfeeds and mobile feeds").

complaints with regulators based on a diverse set of accumulated privacy concerns. Many months later, as regulators released their findings, Facebook implemented or announced changes in the relevant practices. But this activity occurred in parallel with a steady flow of fresh or newly designed features; these features often supported, but sometimes undermined, agreed-upon compliance measures and spawned another round of complaints, regulatory demands, and yet another cycle of adjustment.

One might argue that Facebook ought to have slowed both its rapid pace of innovation and its incessant tinkering with privacy settings. The former does not fly, but might the latter? At the very least, Facebook might have avoided coupling privacy revisions at the behest of regulators with sudden changes to how it classified profile information (i.e., as “publicly available”). Second, in making changes in response to regulatory concerns, it might have ensured that any transition tools or privacy wizards it offered were neutral, not self-serving, and given users a full range of privacy-protective options. Third, Facebook might have continued down the road taken in May 2010, when it engaged in consultations with consumers and privacy advocates before overhauling its privacy settings. Indeed, Facebook has taken steps to address privacy issues by adding design staff with a background in HCI, as well as policy professionals with deep privacy expertise.⁴⁴⁵

C. SUMMARY

In sum, the preceding counterfactual analyses suggest that all ten privacy incidents might have been avoided by the application of the engineering and usability principles and related design practices discussed in this Article. This is important for two reasons. First, it strongly supports the claim that privacy by design (when so understood) effectively protects consumer privacy. Second, it also suggests that Part II offers a reasonably comprehensive account of privacy engineering and design practices, at least as measured by these ten incidents. Specifically, notice and informed consent were applicable to all of the incidents except Search; data avoidance and minimization were applicable to Gmail, Search, Street View, Buzz, and Facebook Apps; and data retention limits were applicable to Search. In addition, avoiding design pitfalls (per Lederer et al.)⁴⁴⁶ and following design guidelines (per Hull et al.)⁴⁴⁷ would have improved Buzz, News Feed, Beacon, Facebook Apps, and

445. See Whitney, *supra* note 86 (discussing Facebook’s hiring of Chris Weeldreyer, product design manager from Apple); Zuckerberg, *supra* note 433 (announcing the appointment of Erin Egan as Chief Privacy Officer, Policy, and Michael Richter as Chief Privacy Officer, Products).

446. See *supra* note 200 and accompanying text.

447. See Hull et al., *supra* note 350.

Photo Tagging, possibly averting all of the privacy incidents involving social networking. We suspect that these and other principles and practices described in Section II.B would be relevant to a broader set of privacy incidents.

The ten Google and Facebook privacy incidents also suggest other interesting patterns. Not every incident involved an unmitigated failure—both Gmail and Street View involved a mix of design successes and failures. Several incidents involved norm violations (News Feed and Beacon) or unsettled norms (Gmail and Street View). Quite a few incidents—Street View, Buzz, News Feed, Beacon, Facebook Apps, and Photo Tagging—were characterized by company delay in adding privacy features, revealing a “ship now and ask privacy questions later” mentality.⁴⁴⁸ Both Google and Facebook ran into privacy difficulties when they allowed business necessities to override privacy concerns or forced users into all or nothing choices, specifically in Gmail, Search, Buzz, Google’s new privacy policy, Facebook Apps, and several new Facebook features rolled out at the F8 developers’ conference.⁴⁴⁹ In all of these business-driven cases, the stated rationale of both firms was either opaque or self-serving. Almost all of the Google and Facebook privacy incidents resulted from multiple causes or flaws. Interestingly, only one incident—the Street View Wi-Fi data collection—was attributable to an apparent break down in internal review processes. In short, these patterns seem to confirm that all of these incidents were largely avoidable.

IV. LESSONS LEARNED

Having analyzed what went wrong and what Google and Facebook might have done differently in ten privacy incidents, what have we learned? What lessons does this counterfactual analysis hold for regulators that are now placing bets on privacy by design?

The first lesson is that companies and regulators should avail themselves of the rich body of research related to privacy engineering and usability design as described in Section II.B. Too often, regulators recommend that companies “build in” privacy or “design and implement” reasonable privacy controls, without explaining what they mean.⁴⁵⁰ As designers motivate their

448. Rapid, iterative software development tends to neglect security and privacy requirements, but this is no excuse given the availability of relevant guidance adapted to the fast pace of Agile development methods. *See supra* note 78.

449. *See* Terdiman, *supra* note 425.

450. *See, e.g.*, FTC FINAL REPORT, *supra* note 2, at 2 (“The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data

own work by means of principles and examples, it would be very helpful for regulators to provide more detailed principles and specific examples as well. We hope that Section II.B begins the process of defining what privacy by design means in engineering and design terms.

