INFORMATION PRIVACY AND DATA SECURITY

Lauren Henry[†]

Legal academic and policy discourse generally presumes that information privacy and data security are interchangeable goals. The conventional wisdom is that data security is a handmaiden of information privacy, and so what serves data security will serve information privacy. However, this view is an oversimplification of the relationship between the two fields. This Essay aids law and policy development in both fields by correctly defining their relationship to one another. Data security has separate objectives from information privacy that can be agnostic or even in opposition to information privacy. The law should acknowledge information privacy and data security as separate institutional objectives to prevent undesirable—or at least unpredictable—results in edge cases in which data security's objectives run counter to those of information privacy.

TABLE OF CONTENTS

† Knight Law and Media Scholar and Resident Fellow, Information Society Project at Yale Law School; J.D., Harvard Law School. The author would like to thank Derek Bambauer, David Thaw, Viktor Mayer-Schönberger, Lea Shaver, Tamara Piety, Cory Francis Myers, Christina Spiesel, Jack Balkin, and the participants in the Harvard-Yale-MIT-Columbia Cyberscholars Workshop Series for comments on earlier drafts of this essay.

INTRODUCTION

In legal academic writing and policy discussions alike, information privacy and data security are typically handled together, with the unexamined assumption that data security falls under the broad heading of information privacy.[1] The Federal Trade Commission handles information privacy and data security cases in similar ways, under the same grant of authority,[2] and draws upon the same group of experts for handling both types of cases.[3] Derek Bambauer has observed that there is widespread conflation in the existing legal literature between information privacy and data security issues.[4] By contrast, until the past decade or so, industry had largely tackled data security and information privacy separately.[5] In fact, companies are still dismantling the legacy practice of solving problems of information privacy and data security through entirely separate corporate channels.[6] Only within the past decade or so have industry professionals begun to consciously work to bring the distinct field of information privacy and data security

---

1 *E.g.*, Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013) ("During the past decade, the problems involving information privacy—the ascendance of Big Data and fusion centers, the tsunami of data security *breaches*, the rise of Web 2.0, the growth of behavioral marketing, and the proliferation of tracking technologies—have become thornier." (emphasis added)); Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1637 (2013) ("To illustrate current state privacy laws, we can begin with those state data security laws that impose a substantive requirement of 'reasonable security' before any data processing may occur."); Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1814–15 (2010) (citing data security breaches as an example of cases in which financial injuries can be multiplied in the modern digital age).

2 *See* Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 610–19 (2014) (discussing data security-focused enforcement actions alongside information-privacy enforcement in a discussion of the FTC's use of its authority in these areas); Lauren Henry, Note, *Institutionally Appropriate Approaches to Privacy: Striking a Balance Between Judicial and Administrative Enforcement of Privacy Law*, 51 HARV. J. ON LEGIS. 193, 201–11 (2014) (discussing the FTC's common approach to the information privacy and data security matters it has addressed since the mid-1990s through analyzing all of the major enforcement actions over that time period, with an emphasis on decoding how the FTC's approach has evolved).

3 Press Release, Fed. Trade Comm'n, FTC Seeks Technologists for New Research, Investigations Office (Mar. 23, 2015), https://www.ftc.gov/news-events/press-releases/2015/03/ftc-seeks-technologists-new-research-investigations-office ("The OTRI will provide expert research, investigative techniques and further insights to the agency on technology issues involving all facets of the FTC's consumer protection mission, including privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things.").

4 *See* Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667 (2013).

5 *E.g.*, Daniel Krege Christensen & Malcolm Harkins, Look, C-Suite, No Hands! Communicating the Top 10 Privacy and Security Topics to Executives (Mar. 6, 2015), *available at* https://privacyassociation.org/media/presentations/15Summit/S15_Look_C_Suite_PPT.pdf. The IAPP Global Privacy Summit is an annual conference that provides continuing education for privacy professionals, as well as an important opportunity to network with others in the field.

