Washington and Lee Law Review

Volume 70 | Issue 1 Article 6

Winter 1-1-2013

Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency

Jay P. Kesan

Carol M. Hayes

Masooda N. Bashir

Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency

Jay P. Kesan*
Carol M. Hayes**
Masooda N. Bashir***

Abstract

So many of our daily activities now take place "in the cloud," where we use our devices to tap into massive networks that span the globe. Virtually every time that we plug into a new service, the service requires us to click the seemingly ubiquitous box indicating that we have read and agreed to the provider's terms of service (TOS) and privacy policy. If a user does not click on this box, he is denied access to the service, but agreeing to these terms without reading them can negatively impact the user's legal rights.

As part of this work, we analyzed and categorized the terms of TOS agreements and privacy policies of several major cloud services to aid in our assessment of the state of user privacy in the cloud. Our empirical analysis showed that providers take similar approaches to user privacy and were consistently more detailed when describing the user's obligations to the provider than when describing the provider's obligations to the user. This asymmetry, combined with these terms' nonnegotiable nature, led us to

* Professor and H. Ross & Helen Workman Research Scholar, University of Illinois College of Law.

** Research Associate, University of Illinois College of Law; Fall 2010 Fellow in the Christine Mirzayan Science and Technology Policy Graduate Fellowship program at the National Academy of Sciences.

*** Assistant Director for Social Trust Initiatives, Information Trust Institute, University of Illinois. The authors also wish to acknowledge the excellent research assistance of Robert Zielinski in preparing this work.

conclude that the current approach to user privacy in the cloud is in need of serious revision.

In this Article, we suggest adopting a legal regime that requires companies to provide baseline protections for personal information and also to take steps to enhance the parties' control over their own data. We emphasize the need for a regime that allows for "data control" in the cloud, which we define as consisting of two parts: (1) the ability to withdraw data and require a service provider to stop using or storing the user's information (data withdrawal); and (2) the ability to move data to a new location without being locked into a particular provider (data mobility). Ultimately, our goal with this piece is to apply established law and privacy theories to services in the cloud and set forth a model for the protection of information privacy that recognizes the importance of informed and empowered users.

Table of Contents

"You have zero privacy anyway. Get over it."

—Scott McNealy, Chairman and former CEO of Sun Microsystems, 1999

I. Introduction

What price for your privacy? As social interactions and business activities have shifted online, or into "the cloud," personal information has become a currency with an undervalued exchange rate. What data are consumers willing to trade in exchange for convenience and services online? Would they be as willing to engage in this trade if their privacy rights were more protected and if they had the ability to exercise meaningful control over their data?

Technological and social changes have stimulated many developments over the last decade as the Internet became ingrained in society and social interactions. Substantial technological changes require the law to adapt. When our perceptions change, policymakers amend the law accordingly to address evolved expectations. In this Article, the perceptions and law that we are concerned about are those associated with privacy, especially privacy in the context of services provided over the cloud.

This is not the first time that conceptions of privacy have been shaped by technology. *The Right to Privacy*, published in 1890, was the seminal work of Samuel Warren and Louis Brandeis that substantially influenced privacy law in the United States in the twentieth century.[1] The publication of this piece was spurred by the authors' concerns about intrusions into personal privacy by the press, especially considering the technological improvements that had enabled the production of small, affordable cameras.[2]

Portable cameras were just the beginning of technology that prompted major changes in privacy law and theory. Around the middle of the twentieth century, computers were becoming more pervasive and powerful, enabling the creation of databases that could hold and process huge amounts of information. The idea of informational privacy developed in greater detail around this time, as people realized that personal privacy could be threatened not just by appropriation of one's name and likeness, but by access to and use of other information about a person.[3]

While these informational privacy concerns were becoming more visible, the future of connecting computers in a global telecommunications network was just a glimmer in the eyes of some of the more innovative researchers. Today, in exchange for our personal information, we have access to free e-mail and free data storage, and we can use free services to keep in touch with former classmates and colleagues around the country and around the world. Thanks to Facebook, attendees of modern high school

---

1. *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1891–93 (2010) (describing the impact of the article on the landscape of privacy law).

2. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 137 (2006) [hereinafter SOLOVE, DIGITAL PERSON]. Recent research posits that the authors' concern about privacy stemmed from Warren's experiences with the press when he married Mabel Bayard, the daughter of a politician. *See* Amy Gajda, *What If Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage That Led to "The Right to Privacy,"* 2008 MICH. ST. L. REV. 35, 43–44 (explaining the suggestion of Warren and Brandeis that everyone has the right to keep the press away).

3. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1836–37 (2011) (describing the myth of anonymity on the Internet).

reunions who live on opposite sides of the country can focus on catching up on events of the last week instead of the last ten years.

As with any improvement in technology, however, there are also tradeoffs. Free services online are often funded by advertising revenue, and these ads are made more effective by utilizing the user's personal information to target ads to their interests. To set up accounts for services online, consumers must typically click the ubiquitous box indicating that they have read and agreed to the website's terms of service (TOS) and privacy policy. These agreements often contain broad provisions for what the provider is permitted to do with the consumer's information, while giving the consumer few, if any, options for redress. In the majority of cases in which services are marketed to individual users, there is zero negotiability in these terms, and almost no one reads these terms anyway.

In this Article, we urge the creation of baseline regulations that would guarantee a minimum level of protection of consumer privacy while preserving market vitality. One of the essential elements for this baseline regime would be the protection of the consumer's right to control his data. People are often denied meaningful control over their personal information and the other information that they store with these services. Companies often do not address beforehand how a consumer can exercise control over their information in the event that the service is terminated, and many companies reserve a nonrevocable license to use the consumer's intellectual property that is stored with its service. We view this right of data control as consisting of two parts: (1) data mobility, which we summarize as a right to move one's data and terminate a relationship with a particular service provider, under which providers would be required to provide data to departing customers in a generally accepted file format such that customers do not become "locked in"; and (2) a broader right of data withdrawal that would permit a consumer to withdraw his information from the records of any entity, including a third party, through a notice-and-takedown process.

In Part II, we explain the idea of cloud computing and introduce a number of issues related to it. In Part III, we turn to an examination of privacy fundamentals, first examining different theoretical approaches to privacy before turning to a

discussion of privacy law in the United States and an examination of statutes and case law. In Part IV, we describe issues relating to companies and customer data, including concerns about TOS agreements, privacy policies, and data security. In Part V, we turn to the results of our empirical analysis of the TOS agreements and privacy policies of a sample of cloud service industry leaders. Finally, in Part VI, we offer our recommendations based on our empirical work, as well as our research into privacy issues and the cloud.

II. Cloud Computing Fundamentals

In examining the legal implications of privacy and cloud computing, it is important to understand some of the background. In this Part, we will examine some of the technical background of the current technologies before discussing cloud computing and its advantages and disadvantages in more detail. We will also introduce some legal issues that arise in the cloud context and briefly review various calls for action that have sounded with respect to the cloud, such as calls for amending legislation, proposing legislation, or calling for standards or increased transparency.

A. Background Technology

Before the World Wide Web (Web) became so prevalent, there were two paradigms of computer use. The first was mainframe computing, and under this paradigm, users worked at "dumb terminals" that were connected to a large mainframe system, which in turn processed the users' requests.[4] As microprocessors became available, the personal computing paradigm took over, and the files and data were under the users' physical control.[5]

---

4. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1197 (2010).

5. Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2.0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 362 (2010).