The second lesson is that usability is just as important as engineering principles and practices. As we have seen, usability and user experiences are especially relevant to the privacy issues that arise whenever people voluntarily share personal information via social networks such as Buzz, Google+, and Facebook. We believe that the best way to preserve the social dynamics of privacy is by following design guidelines as summarized above.

The third lesson is that more work needs to be done on refining and elaborating design principles—both in privacy engineering and usability design. This implies that U.S. and European regulators need to increase their efforts to understand and develop these principles by convening working sessions with companies, academics, user groups, and design professionals; identifying and codifying best practices; funding more research in privacy engineering and usability studies; and encouraging ongoing efforts to define international privacy standards.⁴⁵¹

The fourth and final lesson is that regulators must do more than merely recommend the adoption and implementation of privacy by design. Recommending—or even requiring—privacy by design seems insufficient given the fact that, throughout the period of time involving the ten privacy incidents, Google and Facebook already were committed to embedding privacy into their development processes. And yet these privacy incidents still occurred. It is not at all clear that anything would change if these companies now recommitted—voluntarily or under a regulatory mandate—to adopting privacy by design. Something more is needed.

Recall that Gmail, Search, and Street View are all well-engineered services and that, in advance of their release, Google gave considerable thought to their privacy implications.⁴⁵² Buzz, of course, is different. Was it rushed to market for competitive reasons without a proper internal privacy review? Perhaps. And yet it seems unlikely that a major product release like Buzz

accuracy.”); Google Settlement, *supra* note 25, at 5 (requiring Google to establish a program including “the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment”). In neither case does the FTC explore this notion in greater depth. *Id.*

451. *See, e.g.*, INTERNATIONAL STANDARDS, ISO/IEC 29100 INFORMATION TECHNOLOGY-SECURITY TECHNIQUES-PRIVACY FRAMEWORK (Dec. 15, 2011).

452. For purposes of this argument, we emphasize the notice and consent aspects of Street View, including opt-out and visual blurring mechanisms, and not the disputed aspects of Google’s collection of Wi-Fi payload data.

would escape internal review by Google's privacy experts or that no one realized the privacy implications of the auto-enroll feature. It seems more plausible to suppose that—much like the internal debates at Microsoft over how proposed privacy features in IE 8 might affect business goals such as enabling a desirable ad platform for business partners⁴⁵³—there were internal divisions at Google over whether a more privacy-friendly version of Buzz would hinder business imperatives such as quickly catching up with Facebook and Twitter.⁴⁵⁴ As for Google's newly integrated privacy policy, it strikes the authors as ludicrous to think that Google failed to conduct an internal privacy review before announcing, much less implementing, such major policy changes. To the contrary, the foregoing analysis suggests that these changes were carefully planned and very well executed, notwithstanding the negative reactions they garnered from regulators and the public. Indeed, the Buzz settlement legally obligated Google to implement a comprehensive privacy program and to all appearances it has done so.⁴⁵⁵ So what is happening here? We believe that Google (like many of its peers) understands privacy requirements in a flexible manner that nicely accommodates its own business interests. We believe that the five privacy incidents we examined in Section III.A demonstrate that Google's corporate policy permits it to “balance” privacy requirements against core business goal like increasing advertising revenues.⁴⁵⁶ Furthermore, this balancing process is almost completely hidden from outside observers.

Along similar lines, Facebook, despite its many privacy woes, has long prided itself on offering users extensive control over how they share information and who has access to it. In a nutshell, this is what Facebook seems to mean by privacy—it is a recurrent theme in Facebook's public statements about privacy, dating back at least to September 2005 when it hired its first Chief Privacy Officer.⁴⁵⁷ Of course, Facebook offered very weak controls in rolling out a few early features like News Feed⁴⁵⁸ and Beacon.⁴⁵⁹ But in announcing new privacy settings for News Feed and later

453. See *supra* note 32 and accompanying text.

454. See *supra* note 297 and accompanying text.

455. See Google Settlement, *supra* note 25.

456. See Fleischer, *supra* note 251 (citing “balance” as a factor in Search privacy); Fleischer, *supra* note 263 (citing “balance” as a factor in Street View privacy).

457. See *Making the Internet Safe for Kids: The Role of ISP's and Social Networking Sites: Hearings Before the Subcomm. on Oversight and Investigations of the H. Comm. of Energy and Commerce*, 109th Cong. 214, 215 (2006) (written statement of Chris Kelly, Chief Privacy Officer, Facebook) (“[W]e put power in our users' hands to make choices about how they reveal information.”).