6 *Id.*

together to learn from one another.[7]

There are few works expressly dedicated to building a theory of how information privacy and data security interrelate. A notable exception to this is Derek Bambauer's *Privacy Versus Security*, in which Bambauer defines information privacy and data security and stresses the importance of keeping the two separate at law.[8] However, Bambauer does not go far enough in distinguishing between information privacy and data security. Bambauer defines data security as the technology and institutional practices that implement the normative decisions an institution has made about information privacy.[9] While Bambauer stresses the importance of keeping information privacy and data security separate,[10] he also defines the two fields in such a way that data security's objectives necessarily serve information privacy's objectives.

This Essay contends that data security has separate objectives from information privacy that is agnostic or even in opposition to information privacy. The law should acknowledge information privacy and data security as separate institutional objectives to prevent undesirable—or at least unpredictable—results in edge cases in which data security's objectives run counter to those of information privacy.

This Essay will proceed as follows. First, it will briefly define information privacy and data security, and sketch their status in law and industry. Second, it will examine reasons why scholars and lawyers have struggled to keep them separate. Third, it will discuss how and why information privacy and data security have often been handled separately in practice. Fourth, it will discuss the characteristics of the relationship between information privacy and data security and the consequences of that relationship. Information privacy and data security are linked from the perspectives of institutions that handle personal information due to their shared relationship to databases that contain personal information. However, an institution's interest in its own data security is not necessarily consonant with the information privacy interests of the individuals whose personal information is housed. Finally, the Essay concludes with some observations about the implications of my analysis and the future research it suggests.

I. DEFINITIONS

This section will broadly and briefly define both information privacy and data security. The way in which information privacy and

---

[7] *Id.*
[8] Bambauer, *supra* note 4.
[9] *Id.*
[10] *Id.*

data security are defined and their significance is somewhat bifurcated. As Kenneth Bamberger and Deidre Mulligan have noted in their influential Stanford Law Review article, *Privacy on the Books and on the Ground*, the actual contours of privacy at law and the definitions used in industry are quite different.[11]

The predominant definition of information privacy in American legal literature and existing statutory law defines information privacy as the right to control one's personal data.[12] This puts a large amount of emphasis on notice and consent. Privacy, from this point of view, has no substantive content. It is an individual right to have control over data. This point of view has been widely critiqued because it appears to give undue legitimacy to clickwrap contracts and other forms of "consent" that do not seem to reflect any actual understanding by individuals of information usage by other actors.[13] The sheer number and complexity of privacy policies are impracticable for any person to read, and, even if they did, cognitive biases tend to limit the average person's ability to rationally pursue their self-interest in the market for information privacy.[14] However, even where the power of notice, transparency, and consent is questioned, many privacy advocates merely seek to replace formal consent with a thicker, "meaningful" consent.[15]

---

[11] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 295 (2011) ("While the dominant account of U.S. privacy regulation—of privacy 'on the books'—correctly argues that U.S. law fails to provide the robust [Fair Information Practice Principles (FIPPs)] protections and comprehensive rule and enforcement structures developed in Europe, the alternative account illuminates the concurrent entry of a new force into the regulatory space—the FTC—and the way in which its activities, together with the involvement of advocates, professionals, and market forces, helped frame a new discourse regarding privacy protection.").

[12] *E.g.*, Charles Fried, *Privacy*, 77 YALE L. J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."). Helen Nissenbaum's contextual integrity approach is gaining momentum as a counter approach in policy discussions. *E.g.*, Michael Hoven, *Balancing Privacy and Speech in the Right to Be Forgotten*, JOLT DIGEST (May 2, 2012), http://jolt.law.harvard.edu/digest/privacy/balancing-privacy-and-speech-in-the-right-to-be-forgotten (discussing the debate over the right to be forgotten using contextual integrity as the working definition of the privacy interest); *see generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010). Another increasingly influential approach is Julie Cohen's autonomy-based approach to information privacy protection. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject As Object*, 52 STAN. L. REV. 1373, 1423–36 (2000). Other historically significant approaches to privacy include intimacy and the reasonable expectation approach adopted in Fourth Amendment jurisprudence. JULIE C. INNESS, PRIVACY INTIMACY AND ISOLATION (1992) (discussing privacy as intimate); Smith v. Maryland, 442 U.S. 735 (1979) (elaborating the reasonable expectation of privacy test).