The personal computing paradigm has weaknesses, however, including the low degree of scalability of individual systems, the need for technological expertise to assemble and maintain computer systems, and a low level of redundancy such that data loss through equipment failure is a significant danger.[6] Under the traditional model of information technology (IT) management, based on this paradigm, a lot of space and human capital is required to maintain and secure the systems of a large enterprise.[7]

Moving our technological worlds to the cloud is another paradigm shift that some view as the future of computing.[8] Mark Weiser predicted in 1991 that the third wave of computing, after mainframe computing and personal computing, would be ubiquitous computing, where computers become so small, inexpensive, and ubiquitous that they virtually disappear.[9] Today, technologies continue to improve, but the truly ubiquitous nature of modern computing is not because of the computer's size

---

6. *See* Robison, *supra* note 4, at 1200–01 (explaining the inefficiencies that occur when everyone has his or her own computer).

7. Mark H. Wittow & Daniel J. Buller, *Cloud Computing: Emerging Legal Issues for Access to Data, Anywhere, Anytime*, 14 NO. 1 J. INTERNET L. 1, 5 (2010). Wittow and Buller note that these limitations are mitigated by the use of things like centralized disk storage, the use of more advanced servers with smaller hardware footprints, and system virtualization. *Id.* Virtualization is one of the major technologies behind some applications of "cloud computing," where spaces on hard drives are turned into "virtual machines" that segment the processing of different requests. VMWare, *Virtualization Basics*, http://www.vmware.com/virtualization/virtualization-basics/how-virtualization-works.html (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review).

8. *See* Ilana R. Kattan, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 621 (2011) (noting the transitions between paradigms); Soghoian, *supra* note 5, at 364 (noting that cloud computing has been deemed by many commentators to be the future of computing). Some suggest that the decentralized cloud computing model has the potential to make such services comparable to utilities, with data centers being the equivalent of power plants in the electrical utility context. Kevin Werbach, *The Network Utility*, 60 DUKE L.J. 1761, 1817 (2011). If cloud providers are utilities, the argument for regulation of services on the cloud becomes stronger. *Id.* at 1818.

9. Gary M. Olson & Judith S. Olson, *Human-Computer Interaction: Psychological Aspects of the Human Use of Computing*, 54 ANN. REV. PSYCHOL. 491, 499 (2003).

or power. The Internet and high-speed connections allow people to be in touch not only with each other, but with service providers that can essentially rent out processing power and storage space over the Internet. Moving some functions to the cloud can allow users access to high-end services and technology without having to trade quality for mobility.[10] This future of computing, however, may challenge the default assumption that a user will be able to control her own data.[11]

1. The Internet

The history of the Internet is often traced back to the late '60s and ARPANET.[12] Even before ARPANET, however, some recognized the possible future value of computers being connected using communication lines.[13] Regardless of how the ideas emerged, there is no doubt that the Internet is a pervasive element of today's society.

To say that the Internet has become a staple of modern life is an understatement. The Internet has had a substantial effect on the world and how people interact.[14] Cyberspace is a major social

---

10. Additionally, increasingly large networks of computers can be used to create "ad hoc supercomputers" through distributed computing. Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2064 (2004) [hereinafter Schwartz, *Property*].

11. Werbach, *supra* note 8, at 1820.

12. *See* J.R. OKIN, THE INTERNET REVOLUTION 318 (2004) (describing the Advanced Research Projects Agency Network, created in the late 1960s, that eventually became today's Internet).

13. *See* J.C.R. Licklider, *Man–Computer Symbiosis*, 1 IRE TRANSACTIONS ON HUM. FACTORS IN ELECTRONICS 4 (1960), *available at* http://groups.csail.mit.edu/medg/people/psz/Licklider.html (explaining the benefits of a system with "thinking centers" connected to each other by wide-band communication lines and to individual users); Werbach, *supra* note 8, at 1793 (explaining that major network operators in the 1960s were cognizant that computers would increasingly become the technical foundation for the telecommunications system itself). Werbach notes that some researchers viewed networked computers as having the potential of being a new class of public utility. *Id.* at 1793–94.

14. *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 626 (2011) ("It is not just that 'the Internet is different'; it is that the Internet, like every major advance in infrastructural technology before it, has made

outlet that is often intertwined with the physical realm.[15] People keep in touch through a variety of electronic messaging technologies, including e-mail, text messaging, other instant messaging over the Internet, and social networking websites.[16] Research by the Kaiser Family Foundation suggests that the average youth between the ages of eight and eighteen spends every permissible waking moment using electronic devices, many of which are connected to the Internet, like smart phones and computers.[17] A study by the Nielsen Company found that across all ages, the average American Internet user is online over fifty-five hours per month.[18]

The Internet works because computers on the network use identical protocols that enable interconnection so that data can be delivered across the network.[19] One of the well-known protocols is the Simple Mail Transfer Protocol (SMTP), which enabled e-mail exchanges in the 1980s in the days before the World Wide Web.[20] In the mid-1980s, the transfer of e-mail was fairly fragmented, with communications being transmitted from server to server, stored at various locations temporarily during the trip before being downloaded by the recipient.[21] Today, webmail still uses the SMTP protocol, as well as the Internet Message Access

---

everything different.").

15. *Id.* at 639.

16. *See* John Soma, Melodi Mosley Gates & Michael Smith, *Bit-Wise but Privacy Foolish: Smarter E-Messaging Technologies Call for a Return to Core Privacy Principles*, 20 ALB. L.J. SCI. & TECH. 487, 497–502 (2010) (explaining the five technologies, including telephone systems, e-mail, text messaging, instant messaging, and social networking); Strandburg, *supra* note 14, at 655–56 (explaining how social media promise to change social interactions by supplementing physical interaction or replacing it).

17. Andrea Cascia, *Don't Lose Your Head in the Cloud: Cloud Computing and Directed Marketing Raise Student Privacy Issues in K–12 Schools*, 261 WEST'S EDUC. L. REP. 883, 894 (2011).

18. Paul Lanois, *Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?*, 9 NW. J. TECH. & INTELL. PROP. 29, 29 (2010). About half of that time is spent on social networking, e-mails, games, and instant messaging. *Id.*

19. *See* Werbach, *supra* note 8, at 1769 (explaining the functionality and concept of the Internet).

20. OKIN, *supra* note 12, at 212.

21. *See* Robison, *supra* note 4, at 1205–06 (explaining the functionality of electronic communication services).

Protocol (IMAP). IMAP allows e-mails to be accessed from anywhere with an Internet connection, with e-mails being perpetually stored on the provider's servers.[22] The ability to access information from anywhere is important for mobility and mobile computing.

2. Mobile Computing

Computers have shrunk in size over the last fifty years, from room-size computers to thirty-pound desktops to five-pound laptops to smart phones weighing just a few ounces. The early 1980s saw the invention of the first laptop and the first cellular phone, and the first personal digital assistant (PDA) was released in 1993.[23] This increase in mobility has been helpful for both personal and professional tasks. The Blackberry became a popular office tool after its release in 1999, functioning as both a cell phone and a PDA that permitted remote access to office e-mail.[24] Today's smart phones go beyond the original Blackberry, giving users access to e-mail, the Web, appointment calendars, and even software that allows the users to review word processing files and full color PDFs in the palms of their hands. It is estimated that by 2013, about half of the mobile phone market will be smart phones,[25] and many if not all of these are likely to have access to 3G or 4G data networks that do not require a separate wireless connection.[26]

---

22. *See IMAP & POP*, UNIVERSITY OF MINNESOTA E-MAIL AND INTERNET ACCOUNTS GUIDES, http://www.oit.umn.edu/email/imap-pop (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review).

23. Kimberly L. Rhodes & Brian Kunis, *Walking the Wire in the Wireless World: Legal and Policy Implications of Mobile Computing*, 16 J. TECH. L. & POL'Y 25, 27–28 (2011). The first laptop computer was invented in 1981, and Motorola invented the first cellular phone in 1983. *Id.*

24. *Id.* at 28.