458. See *supra* Section III.B.1.

459. See *supra* Section III.B.2.

products, Zuckerberg and other company officials consistently described what they were doing in terms of developing new privacy controls.⁴⁶⁰ Even after Facebook settled with the FTC, at which point it was legally obligated to implement a comprehensive privacy program, Zuckerberg insisted that giving people “complete control over who they share with at all times” has been “the core of Facebook since day one.”⁴⁶¹ And while Zuckerberg conceded that the company had to “improve and formalize the way we do privacy review as part of our ongoing product development process,” he continued to emphasize the “more than 20 new tools and resources designed to give you more control over your Facebook experience.”⁴⁶² In short, Facebook, just like Google, has its own preferred and idiosyncratic way of defining privacy. For Facebook, privacy means giving users multiple controls and settings over profile and other information sharing on a feature-by-feature basis, which may be redesigned from time to time when the sheer number and complexity of these controls becomes overwhelming. Like Google, however, Facebook always reserves the right to weigh the need for any privacy controls against business objectives such as maximizing advertising revenues, and it too reaches these decisions behind closed doors.⁴⁶³

460. See Press Release, Facebook, Facebook Launches Additional Privacy Controls for News Feed and Mini-Feed (Sept. 8, 2006), <http://www.marketwire.com/press-release/facebook-launches-additional-privacy-controls-news-feed-mini-feed-facebook-responds-7751-81.htm> (“[The features] put control of who sees what information . . . directly into the hands of our users, just as they requested.” (quoting Mark Zuckerberg, founder and CEO)). Chris Kelly used similar language when he testified before Congress for a second time two years later. See *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 110th Cong. 40, 41 (2008) (statement of Chris Kelly, Chief Privacy Officer, Facebook) (“Facebook follows two core principles: First, you should have control over your personal information Two, you should have access to the information that others want to share.”). Elliot Schrage did the same in announcing Facebook’s August 2009 response to the recommendations of the Canadian privacy regulators. See *Facebook Announces Privacy Improvements in Response to Recommendations by Canadian Privacy Commissioner*, FACEBOOK NEWSROOM (Aug. 27, 2009), <http://newsroom.fb.com/News/194/Facebook-Announces-Privacy-Improvements-in-Response-to-Recommendations-by-Canadian-Privacy-Commissioner> (“Our productive and constructive dialogue with the Commissioner’s office has given us an opportunity to improve our policies and practices in a way that will provide even greater transparency and control for Facebook users.” (quoting Elliot Schrage, Vice-President of Global Communications and Public Policy)). Zuckerberg most recently echoed this sentiment in a May 2010 op-ed announcing Facebook’s plans to redesign its privacy controls. See Zuckerberg, *supra* note 422 (“If we give people control over what they share, they will want to share more.”).

461. Zuckerberg, *supra* note 433.

462. *Id.*

463. See Joseph Bonneau & Sören Preibusch, *The Privacy Jungle: On the Market for Data Protection in Social Networks*, WEIS ‘09: PROCEEDINGS OF THE EIGHTH WORKSHOP ON THE

Given these behaviors of Google and Facebook, the fourth lesson, then, is that regulators wishing to embrace privacy by design must grapple with the inherent tensions between business models that seek to monetize personal data, and engineering and usability principles which, if properly implemented, tend to inhibit the collection and use of such data, and the balancing that companies undertake as part of their internal business processes. It follows that if regulators want privacy by design to be an effective means of improving consumer privacy, they must take at least two additional steps.

To begin with, regulators must ensure that when companies balance privacy design requirements against business objectives, they adhere to the well-established engineering and usability principles discussed throughout this Article. Because business and privacy demands often conflict, companies would benefit from regulatory clarity. Without well-defined guidelines about what it means to implement privacy by design, business considerations will always prevail over privacy: internal privacy champions will never have enough weight on their side to win the close calls.⁴⁶⁴ In contrast, if regulators developed a reasonableness standard for designing privacy into products and services, companies would both know what was expected of them and take design requirements more seriously in achieving an appropriate balance.⁴⁶⁵

ECONOMICS OF INFORMATION SECURITY 1 (2009) (arguing that the “economically rational choice for a site operator is to make privacy control available to evade criticism from privacy fundamentalists, while obfuscating the privacy control interface and privacy policy to maximise sign-up numbers and encourage data sharing from the pragmatic majority of users”). Thus Bonneau and Preibusch claim that Facebook deploys “overly-complicated privacy settings with open defaults . . . [to] reduc[e] privacy complaints while still minimising salience.” *Id.* at 31.