[13] Solove, *supra* note 1, at 1880–82.

[14] *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S J.L. & POL'Y FOR INFO. SOC'Y 540 (2008) (empirical study showing the barriers, both practical and psychological, to the average person meaningfully reading, understanding, and responding rationally to privacy policies).

[15] Solove, *supra* note 1, at 1881 ("With each sign of failure of privacy self-management, however, the typical response by policymakers, scholars, and others is to call for more and

By contrast, in industry and in the Federal Trade Commission's regulation thereof through enforcement actions, the predominant approach to privacy is to construct a regime for using personal information that comports with a conservative reading of social norms surrounding information privacy. As Bamberger and Mulligan stated:

> Each of the corporate privacy leaders . . . understood the meaning of "privacy" to depend on the beliefs and assumptions of consumers as to the appropriate treatment of individual information and personal identity—expectations that evolve constantly and change by context. The success of privacy protection, then, would be measured not by the vindication of notice and consent rights, but in the actual prevention of substantive harms, such as preventing data breaches, or treating information in a way that protects the "trust" of those whose information is at stake.[16]

In practice, companies have an understanding of information privacy as a collective benefit for the community of users, as opposed to an interest held by each individual user.[17] Put another way, industry and the FTC tend to weigh the privacy interests of the community against the cost in terms of ensuring those privacy preferences are met, as opposed to weighing the interest of an individual against innovation at large, as industry and the FTC tend to do.[18] There may be a collapse of these two approaches, as recent scholarship has argued for a transfer of the industry approach to privacy to legal understandings of privacy, but as of the time of this writing, the difference between the definition of privacy in policy and in industry practice remains. For the purposes of this Essay, when I refer to "information privacy," I mean a definition of information privacy as combining the two: those series of policies with respect to collected personal information that reflect an individual's liberty interest in deciding what to do with that information and social norms regarding how personal information should be used, distributed, and processed.[19]

---

improved privacy self-management."). In many ways, the call for a form of consent outside of the formal content of adhesion content harkens back to earlier discussions of contract law, in which some argued that contracts of adhesion are and should be governed by different standards from normal contracts. Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1176 (1983) ("My broad conclusion is that, quite contrary to 'ordinary' contract law, the form terms present in contracts of adhesion ought to be considered presumptively (although not absolutely) unenforceable. . . . I try to show how this broad conclusion, and its more detailed ramifications, can be transformed into at least the outline of new doctrine.").

16 Bamberger & Mulligan, *supra* note 11, at 251–52.

17 *Id.*

18 *See* Henry, *supra* note 2, at 194–98 (arguing that administrative agencies are well-suited to balance one societal interest against another, in contrast to courts, which are designed for bipolar disputes).

19 The author does not endorse this as the only proper definition of privacy, a theoretically multifaceted concept. The literature attempting to define and classify privacy is vast. *E.g.*, Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 211–13 (2012); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 484 (2006) (two recent taxonomies of

The definition of data security understanding is similar in the law literature, the case law, and in industry: it roughly means institutional rules and technical methods that an institution uses to ensure that data is only accessed by authorized people.[20] In contrast to information privacy, in which overwrought debates about the exact meaning of the term can veil actual consensus on what problems privacy law should solve,[21] fewer scholars examine what is meant by data security and how the law approaches its regulation.[22] Many policymakers and scholars assume that data security is a self-evident term. However, the supposed simplicity of data security[23] is a chimera, as this Essay's discussion will illustrate. Often the difficult ethical questions in data security are shoehorned under the heading of information privacy. For example, the moral obligation of credit card companies and retailers to take basic steps to avoid breach is very often described as an information privacy issue when it is clearly a data security issue.[24]

Having sketched the two major terms at stake, the Essay now

---

privacy at law and in society).