25. Daniel Zamani, Note, *There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones*, 38 HASTINGS CONST. L.Q. 169, 170 (2010).

26. *Strategy Analytics: Global LTE Phone Shipments Will Surge Tenfold to 67 Million Units in 2012*, BUS. WIRE (Mar. 23, 2012), http://www.virtual-strategy.com/2012/03/23/strategy-analytics-global-lte-phone-shipments-will-surge-tenfold-67-million-units-2012 (last visited Feb. 3, 2013) (on file with the

The desire for technologies that can go anywhere makes cloud computing more appealing. Even with improvements in personal computing technology, increased mobility generally requires a tradeoff with the hardware abilities of the device. This is where the value of the cloud becomes clearer: there are fewer tradeoffs from having smaller and cheaper end-user devices because these devices can tap into the power of network-based services.[27]

However, mobile devices are vulnerable to the same sorts of security threats as full-sized computers, including spyware and viruses, and data transmitted using these devices may not be secure.[28] For this reason, and because of the significant security concerns that arise in the cloud computing context, we turn to this topic next.

3. Security

The security of any information in the cloud is often unclear. There was an uproar when Scott McNealy of Sun Microsystems dismissed online privacy concerns by proclaiming in 1999, "You have zero privacy anyway. Get over it."[29] But regardless of whether consumers will be persuaded by assertions about the nature or extent of privacy, active efforts by third parties to infringe on privacy should properly raise red flags.

One threat to devices accessing the cloud is spyware. One can define spyware as software that installs itself, runs, and uses its host computer, all without the owner's permission.[30] Similar software has been called "adware," an example of which was the software produced by Gator, which was ad-supported and sent

---

Washington and Lee Law Review).

27. *See* Werbach, *supra* note 8, at 1816 (explaining how cloud computing is changing the way people think about computers and computer networks).

28. *See* Rhodes & Kunis, *supra* note 23, at 32–33 (noting the existence of malware that targets mobile devices, worms with the ability to monitor and record cell phone conversations, and the exploitation by hackers of information transmitted using wi-fi hotspots).

29. *See* Robison, *supra* note 4, at 1196 (quoting John Schwartz, *As Big PC Brother Watches, Users Encounter Frustration*, N.Y. TIMES, Sept. 5, 2001, at C6).

30. Schwartz, *Property*, *supra* note 10, at 2065.

information about the user and his computer back to the company.[31] In 2004, sources indicated that Gator software was installed on about thirty-five million computers located in the United States.[32]

4. Related Regulations

The degree to which the Internet is or should be regulated is the subject of much debate.[33] Werbach traces the origins of the broadband regulation debate back to the 1960s, when the FCC launched the Computer Inquiries to determine when and how data processing services would become sufficiently intertwined with communications that they would be covered by the Communications Act.[34] In the first of the Computer Inquiries, Computer I, the FCC concluded that there was "no public interest requirement for regulation by government of such activities" because of the competitive nature of the market for data processing services.[35] However, the FCC did recognize that the communications circuits that carried these services might need to be regulated.[36]

---

31. *Id.* at 2066.

32. *Id.* at 2065.

33. *See* Shawn Hess, *Research Shows America Hates Gov't Regulation*, WEBPRONEWS (Mar. 8, 2012), http://www.webpronews.com/research-shows-america-hates-govt-regulation-2012-03 (last visited Feb. 3, 2013) (addressing attitudes toward search engine regulation) (on file with the Washington and Lee Law Review).

34. *See* Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.); Werbach, *supra* note 8, at 1804; *see also* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities (*Computer I Final Decision*), 28 F.C.C. 2d 267 (1971) (final decision and order).

35. *See* Regulatory and Policy Problems Presented by the Interdependence of Computer and Communication Services and Facilities (*Computer I Tentative Decision*), 28 F.C.C. 2d 291, 297 (1970) (tentative decision); *see also* Werbach, *supra* note 8, at 1804 (discussing *Computer I* and the Communications Act).

36. *Computer I Final Decision*, 28 F.C.C.2d at 269 ("[W]ithout appropriate regulatory safeguards, the provision of data processing services by common carriers could adversely affect the statutory obligation of such carriers to provide adequate communication services under reasonable terms and conditions and impair effective competition in the sale of data processing

At the turn of the century, questions about regulating these communications circuits came to the fore. The Telecommunications Act of 1996[37] established a category of services called "information services," which the Act defines as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications."[38] Information services are not regulated as a common carrier under Title II of the Telecommunications Act. In 2002, the FCC designated cable Internet as an "information service" instead of a "telecommunications service," a designation that was upheld by the Supreme Court,[39] and later expanded to include DSL service.[40] The *National Cable & Telecommunications Ass'n v. Brand X* case was regarded by some as marking a decision to not regulate the Internet, given the lesser degree to which information services were regulated compared to telecommunications services.[41]

B. What Is Cloud Computing?

Up to this point, we have referenced "the cloud" in the context of cloud computing as a new computing paradigm. In this subpart, we will go into more detail about cloud computing and what it is.

---

services."); Werbach, *supra* note 8, at 1825.

37. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified in scattered sections of 47 U.S.C.).

38. 47 U.S.C. § 153(20) (2006).

39. Nat'l Cable & Telecomm. Ass'n v. Brand X, 545 U.S. 967 (2005).

40. *In re* Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, 20 F.C.C.R. 14853, 14864 para. 15 (Aug. 5, 2005) (report, order, and notice of proposed rulemaking).

41. *Brand X*, 545 U.S. at 967; Note, *How Chevron Step One Limits Permissible Agency Interpretations: Brand X and the FCC's Broadband Reclassification*, 124 HARV. L. REV. 1016, 1021 (2011) ("The Supreme Court affirmed the FCC's authority to deregulate cable broadband service in *Brand X* . . . .").

1. Defining Cloud Computing

The term "cloud computing" has become popular and trendy, but there are many concepts behind this idea. On a general level, "cloud" is used as a metaphor for the "ethereal Internet" and the virtual platform that it provides.[42] Some view cloud computing abstractly as the result of the convergence of computing and communications,[43] or more practically as a "scalable network of servers,"[44] as "IT as a service,"[45] or as the convenience of being able to access a shared pool of computing resources over a network like the World Wide Web.[46]

---

42. *See* David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2205, 2216 (2009); Wittow & Buller, *supra* note 7, at 1 (noting that "cloud" is essentially a metaphor for the Internet).

43. Werbach, *supra* note 8, at 1811.

44. *See* Konstantinos K. Stylianou, *An Evolutionary Study of Cloud Computing Services Privacy Terms*, 27 J. MARSHALL J. COMPUTER & INFO. L. 593, 594–95 (2010) (stating that most business executives, lawyers, and computer technicians understand cloud computing as a scalable network of servers on which users store data that would traditionally reside on a local computer). Werbach also embraces this interpretation. Werbach, *supra* note 8, at 1811 ("Cloud computing is an approach that places application processing and storage in network-based data centers, rather than in end-user devices such as personal computers."); *see also* Timothy D. Martin, *Hey! You! Get Off of My Cloud: Defining and Protecting the Metes and Bounds of Privacy, Security, and Property in Cloud Computing*, 92 J. PAT. & TRADEMARK OFF. SOC'Y 283, 292–94 (2010) (explaining cloud computing as "Infrastructure-as-a-Service").

45. *See* Rhodes & Kunis, *supra* note 23, at 30 (stating that at its core, cloud computing is an IT service because providers "rent" their services to customers). Wittow and Buller similarly note that definitions of cloud computing typically involve a third party provider who supplies a subscription-based service for computing and storage needs. Wittow & Buller, *supra* note 7, at 5.