464. See Bamberger & Mulligan, *supra* note 5, at 274, 277.

465. The Proposed E.U. Regulation would require data controllers to “implement *appropriate* technical and organisational measures” for safeguarding personal data. *Proposed E.U. Regulation*, *supra* note 2, art. 23(1) (emphasis added). Similarly, In the United States, section 103 of the proposed Commercial Privacy Bill of Rights Act would have required:

Each covered entity shall . . . implement a comprehensive information privacy program by—

(1) incorporating necessary development processes and practices throughout the product life cycle that are designed to safeguard the personally identifiable information that is covered information of individuals based on—

(A) the reasonable expectations of such individuals regarding privacy; and

(B) the relevant threats that need to be guarded against in meeting those expectations

Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. § 103 (2011).

Additionally, regulators should consider developing oversight mechanisms that would allow them to assess whether companies that claimed the mantle of privacy by design are adhering to the engineering and usability principles identified in this Article and related works. For example, they might require companies to maintain privacy design documents and, if appropriate, disclose them in the event of an investigation or lawsuit. Of course, disclosure is no magic bullet. Requiring disclosure after the fact may have less effect on the way that companies make privacy decisions than on how they discuss and document them.⁴⁶⁶ It worth noting, however, that firms, U.S. regulators, and European regulators have already begun experimenting with maintaining privacy-related documentation,⁴⁶⁷ which might be easily extended to cover “design documents”⁴⁶⁸ as well.

V. CONCLUSION

Privacy regulators in both the United States and Europe are placing great faith in privacy by design as they set out to reform existing privacy regimes

466. We thank Tal Zarsky for sharing this observation. For discussion of effective transparency policies, see generally ARCHON FUNG ET AL., *FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY* (2007). For additional discussion of regulatory approaches to privacy by design, see Rubinstein, *supra* note 1, at 1444–53; Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S: J.L. & POLY INFO. SOC'Y 355 (2011).

467. As previously noted, this is already the case for Google. *See supra* note 310 and accompanying text (describing Google’s voluntary pledge to maintain privacy design documents for internal purposes). In the United States, the FTC consent decrees with both Google and Facebook obligate them to develop comprehensive privacy programs and to conduct third-party audits certifying that these programs satisfy the requirements of the FTC order, while maintaining pertinent records, which extends to “all materials relied upon . . . including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments.” *See Google Settlement, supra* note 25, at 6; Facebook Settlement, *supra* note 25, at 7–8. In Europe, Article 25 of the Proposed E.U. Regulation introduces the obligation for controllers and processors to maintain documentation of the processing operations under their responsibility. *Proposed E.U. Regulation, supra* note 2, art. 25. If read in conjunction with Article 23 (data protection by design and default), this documentation requirement arguably covers “design documents.” *Id.*, art. 23.

468. For UX specialists, “design documents” address alternative designs considerations in the form of mockups, wireframes, presentations, etc. *See Design Documents in Programming Methodology*, EXFORSYS INC. (Sept. 17, 2006), <http://www.exforsys.com/tutorials/programming-concepts/design-documents-in-programming-methodology.html> (“[T]he design document gives in a nutshell the main idea and structure of the product that would be developed by developers.”). For example, an early mockup might have a button clicked on instead of off. More broadly, design documents in engineering might include information about every version of code stored in a code repository including comments, code changes, authors, date and time.

and make them more protective of consumers. This Article's goal has been to show what privacy by design might entail by undertaking a counterfactual analysis of ten privacy incidents. These incidents included five from Google—Gmail, Search, Street View, Buzz, and recent changes to its privacy policy; and five from Facebook—News Feed, Beacon, Facebook Apps, Photo Sharing, and recent changes to its privacy policies and settings. Using engineering and usability principles and practices derived from the research literature and described in Section II.B, we determined that each of these incidents might have been avoided if Google and Facebook had followed these principles and practices. Moreover, we described in specific detail what the two companies might have done differently in each of the ten cases.

This Article also explored the strengths and weaknesses of FIPs as the basis for privacy engineering and repeatedly emphasized the need to complement a FIPs-based engineering approach with engineering and usability principles and an extension of such principles to address the “social dynamics” of privacy. It explored the connections between privacy and existing design processes, such as UX design, which focus on usability. It also provided a more detailed look at privacy design pitfalls and guidelines inspired by the work of Altman and Nissenbaum. Sections III.A and III.B offered ten case studies and counterfactual analyses, which found that privacy engineering and usable privacy design were highly relevant to evaluating and overcoming a range of privacy problems including emergent issues affecting social networking services. The Article closed with a few modest lessons for regulators, which should be heeded if privacy by design is to achieve its promise of improving consumer privacy.