[20] While this is the understood meaning, detailed definitions of data security are rare, despite the prevalence of state data security laws. John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 206 (2013) ("Although several states have data security laws that require businesses to adopt reasonable security measures to protect personal information, of which the most notable and comprehensive may be Massachusetts Regulation 17, those statutes do not define what constitutes reasonable data security." (citations omitted)). One statute that features a rigorous definition of data breach is found in California's Security Breach Information Act (SBIA). The SBIA defines a "breach of the security of the system" as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information." CAL. CIV. CODE § 1798.82(d) (West 2015).

[21] *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008) (advocating for a "family resemblances" approach to information privacy that would target policy making at solving the assortment of social problems arising in the information privacy space); Lauren Henry, Levels of Privacy Policy Analysis (May 1, 2015) (unpublished manuscript) (on file with author) (arguing that privacy problems can be divided into four levels of analysis, and as long as there is consensus on a lower, more practical level of analysis as to how to address a given problem, there is no need to seek consensus on the higher, more theoretical levels; *i.e.*, if there is broad social agreement that individuals have a privacy interest in their home, there is no need to establish whether society is grounding its approach to privacy under control, intimacy, contextual integrity, or any other particular theoretical approach).

[22] For an example of this uncommon, but important, type of work see generally David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2014) (classifying, describing, and evaluating approaches to regulating data security).

[23] *E.g.*, Bambauer, *supra* note 4, at 676 (Bambauer highlights the perception of data security debates as a morally uncomplex area, while gesturing toward the normative debates hiding just beneath the surface: "Security's debates are more cold-blooded and technical—they are about relative informational advantages, the ability to bear costs, and the magnitude and probability of harm. Like precautions against civil harms (the domain of tort law), security measures exist along a continuum. Perfection is generally unattainable or unaffordable. Where there are normative choices—such as who should bear residual risk—they tend to be more deeply buried, or subsumed in utilitarian methodologies." (citations omitted)).

[24] *E.g.*, Kashmir Hill, *Hackers Breaking Into Baby Cams Are Actually Trying to Help*, FUSION (Apr. 7, 2015), http://fusion.net/story/115649/hackers-breaking-into-baby-cams-are-actually-trying-to-help (framing some baby camera companies' refusal to provide security that is now known to be hackable by anyone with an Internet connection as a morally reprehensible refusal to provide data security at a level that any parent is entitled to expect).

moves to discuss the major similarities and differences between the two fields.

II. INFORMATION PRIVACY AND DATA SECURITY'S COMMONALITIES

As the previous section illustrates, information privacy and data security can be conceptually distinguished. This section will discuss the commonalities between the two fields by way of explaining the impulse to conflate the two. Information privacy and data security speak to the same databases, and concern trust and legitimacy issues from the consumer perspective. More discussion and examples of these commonalities follows.

First, similar facts are pertinent to both information privacy and data security. The way in which actors collect, store, and distribute the personal information they hold about others reflects those institutions information privacy policies and their data security policies. An increasing number of institutions that are voluntarily provided with personal information are seeking ways to learn from and create income from the information in their possession.[25] Furthermore, other companies are in the business of collecting or purchasing information without the direct action of the consumer to form "digital dossiers" about the characteristics of individuals.[26]

Second, actors' incentive to give attention to both information privacy and data security comes from trust and legitimacy concerns. From the perspective of consumers, whether their personal information is distributed with the consent of the institution housing it or not, if the information ends up in a place that the consumer does not like, it reflects poorly on that institution. Whether it is a matter of information privacy or data security, from the perspective of the consumer, increasing the vulnerability or distribution of information in a socially unacceptable or "creepy"[27] way erodes the trust they have in that institution. The consumer's pragmatic, consequentialist attitude toward breaches of trust promotes the theoretical collapse of information

---

25 *A Different Game: Information Is Transforming Traditional Businesses*, The ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557465.