46. *See* Couillard, *supra* note 42, at 2216 ("Cloud platforms give users 'anywhere access' to applications and data stored on the Internet."); William R. Denny, *Survey of Recent Developments in the Law of Cloud Computing and Software as a Service Agreement*, 66 BUS. LAW. 237, 237 (2010) (describing cloud computing as technology that gives users convenient network access to a shared pool of computing resources); Lanois, *supra* note 18, at 29 (referring to cloud computing as being based on the idea of storing software and data on Internet servers instead of locally); Martin, *supra* note 44, at 287 (quoting a definition for cloud computing as "a platform for the delivery of software services and other applications through remote file servers" in which the data and software stay on remote servers and are accessible from any computer anywhere); Fernando M. Pinguelo & Bradford W. Muller, *Avoid the Rainy Day: Survey of U.S. Cloud*

Denny maintains that there is not a uniform definition of cloud computing.[47] On the other hand, many commentators also authoritatively cite the definition of cloud computing put forth by the National Institute for Standards and Technology (NIST), which currently defines it as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[48] For our purposes, we accept the NIST's definition because it is broad enough to encompass the variety of uses for cloud computing.

2. Growth of Cloud Computing

Cloud computing is a growing segment of technology services, thanks in part to the availability of high speed Internet service.[49] A study by the Pew Internet and American Life Project concluded that about 69% of Internet users in the United States already use webmail, other software programs located solely

---

Computing Caselaw, 2011 B.C. INTELL. PROP. & TECH. F. 1, 1 (defining cloud computing as "a computer networking model that gives users on-demand access to shared software applications and data storage."); Robison, *supra* note 4, at 1200 (drawing a parallel between "dumb" terminals in the mainframe paradigm and how personal computers are used in the cloud paradigm); Soghoian, *supra* note 5, at 364 (applying the term "cloud computing" to "software offerings where the application is executed in a web browser, via software code that is downloaded (as needed) from a remote server that also stores users' files."); Wittow & Buller, *supra* note 7, at 1 (defining cloud computing as when "an Internet connection delivers hardware power and software functionality to users regardless of where they are or which computer they are using").

47. Denny, *supra* note 46, at 237.

48. *See* Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing*, Nat'l Inst. of Standards & Tech. (Sept. 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; *see also* David S. Barnhill, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 638–39 (2010) (discussing the NIST definition of cloud computing); George Jiang, *Rain or Shine: Fair and Other Non-Infringing Uses in the Context of Cloud Computing*, 36 J. LEGIS. 395, 412 (2010) (discussing the NIST definition of cloud computing); Kattan, *supra* note 8, at 620–21 (discussing the NIST definition of cloud computing).

49. Robison, *supra* note 4, at 1201.

online, or online data storage.[50] A survey of technology insiders and critics in 2010 reflected a view by the majority that cloud computing technologies will be heavily used in work environments by 2020, with most expecting the PC model to decrease in importance.[51] Some suggest that as cloud computing grows and more activities transition onto the Internet, there will be a greater focus on interoperability between cloud platforms and applications.[52]

As a result of more people using cloud services, the revenue in this industry is expected to grow substantially. The cloud services industry saw revenue of $58.6 billion in 2009, and some analysts are anticipating that the industry's revenue will increase between $40 billion and $160 billion over the next few years.[53] Because of these large growth forecasts, many companies are pushing to be at the forefront of this movement.[54]

---

50. *See* John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RES. CTR. (Sept. 12, 2008), http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review). A majority of those responding in the Pew study also indicated that they were very concerned about the use of their personal data by cloud providers. *See id.*; *see also* Martin, *supra* note 44, at 298 (discussing the Pew Research Center study); Wittow & Buller, *supra* note 7, at 5 (same).

51. Kattan, *supra* note 8, at 620. Some have noted that cloud computing has the potential to partially replace the desktop computer. *See* Stylianou, *supra* note 44, at 604; *see also* Werbach, *supra* note 8, at 1813–14 (discussing how the rise of smart, connected mobile devices will increase incorporation of cloud computing).

52. *See* Stylianou, *supra* note 44, at 597 (stating that some platforms and applications will allow interoperability, which will allow users to transfer content easily).

53. *See* Lanois, *supra* note 18, at 30 (citing a study anticipating growth to $148.8 billion in revenue by 2014, and a study anticipating over a 20% increase in spending on cloud services by organizational customers); Soghoian, *supra* note 5, at 361 (citing analyst expectations of industry revenue growth between $40 billion and $160 billion).

54. *See* Lanois, *supra* note 18, at 30 (referring to a "recent bidding war between Hewlett-Packard and Dell to acquire cloud storage firm 3PAR").

3. Uses of Cloud Computing

There are a lot of uses of cloud computing and a lot of aspects to those uses. One of the earliest forms of cloud computing was server-side e-mail storage.[55] There are many companies offering cloud services.[56] Webmail in particular is very popular, and sometimes an organization may contract with cloud providers for e-mail in order to save money over running its e-mail system in-house.[57] Google provides such services to organizations through its Google Apps service,[58] as well as free services to individuals over the Web. Google's services to the public include webmail through Gmail and Web-based productivity software through Google Docs.[59]

There are also a number of other uses that are not as immediately visible. Users can take advantage of the cloud to improve the functionality of locally run software, like the Weave add-on for the Firefox Web browser, which allows users to synchronize bookmarks, saved passwords, and cookies across multiple computers by storing this information on Mozilla's servers.[60] Additionally, Ford is working on a system that would bring features of cloud computing and social networking to new cars, perhaps including things like traffic alerts and real-time fuel consumption monitoring.[61] Cloud computing could also be useful in education to increase student engagement and provide

---

55. *See* Couillard, *supra* note 42, at 2218 (explaining that server-side e-mail was one of the first iterations of cloud computing); Robison, *supra* note 4, at 1203 (referring to server-side e-mail storage as one of the first cloud computing services available to the public).

56. *See* Lanois, *supra* note 18, at 30 (listing offerings of companies, including Amazon, Microsoft, IBM, and VMWare).

57. Soma, Gates, & Smith, *supra* note 16, at 516.

58. *See* Soghoian, *supra* note 5, at 367–68 (describing services offered by Google Apps).

59. John T. Kivus, *Spring Training for Electronic Search: Examining* U.S. v. Comprehensive Drug Testing, Inc. *with Regards to Evolving Trends in Computing*, 11 N.C.J.L. & TECH. ON. 115, 128–29 (2009).

60. *See* Soghoian, *supra* note 5, at 397 (explaining the characteristics of Firefox, Mozilla's browser).

61. Lanois, *supra* note 18, at 32.

students with additional tools like online forums and storage space in the cloud.[62]

The cloud is also leading to many innovations in entertainment. Some gaming services are appearing in the cloud, like OnLive and Gaikai, and some posit that the cloud has the potential to let gamers play games with high-end graphics without having high-end computers.[63] Other entertainment uses of the cloud include subscription or ad-supported video streaming services like Netflix and Hulu.[64] There are also social networking websites, like Facebook, that behave in ways consistent with the NIST's definition of cloud computing.[65]

The providers of cloud services may take a variety of approaches to service provision, differing in areas like cost models, user interfaces, and treatment of user data. Because cloud services are still fairly new, some companies may also seek to ease the transition to the cloud by making their services resemble software that is run locally on a computer.[66] In addition to easing the transition by focusing on the user experience, cloud service providers also may make their services more appealing by offering them for free. There are many cloud services that are already provided for free, and these services can remain profitable by relying on ad support.[67] Companies that do so often

---

62. *See* Cascia, *supra* note 17, at 884 (discussing the benefits of integrating cloud computing in schools). The Department of Education takes the position that cloud computing, data mining, and data aggregation could play valuable roles in increasing student performance and keeping school districts accountable. *Id.* at 887.

63. Lanois, *supra* note 18, at 31. OnLive launched in June 2010, but is said to already be worth $1.1 billion. *Id.*

64. Netflix, *How Netflix Works*, https://signup.netflix.com/MediaCenter/HowNetflixWorks (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review); Hulu, *More About Hulu*, http://www.hulu.com/about (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review).

65. *See supra* note 48 and accompanying text (discussing the NIST definition of cloud computing).

66. *See* Soghoian, *supra* note 5, at 369–70 (explaining single-site browser technology). A cloud service provider, looking to ease the transition between local computing and cloud computing, might also choose to provide support for offline access, such as Google's Gears browser add-on that allows limited access to Gmail. *Id.* at 370–71.

67. *See* Jiang, *supra* note 48, at 415 (explaining different business models for cloud computing).

use customer information to generate targeted advertisements, which some criticize as effectively monetizing users' private data.[68]

Providers may also take very different approaches to data protection and encryption depending on the service, and we argue that the public should be made aware of data protection issues. Remotely stored data that is not intended for public access is likely to be encrypted, password protected, or have unlisted links.[69] Other data, especially data that is not considered "sensitive," are typically stored in an unencrypted format.[70] Because cloud computing technology is still emerging, added features like increased security would cost more for early adopters, and this cost plus the current lack of market demand means that cloud service providers currently do not have much incentive to invest in enhancing security for a lot of the data involved.[71] One of the things that current customers demand, however, is reliability, so cloud service providers often go to great lengths to have their services available at least 99.9% of the time.[72]

4. Types of Cloud Computing Services

Cloud services may be private, public, or some hybrid of the two.[73] Private clouds may also be referred to as "internal" clouds, and are located solely within that organization and use only that

68. Soghoian, *supra* note 5, at 396.

69. Couillard, *supra* note 42, at 2217. Mozy asserts that it uses encryption technologies when user data is transmitted and stored, which is different from most other companies that say that they use SSL encryption for the exchange of data but do not specify whether data in storage is encrypted. Stylianou, *supra* note 44, at 603.

70. Stylianou, *supra* note 44, at 605. Because Google does not encrypt stored e-mails, for example, Google's software can scan e-mail content for key words for the purpose of targeted advertising. *Id.*

71. *Id.* at 606.

72. *Id.* at 607.

73. Barnhill, *supra* note 48, at 640.

organization's infrastructure.[74] Public clouds are offered over the Internet and are supported by ads or fees.[75]

There are three primary models for public cloud services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).[76] Companies that provide servers and storage for remote use are providing IaaS, while companies that provide platforms on remote servers to run applications are providing PaaS.[77] A company that makes software applications available over the Internet, including webmail, is providing SaaS.[78] Gmail and Facebook are examples of SaaS cloud services.[79] SaaS goes much further, however, and includes services like online gaming and online legal research.[80]

SaaS is arguably the level that consumers are most familiar with. The other types of cloud computing services may be more appealing to developers and computing professionals. PaaS, for example, gives customers (often software developers) the ability to deliver their own software applications over the Web to end users at a lower cost to the developer since they are using someone else's servers to do so.[81] IaaS, on the other hand, involves cloud providers giving customers access to raw computing resources in a manner similar to a utility service.[82] Because this Article focuses on individual consumers, the most relevant category of cloud service for our purposes is SaaS.

---

74. Couillard, *supra* note 42, at 2216; Martin, *supra* note 44, at 287.

75. *See* Martin, *supra* note 44, at 287 (explaining how cloud computing works).

76. Barnhill, *supra* note 48, at 639–40.

77. *Id.*

78. *Id.* at 639; Denny, *supra* note 46, at 237.

79. Rhodes & Kunis, *supra* note 23, at 31.

80. Martin, *supra* note 44, at 287–88 ("Under the SaaS model, a user interacts with an online service through the Internet, and the online service's vendor provides the necessary software applications and remote data storage.").

81. *See id.* at 289 (explaining the lower costs of PaaS compared to SaaS); Robison, *supra* note 4, at 1203 (noting the use of PaaS by third-party developers).

82. Robison, *supra* note 4, at 1204.

C. Advantages and Disadvantages of Cloud Computing

Moving more services onto the cloud has many promises and pitfalls. It is possible that the future success of cloud services will depend on how these advantages and disadvantages balance with each other and, more importantly, with the public's expectations.[83]

Advantages of the cloud paradigm include data preservation,[84] high levels of expertise on the part of cloud service providers,[85] scalability,[86] affordability,[87] and availability.[88] Additionally, some studies have shown that businesses that adopt SaaS enjoy a return-on-investment of almost 600%.[89] Cloud providers are benefited because they have control over content, can set access terms, and can also monitor usage statistics.[90]

---

83. Stylianou, *supra* note 44, at 606 ("In effect, the combination of the sensitive nature of information that cloud services usually attract, the lack of adequate security from cloud services, and the intensification of governmental intrusiveness, stands as an impediment to the spread of cloud services."). Stylianou also suggests that if cloud services implemented stronger security measures, like encrypting stored data, such changes could make cloud services more attractive to business customers. *Id.* at 609.

84. *See* Martin, *supra* note 44, at 294 (describing the benefit of being able to access applications and data from anywhere at any time).

85. *Id.*; Stylianou, *supra* note 44, at 603.

86. *See* Cascia, *supra* note 17, at 888 (citing the Department of Education's position that the scalability of cloud-based IT services would help schools cut costs); Jiang, *supra* note 48, at 413; Martin, *supra* note 44, at 294 (stating that cloud computing offers rapid and intelligent resource adjustment as well as economies of scale); Wittow & Buller, *supra* note 7, at 5 (noting that cloud computing allows a system's capacity and capability to be increased without additional infrastructure or personnel investments). Wittow and Buller cite the example of Animoto, which went from 25,000 users to 250,000 users over the course of just three days and was able to keep pace with this very high rate of growth by acquiring more virtual servers. *Id.* at 5–6. The scalability advantage works both ways, allowing small companies to easily expand their technological resources, and allowing downsizing companies to easily cut unnecessary IT costs. Rhodes & Kunis, *supra* note 23, at 31.

87. Barnhill, *supra* note 48, at 640–41; Martin, *supra* note 44, at 289; Soghoian, *supra* note 5, at 366.

88. Jiang, *supra* note 48, at 413; Soghoian, *supra* note 5, at 366.

89. Martin, *supra* note 44, at 289

90. *See* Jiang, *supra* note 48, at 413; *see also* Soghoian, *supra* note 5, at 364–65 (listing the ability to terminate user access and make sure that users are always running the current software version as two advantages of the cloud

These additional advantages for cloud providers also make cloud services attractive to copyright holders because the control exercised by the cloud provider can provide additional security and protect the copyright holder from infringement.[91]

There are also many disadvantages to the cloud paradigm, and many of these disadvantages arise in part because of consumers' loss of control over data. Because consumers are entrusting their data to a third party, they are relying on that third party to adequately secure the information,[92] have the services and data available at all times,[93] and allow the consumer to move their information between providers freely,[94] all in a context in which it is unclear how modern privacy law (including the Fourth Amendment and laws related to confidentiality) may

---

to the service provider).

91. *See* Jiang, *supra* note 48, at 422; Soghoian, *supra* note 5, at 364–65 (noting the value of the cloud for helping content owners better protect copyrights and trade secrets).