26 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002) ("In the Information Age, an increasing amount of personal information is contained in records maintained by Internet Service Providers (ISPs), phone companies, cable companies, merchants, bookstores, websites, hotels, landlords, employers, and private sector entities. Many private sector entities are beginning to aggregate the information in these records to create extensive digital dossiers.").

27 *See generally* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 61–71 (2013–2014) (defining and characterizing innovations in data trafficking that consumers have found "creepy" and have led in a pivot in institutional practice).

privacy and data security.[28] When either a privacy or data security breach reflects a sharp deviation from social norms without anything approximating constructive notice or consent, the legitimacy of the institutions and the progress of technology are compromised.[29] This intuition is why several privacy scholars have proposed theories of privacy invasion centered on a breach of confidence.[30] Depending on how the breach of confidence is defined, some information privacy and data security transgressions could both be barred.[31]

III. HOW INFORMATION PRIVACY AND DATA SECURITY ARE SEPARATED IN PRACTICE

Despite the overlaps discussed above, information privacy and data security can be siloed into very different parts of professional practice. The first section has already defined information privacy and data security as distinct theoretical concepts.[32] Information privacy is that

---

[28] A confidentiality approach to information privacy and data security, which tends to correspond to these consumer intuitions, has support in the common law and has been developed by Woodrow Hartzog. *See* Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 767 (2014) (discussing implied confidentiality in the offline context and suggesting how that doctrine could be applied to the digital context).

[29] *See* Lauren Henry, *Privacy Claims and Institutional Legitimacy*, 37 CARDOZO L. REV. (forthcoming 2016) (arguing that the reception and transparent disclosure of privacy complaints regarding creepy features of modern technologies would help legitimize institutional leaders that are modifying social practices, and give public and private actors concrete ideas for how to minimize dead weight loss from socially detrimental aspects of innovation in the information-privacy space).

[30] *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1312 (2000) (arguing for an approach to privacy at common law in tort based "loosely on the tort doctrine of breach of confidence"); Lauren Henry, *Privacy as Quasi-Property*, 101 IOWA L. REV. (forthcoming 2016) (arguing for an approach to privacy at common law in tort based on the quasi-property model; wherein a relationship of trust or wrongful act or act contrary to social norms can permit the law to simulate property's right to exclude, and thus torts in trespass and misappropriation); Jack Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (Mar. 5, 2014), http://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html ("The idea of an information fiduciary matters when the fiduciary discloses or uses sensitive information about the beneficiary to the beneficiary's disadvantage without permission.").

[31] Some have argued that intent is required for a duty to be violated, whereas the pure incompetence or bad luck as the target of a very sophisticated hack normally associated data security with could never rise to that level. *See generally* Bambauer, *supra* note 4. When one looks into the details of certain data security matters, that position becomes untenable. However, there is increasing evidence that some actors who traffic in data are willfully lax in how they store their data in order to save money because of the asymmetry between the costs and the harms. It is actually a moral question: how much effort is a holder of data obligated to take in order to attempt to avoid data breaches?

[32] Derek Bambauer has argued that there are benefits to a rigorous theoretical distinction between information privacy and data security. Bambauer, *supra* note 4. His analysis uses different definitions of information privacy and data security than this Essay, with the effect of moving most of the easy cases into the data security category. *Id.* As he writes:

> Privacy discourse involves difficult normative decisions about competing claims to legitimate access to, use of, and alteration of information. It is about selecting among

series of policies with respect to collected personal information that reflect an individual's liberty interest in deciding what to do with that information and social norms regarding how personal information should be used, distributed, and processed. Data security comprises of the rules an institution selects and implements to ensure that only authorized people access data. This section discusses the practical reasons why the two fields remain separate, which include different training for professionals, different institutional cultures around developing policy, and different insurance against breaches.