92. *See* Soghoian, *supra* note 5, at 374 ("[N]early all [] leading cloud providers offer products that are by default vulnerable to snooping, account hijacking, and data theft by third parties."). Soghoian suggests that the reason that hackers are a threat to users of cloud services is because cloud providers have not yet adopted strong encryption technologies. *Id.* at 361. Businesses are likely to be very concerned about the potential security issues of the cloud, so they will have to balance the financial benefits of moving to the cloud against the costs of data security like encryption and key management. Couillard, *supra* note 42, at 2217.

93. *See* Kattan, *supra* note 8, at 623 (explaining how cloud computing creates dependency); Martin, *supra* note 44, at 294 (describing the benefit of being able to access applications and data from anywhere at any time). While cloud services strive for reliability, the technology is still developing and thus is still very susceptible to human error and programming bugs, like the leap day bug that caused Microsoft's Azure service to be unavailable all day on February 29, 2012. Bill Laing, *Summary of Windows Azure Service Disruption on Feb 29, 2012*, WINDOWS AZURE TEAM BLOG (Mar. 9, 2012, 6:03 PM PST), http://blogs.msdn.com/b/windowsazure/archive/2012/03/09/summary-of-windows-azure-service-disruption-on-feb-29th-2012.aspx (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review).

94. Martin, *supra* note 44, at 297–98; *see also* Kattan, *supra* note 8, at 623 (noting that a customer who moves data storage and processing onto the cloud may have difficulty if he later decides to revert to the PC model). Martin notes that this lock-in problem is likely to not apply to IaaS because a customer of an IaaS provider will typically have everything on a virtual machine over which the customer can exercise full control. Martin, *supra* note 44, at 294.

apply.[95] Another disadvantage is related to the risk of loss. If a provider fails to secure data and a consumer's information is compromised, the risk of loss is likely to fall on the consumer rather than the cloud service provider.[96]

In this Article, we emphasize the need for data control in the cloud, which we define as consisting of the ability to withdraw data (data withdrawal) and move data to a new location (data mobility). We argue that data control is essential for meaningful consumer choice. Consumers will inherently have less control over data stored in the cloud,[97] but being able to choose (and switch to) providers that are more reliable or that offer stronger security measures is important for preserving consumer

---

95. *See* Lanois, *supra* note 18, at 44 (citing a publication of the World Privacy Forum). Privacy is likely to be especially important to consumers in the context of electronic health records. *See* Colin P. McCarthy, Note, *Paging Dr. Google: Personal Health Records and Patient Privacy*, 51 WM. & MARY L. REV. 2243, 2253 (2010) (discussing the potential problems of personal health records). These concerns are not just limited to health services. Confidentiality is a significant concern to a number of other professions when considering the adoption of cloud services as well. *See* Cascia, *supra* note 17, at 884 (noting that outsourcing IT management to third parties may make it more difficult for schools to make sure that the personal information of students remains private); Martin, *supra* note 44, at 295. Martin mentions the legal field by name as one industry that should be hesitant at this point when considering whether to use cloud services in support of its practices. *Id.* at 300. It is also unclear how the Fourth Amendment will apply to information held by third party cloud service providers. *See id.* at 295–96; *see also* Soghoian, *supra* note 5, at 361 (noting that cloud computing leaves users vulnerable to invasions of privacy by the government, resulting in "evisceration of traditional Fourth Amendment protections of a person's private files and documents"). Martin also notes concerns that the federal statute governing electronic messaging may be difficult or unable to apply to modern technology. Martin, *supra* note 44, at 295–96.

96. *See* Soghoian, *supra* note 5, at 378–79 (discussing why cloud computing providers have little incentive to protect users); *see also infra* Part IV.A (discussing contents of TOS agreements, including explicit limitations on providers' legal liability).

97. *See* Kattan, *supra* note 8, at 623 (noting the customer's dependence on cloud service providers to protect the customer's data); Martin, *supra* note 44, at 289 (noting customers' lack of control over data and the security practices of the cloud vendor); Stylianou, *supra* note 44, at 595 (explaining that some private data will be transferred away from the user's immediate physical control); Wittow & Buller, *supra* note 7, at 6 (noting the lack of control that users have over data in the cloud and the importance that the user be able to trust the cloud service provider).

autonomy. Currently, there are systemic limitations to meaningful choice. SaaS customers may experience lock-in problems because a cloud provider may store the customer's information in a format unique to the cloud provider and thus make it difficult for the customer to switch cloud providers later.[98] This control over content also leads to some concerns about private censorship. Werbach notes the existence of concerns over cloud services having too much power to censor controversial causes, such as when Amazon Web Services dropped Wikileaks as a customer.[99]

D. Cloud Computing Legal Issues

For our purposes, there are two important categories of legal issues raised in the context of cloud computing: data use and procedural issues. Data use issues could include the use of both public and private information, thus our use of the term "data use" also includes privacy concerns, examined in more detail below. Procedural issues relating to cloud computing can include E-Discovery and jurisdiction questions. The appropriate degree of regulation is also in controversy, so even if we could identify all of the possible legal issues related to cloud computing, it may prove difficult to effectively regulate the industry.[100]

One data use issue is the problem of "scraping," specifically the question of how courts should deal with the unauthorized, automated collection of information by, for example, auction services that list relevant auctions in one search across multiple

98. Martin, *supra* note 44, at 297–98; *see also* Kattan, *supra* note 8, at 623 (noting that a customer who moves data storage and processing onto the cloud may have difficulty if they later decide to revert to the PC model). Martin notes that this lock-in problem is likely to not apply to IaaS because a customer of an IaaS provider will typically have everything on a virtual machine over which the customer can exercise full control. Martin, *supra* note 44, at 294.

99. *See* Werbach, *supra* note 8, at 1820 ("From a broader perspective, though, the rise of cloud computing changes a default assumption that data will be within the control of the user.").

100. *See id.* at 1766 (referring to network neutrality as the "final hurrah" of the regulatory framework under the Telecommunications Act, as views of the industry have shifted "from regulated monopoly to managed competition within defined industry segments").

auction websites.[101] Claims relating to scraping have been brought based on the Computer Fraud and Abuse Act (CFAA),[102] the tort of trespass, and a "hot news" theory.[103] An analysis of these options and whether they provide adequate means of redress for companies whose data is mined poses an interesting research question for future research. Our concern about the privacy of individual users also makes us question whether recourse for "scraping" might also apply to protect individuals whose data is mined without their consent, though this is outside the scope of our research.

1. Privacy

Our primary focus in this Article is on the implications of cloud computing and corresponding privacy agreements on personal privacy. There are several legal issues relating to privacy and cloud computing, including the uncertain applications of the Health Information Portability and Accessibility Act (HIPAA),[104] the Stored Communications Act,[105] and the Fourth Amendment, especially the third-party doctrine of Fourth Amendment jurisprudence.[106] If a legal regime is put into place to provide stronger privacy protections, it is unclear

101. *See* Wittow & Buller, *supra* note 7, at 8–9 (discussing how the scraping issue impacts cloud computing).

102. 18 U.S.C. § 1030 (2006).

103. *See id.* (discussing how the scraping issue impacts cloud computing).

104. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified at 29 U.S.C. § 1181 *et seq.*; 42 U.S.C. §§ 300gg, 1320d *et seq*. (2006)); Denny, *supra* note 46, at 239–40 ("Yet another statutory hurdle to cloud computing in the United States is the Health Insurance Portability and Accountability Act ('HIPAA').").

105. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.); Werbach, *supra* note 8, at 1819 (noting that a search warrant is required to access e-mail stored on a user's hard drive, but that under the Electronic Communications Privacy Act, a lower standard would be applied if that same e-mail had been stored on Google's Gmail servers for more than six months).

106. *See* Stylianou, *supra* note 44, at 596–97 ("[I]t is still debatable whether access to online stored data should be considered a search . . . or whether by communicating data to a remote server the subject is considered to have knowingly exposed the information.").

whether data collection should be addressed based on the quantity collected or the type collected, and there is also a lot of uncertainty about how to address the transfer of data between countries with different privacy laws.[107]

Many aspects of the privacy debate rely on an understanding of privacy theories. Several things influence privacy protections online, including social norms, website architecture, and the law.[108] Some note that there are societal obstacles to strengthening privacy protections online, arguing that the younger generation values the interconnectedness and low cost of cloud services more than they value their personal privacy.[109] Werbach asserts that the range of concerns about cloud providers' information practices goes beyond our current concept of "privacy," and suggests referring to it as "information governance."[110] In lieu of creating a new category, Solove suggests revising the concept of "privacy" to encompass these concerns.[111] It is likely that there will be an increase in public policy activity in this area in the near future,[112] underscoring the importance and timeliness of this topic. A significant problem that arises when dealing with technologically sophisticated policy issues, however, is that some judges and other policy makers may be ill-

---

107. *See id.* at 595–96 (discussing whether access to cloud data is a search).

108. *See* Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. TECH. L. REV. 337, 339–41 (2011) ("Certain non-legal mechanisms can affect online privacy and shape the power of individuals to control their personal data.").

109. *See* Robison, *supra* note 4, at 1237–38 ("[Y]ounger users are more likely to embrace the Internet's interconnectedness and convenience by participating in social networking, sharing digital content, and using cloud services."). *But see* Chris Hoofnagle, Jennifer King, Su Li, & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* 20 (Working Paper Series, 2010), *available at* http://ssrn.com/abstract=1589864 (noting that their study results failed to show the expected significant differences between the behavior of young adults and older adults online with regard to privacy).

110. Werbach, *supra* note 8, at 1833.

111. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) [hereinafter Solove, *Taxonomy*] (setting forth a new taxonomy for the understanding of information privacy).

112. *See* Werbach, *supra* note 8, at 1835 ("Public policy activity in this area seems bound to increase.").

informed about the underlying technology, leading these policy makers to hesitate when faced with current issues.[113]

There may also be legal harms arising from data gathering practices. Richards discusses the "database problem," in which there are very large databases that make it efficient and valuable for businesses to use consumer information, but the legal rights of the consumers in these databases are unresolved.[114] Stylianou acknowledges that cloud computing does result in more private information being collected and this could be harmful, but concludes that most of this increase in information collection happens voluntarily, and that the compromises in privacy appear to be no greater than necessary for the delivery of cloud services.[115] Some were critical of the settlement in *Authors Guild v. Google*[116] for its lack of restrictions concerning data gathering, arguing that privacy issues should be addressed in the settlement to protect people from having their reading choices readily available to third parties.[117]

2. Jurisdiction

Jurisdiction issues concerning a court's ability to hear a claim will arise in the context of the cloud for two reasons: (1) the

---

113. For example, in the oral arguments of *City of Ontario v. Quon*, Justices Roberts and Scalia noted their confusion as to how wireless communications are transmitted, with both indicating that they were not aware that these messages were inherently processed by a third party. *See* Transcript of Oral Arguments at 48–50, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332), http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf (exemplifying the confusion of Justices Roberts and Scalia as to how wireless communications are transmitted).

114. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1150, 1156–65 (2005).

115. *See* Stylianou, *supra* note 44, at 594–96 (discussing voluntary information collection).

116. Authors Guild v. Google, Inc., 770 F. Supp. 2d 666 (S.D.N.Y. 2011).

117. *See* Denny, *supra* note 46, at 238–39 ("Much of the recent debate surrounding cloud computing and privacy stems from a settlement in *Authors Guild v. Google Inc.*"); Wittow & Buller, *supra* note 7, at 7 ("Privacy concerns also have been raised in the context of the pending *Authors Guild v. Google* [*Inc.*] book search settlement, which creates a cloud-based database of searchable books.").

lack of borders in cyberspace; and (2) the vast differences between privacy laws in different locations.[118] If a conflict arises with respect to a cloud service, where could that conflict be resolved? If there is a conflict between a customer and cloud provider within the United States, the customer might be bound by arbitration language in a TOS agreement, or by a choice of law or venue clause.[119]

But what about more geographically vague situations? Some discussions about jurisdiction assume that the applicable law will be determined by the physical location of the data, but this information is often unknown to the customer.[120] Sometimes, a defendant may claim that he has insufficient contacts with the forum state for a particular court to exercise jurisdiction.[121] Because of these jurisdictional problems, it is important that the TOS agreements for cloud services specify where data will be stored and which laws will apply.[122] Otherwise, the uncertainties related to jurisdiction in the cloud may chill some online activity by discouraging people from engaging in electronic commerce.[123]

Approaches to informational privacy can vary between nations, and the United States as a whole has a privacy law

---

118. *See* Stylianou, *supra* note 44, at 596 (discussing the transfer of data between countries).

119. *See* Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1)*, 18 INT'L J. L. & INFO. TECH. 176, 178 (2010) [hereinafter Kuner, *Part 1*] (noting the overlap between choice of law and jurisdiction).

120. *See* Lanois, *supra* note 18, at 44 ("[D]ata that might be secure in one country may not be in another, and in many cases, users of cloud services do not know where their information is being held."); Stylianou, *supra* note 44, at 602 ("Because different national laws accord different levels of protection to personal and private information, it is important that users know where their data is stored.").

121. *See* Pinguelo & Muller, *supra* note 46, at 1 ("It is apparent that the use of a cloud can potentially increase the number of 'contacts' a party is found to have for personal jurisdiction purposes, and thus raise its exposure to lawsuits in multiple forums.").

122. *See* Denny, *supra* note 46, at 239 ("According to the Privacy Authors, if readers were worried that information about their reading habits could be disseminated to the government, divorcing spouses, or other interested third parties, these readers would be less likely to view books on controversial topics.").

123. Kuner, *Part 1*, *supra* note 119, at 178.

regime that is much less protective of personal privacy than that of the European Union.[124] Can a court in the European Union exercise jurisdiction over a U.S. company that violates the personal privacy of EU citizens? Generally, the answer will be yes, based on principles of jurisdiction.

In the international context, jurisdiction can be described as the right of one country to regulate actions that are not solely conducted within that nation's borders.[125] Three categories of international jurisdiction are legislative jurisdiction, under which a nation's laws can apply to cases with a foreign element; adjudicative jurisdiction, when the nation's courts have the power to try cases involving a foreign element; and enforcement jurisdiction, when the nation has the power to act in another nation's territory to enforce its own laws.[126]

Exercise of adjudicative jurisdiction may be justified when the acts were committed or completed within the nation's territory, when the perpetrator or victim was a citizen of that nation, when the act has effects within that nation (a justification that is commonly criticized for its open-endedness), or when the act jeopardizes the nation's sovereignty.[127] Because adjudicative jurisdiction can be found when the victim of a wrong is a citizen of the adjudicating nation, this means that service providers in

---

124. *See* Stylianou, *supra* note 44, at 597 (noting that the use of the Safe Harbor agreement allows U.S companies to process the data of European citizens). This agreement is in lieu of a privacy law overhaul to make the U.S. approach to privacy match the approach of the EU. *Id.*

125. *See* Kuner, *Part 1*, *supra* note 119, at 178–79 (defining international jurisdiction as "the State's right under international law to regulate conduct in matters not exclusively of domestic concern." (citation omitted)).