First of all, information privacy and data security professionals tend to have different training. A legal or policy background is considered more pertinent for privacy, whereas information technology or computer science training is perceived as more pertinent for data security.[33] This discrepancy is seen in the training necessary to obtain information privacy certification, as opposed to data security certification. The most common information privacy certification is the Certification in Information Privacy Policy (CIPP), which is in law and regulations, outstripping the Certification in Information Privacy Technology (CIPT), among those who claim the certification on LinkedIn, five fold.[34] By contrast, the preponderance of certified people and types of certification in Global Information Assurance Certification, the leading data security certification body, are in technical spaces.[35] Furthermore, the culture surrounding hacking clearly implicates data security but rarely conceptualizes itself as having something to say about information privacy.[36] Different skills are perceived to be relevant for individuals who work on information privacy versus data security, although there is a trend toward encouraging the hiring and development of technically skilled people in information privacy.[37]

> different philosophies and choosing how various rights and entitlements ought to be ordered. Security implements those choices—it mediates between information and privacy sections. Importantly, [Bambauer's] approach argues that security failings should be penalized more readily, and more heavily, than privacy ones, because there are no competing moral claims to resolve and because security flaw make all parties worse off.

Id. at 683. My analysis, by contrast, proceeds from the observation that information privacy and data security are procedures making distinct kinds of decisions. Both have philosophical and practical elements, and force stakeholders to address easy and hard questions.

33 Bamberger & Mulligan, *supra* note 11, at 262.

34 It may also be instructive to evaluate how common the credentials used by certified persons are in public-facing forums, to gauge the industry value of the credential. On LinkedIn, as of April 9, 2015, 6,596 profiles listed CIPP certification, compared to only 1,331 listing CIPT certification. LINKEDIN, https://www.linkedin.com (last visited Apr. 9, 2015).

35 ABOUT: MISSION STATEMENT, GLOBAL INFORMATION ASSURANCE CERTIFICATION, https://www.giac.org/about/mission (last visited Apr. 10, 2015).

36 *See, e.g.*, THE DEF CON STORY, DEF CON COMMC'NS, INC., https://defcon.org/html/links/dc-about.html (last visited Apr. 10, 2015).

37 Lorrie Faith Cranor, *Wanted: Privacy Engineers*, INT'L ASS'N OF PRIVACY PROF'LS, https://privacyassociation.org/news/a/wanted-privacy-engineers (noting that organizations "are looking for experts who can help them build privacy into their products from the ground up" but

Information privacy issues are increasingly handled at the executive level. Data security tends to be more of a departmental issue and is as likely as not to be handled by consultants or contractors in large companies. Privacy is considered to be a "strategic" issue, which has led to a growing percentage of large companies with Chief Privacy Officers.[38] CPOs often handle data security at a strategic level, but as the title suggests, the primary mission of such individuals and offices is data privacy considerations.

The strategy that institutions pursue to prevent privacy invasion is different from how they would prevent a data leak, at least on a granular level. On a broad level, the same structure applies to both: the institution devotes an amount of resources that it considers optimal to hiring people to gauge and keep abreast of industry norms in the area and best practices, and then it implements them. But since, in information privacy, the goal is to avoid inappropriate collection, processing, or distribution of information by the corporation itself, this is executed by coding information collection, processing, and distribution. By contrast, in data security, the objective is to keep data collection channels and already-collected data as secure from unauthorized access as possible.

While all of these three areas tend to show some signs of collapse into one another, they reflect the ways in which information privacy and data security differ in their implementation.

IV. MAPPING THE RELATIONSHIP BETWEEN INFORMATION PRIVACY AND DATA SECURITY

Information privacy and data security are inexorably related because the same underlying code and infrastructure are implicated in both information privacy and data security.[39] Information privacy and data security are built upon the same premises with respect to technical architecture. That is, both information privacy and data security speak to setting the probabilities of use of a given database containing personal information by particular parties and in particular ways.[40] Since some types of increases in data security can shield personal information from at least some offensive uses, the common

---

are uncertain about where to find such professionals).

38 Bamberger & Mulligan, *supra* note 11, at 261–63.

39 *See* LAWRENCE LESSIG, CODE: VERSION 2.0, 7–8 (2006) (elaborating a theory underscoring the centrality of coded infrastructure in determining the possibilities in law and policy). *See also* Lawrence Lessig, The Architecture of Privacy (Apr. 3, 1998) (unpublished draft), *available at* http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf.

40 Both information privacy and data security are often ex post additions to information processing systems with other goals entirely. *See, e.g.*, In the Matter of Twitter, Inc., FTC File No. 092-3093 (Mar. 2, 2011) (illustrating the difficulties Twitter faced when it integrated security into the software development life cycle relatively late, as an afterthought).

misapprehension is that more data security serves both the company and the information privacy of the individuals whose personal information is in a database,[41] at least up to a certain point.[42] This is untrue. As this section will illustrate, data security can be a shield against information privacy protection.

One example of how the clash between information privacy and data security might play out in practice is a hypothetical based on the facts of the Google Buzz FTC matter.[43] Google Buzz was a social network that Google produced by reorganizing and making public information about Gmail users in order to form social media public profiles.[44] The idea was to create a ready-made social network.[45] However, the FTC alleged that the creation of Google Buzz was unfair or deceptive because Google utilized customers' information provided for Gmail for social networking purposes in violation of the company's privacy policies.[46] This matter was ultimately settled, with Google admitting no culpability, but agreeing to take on an unprecedented, multi-decade comprehensive privacy program subject to periodic external audit.[47]

However, in a more formal legal battle, an institution that traffics in data could have taken another tack. In a forum that accepts that data security's goals serve information privacy, the hypothetical institution might argue that it could not be compelled to disclose or change the algorithms it uses with respect to information privacy or data security. This is because disclosure of that information, or even public disclosure of a broad outline of the processes employed, could put the private information in the database at elevated risk of data breach. So, to make this concrete through reference to the facts of Google Buzz, a hypothetical institution under analogous facts might contend that they could not disclose the process by which they mined the information from the dossiers they had on each user and reframed it as a social media page because such disclosure would put the data security of the database at risk. However, this authentic data security concern would be at odds with the ability of a regulator to seek to enforce the information privacy interests of those individuals whose information is in the

---

41 *E.g.*, Bambauer, *supra* note 4, at 681 ("Thus, security failures generally leave everyone involved (except the attacker) worse off. Privacy failures, by contrast, typically involve a transfer of utility between parties . . . .")

42 As the example of the baby cameras illustrates, in an extreme case, some companies will only see fit to have data security up until a certain point, after which it is no longer worth it for them. *See* Hill, *supra* note 24.

43 Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Googles [sic] Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz.

44 *Id.*

45 *Id.*

46 *Id*.

47 *Id.*

database against the institution that operates the database.

In a future in which transparency may be the most powerful weapon information privacy advocates have against abuses,[48] data security looms as a method for limiting the ability of information to come out to correct undesirable information privacy practices. Far from being a marginal, hypothetical case, situations where data security may conflict with information privacy should be a major area of study for scholars, policymakers, and stakeholders.

CONCLUSION

This Essay provides a roadmap on how to think about information privacy and data security's relationship to one another. It is axiomatic that information privacy alters the assumptions and premises upon which data security operates, and vice versa. While the problems can be separated, an awareness of their impact on one another is mandatory for best practices.

There is a large and growing professional culture cropping up around consumer demands for both information privacy and data security. As the issues become increasingly complicated and specialized, a way to understand how they relate to each other becomes increasingly important. Rather than being surprised about how changes in the code and procedure of data security influence information privacy, and vice versa, corporations and policymakers should be looking ahead to how changes to the one might impact the other.

The demands and objectives of data security and information privacy are not identical, and legal approaches that presume institutions' data security interest necessarily serves the public's interest in information privacy with respect to their personal information are thus doomed to run into serious problems. Therefore, it will not do to assume normative problems in data security are sufficiently addressed by work on information privacy.

---

[48] *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998) (arguing that some degree of privacy can be protected even in a society with pervasive surveillance through pervasive transparency).