126. *See id.* at 184 (discussing categories of jurisdiction). Generally, direct enforcement of one nation's laws in another nation is not permitted, though a nation may apply its domestic law to conduct that occurs elsewhere, provided recognized legal grounds exist for doing so. *Id.* at 185. Enforcement jurisdiction, however, is rarely found. *See* Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 2)*, 18 INT'L J. L. & INFO. TECH. 227, 232 (2010) [hereinafter Kuner, *Part 2*] ("[A] State may not carry out an investigation in another State, if the purpose is to enforce its own administrative, criminal, or fiscal law. These restrictions apply even if the persons or entities in the second State consent to the first State's enforcement actions.").

127. *See* Kuner, *Part 1*, *supra* note 119, at 188–90 (examining adjudicative jurisdiction in detail).

the United States must act carefully to comply with the privacy laws of other jurisdictions when a customer is a foreign citizen.

E. Calls for Action in the Cloud

The current legal regime applicable to cloud computing has drawn a lot of criticism from organizations that want the law to consider current technologies.[128] Legislative reform will likely be necessary to address the new environment created by cloud computing, but such reform will need to take into account many different concerns.[129] For example, reforms will need to take data protection into consideration because customers are likely to want data stored in the cloud to be protected the same as it would be on the customer's own tangible storage devices.[130]

The Electronic Communications Privacy Act (ECPA)[131] is examined in detail below in Part III.B.2. Several institutions have urged lawmakers to amend the ECPA. Microsoft proposed the Cloud Computing Advancement Act (CCAA)[132] in 2010, and the Center for Democracy and Technology has also recommended

---

128. *See* Kattan, *supra* note 8, at 645 (suggesting revision of the Stored Communications Act and referencing the position of the nonprofit Digital Due Process that the ECPA should be modernized and clarified); Martin, *supra* note 44, at 286 (noting recommendations made by Microsoft and the Center for Democracy and Technology). Digital Due Process is an organization that is focused on modernizing the approaches of law enforcement to electronic data, and they encourage the reformation of the ECPA to take into account recent and emerging technologies. Lanois, *supra* note 18, at 45.

129. *See* Werbach, *supra* note 8, at 1826 ("The solution to the contemporary challenges of cloud computing likely requires some legislative reform in addition to FCC action.").

130. *See* Couillard, *supra* note 42, at 2205–06 ("Despite the shift in Internet usage, users expect their information to be treated the same on this virtual cloud as it would be if it were stored on their own computer, phone, or iPod.").

131. *See* Electronic Commc'n Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510–2522, 2701–2712 (2006)).

132. *See* Brad Smith, Gen. Counsel, Microsoft Corp., Speech at the Brookings Institute Policy Forum: Cloud Computing for Business and Society (Jan. 20, 2010) *available at* http://download.microsoft.com/download/C/0/0/C00D24A5-A686-4109-9DB8-14A29E058069/Building_Confidence_in_the_Cloud_General_Counsel_Brad_Smith_Brookings_Speech.docx.

legislative action to address cloud computing issues.[133] The CCAA would strengthen the privacy protections of the ECPA, unifying the concepts of "electronic communications service" and "remote computing service," and would also enhance the Computer Fraud and Abuse Act (CFAA)[134] by presuming a loss of $500 for each count of unauthorized access.[135] The CDT proposal, on the other hand, focuses more on civil liberties, urging Congress to amend the ECPA to require probable cause before a seizure of online information can be executed without notice.[136]

1. Transparency and Control

Other calls for revisions of the system have focused on the need for transparency.[137] To say that practices of cloud providers should be transparent about information use means that customers should be well-informed of what companies are doing with the customers' personal data. In examining Internet issues, the FCC maintains that transparency is important for consumer protection in the telecommunications context.[138] Martin suggests that when addressing cloud computing concerns, it will be important to ensure that the practices of cloud providers are understood and that customers have the ability to exercise control over their data.[139] Transparency could have additional advantages by encouraging cloud platforms to be more interoperable, allowing for greater data portability.[140] If the

133. *See* Martin, *supra* note 44, at 286 (discussing recently proposed legislation, standards, and governing principles).

134. 18 U.S.C. § 1030 (2006).

135. Martin, *supra* note 44, at 309–10.

136. *Id.* at 310.

137. *See, e.g.*, Werbach, *supra* note 8, at 1767 ("To achieve its public interest mandates, the FCC must consider . . . [and examine] transparency.").

138. *See id.* at 1837 (discussing the FCC's adoption of a transparency mandate in its Open Internet Order).

139. *See* Martin, *supra* note 44, at 286 ("Any solution needs to incorporate guarantees that data owners would be able to gain control of their data in a usable form should their service providers become inoperable.").

140. *See* Werbach, *supra* note 8, at 1839 (noting the ancillary benefits of transparency).

industry takes an approach to personal data that focuses on the ability of users to control their data, transparency may prove beneficial and alleviate some of the information asymmetry between cloud providers and their customers.[141]

Industry leaders are conscious of transparency concerns. A consortium of industry leaders put forth the Open Cloud Manifesto, advocating the use of standardization and collaboration to develop an "open cloud."[142] The Open Cloud Manifesto focuses on transparency and interoperability between cloud providers, with one of the goals being to minimize the lock-in issue.[143] If implemented, this manifesto might mitigate some of the data control issues that we are concerned about in this Article.

It could also facilitate transparency for users to be proactive about seeking information. The European Network and Information Security Agency (ENISA) suggests that users ask cloud providers about things like the provider's personnel security procedures, use of subcontractors, operational security procedures, disaster recovery protocol, and miscellaneous legal issues like data location, jurisdiction issues, and how the customer can recover data upon termination of the service.[144] We posit that users who are given the right to control their information are likely to be more involved in the process of controlling their own data.

F. Cloud Services in Different Industries

There are a number of professions in which practitioners are required to handle client or patient data with care, making data protection in these sensitive industries very important. One of these industries is the legal field, in which attorneys and their staff

---

141. Schwartz & Solove, *supra* note 3, at 1882.

142. Martin, *supra* note 44, at 286.

143. *See id.* at 310 (discussing the Open Cloud Manifesto in detail).

144. *See id.* at 311 (examining the European Network and Information Security Agency report, which recommends a series of user procedures that can be employed for self-protection).

are required to take great steps to protect client confidentiality.[145] Still, some state bar associations may recognize the convenience of cloud services and may be inclined to approve of attorney practices in which client information is stored using public cloud services.[146] Martin, however, suggests that the ABA should establish ethical guidelines relating to topics like document storage, e-mail, and confidentiality in the cloud.[147]

In the health care industry, there has been a shift toward using electronic medical records (EMR) as an alternative to paper records.[148] A more recent push is toward maintaining personal health records (PHR) online through services like Epic, Microsoft's HealthVault, and Google Health, in which the patient will have control over her records.[149] However, PHR providers do not fall within one of the statutory categories of "covered entities" under HIPAA, so the storage and transmission of personal health information is not currently regulated by HIPAA or any of the related rules.[150]

In addition to control, security of health information is also of paramount concern. McCarthy notes that the Health Information Technology for Economic and Clinical Health Act[151] requires users to be notified if there is a breach threatening PHR data,

---

145. MODEL RULES OF PROF'L CONDUCT R. 1.6, 5.3 (1983) (discussing confidentiality and the duties of nonlawyer staff, respectively).

146. *See* Martin, *supra* note 44, at 300–01 (citing a New York bar opinion about using e-mail services that scan e-mail content to generate targeted advertising).

147. *See id.* at 313 ("[T]he ABA should move quickly to establish ethical guidelines for lawyers who use cloud computing services . . . [including] document storage, e-mail, collaboration, due diligence for confidentiality, and breach notification related to cloud services.").

148. McCarthy, *supra* note 95, at 2250–51. EMRs, however, are generally limited to that specific provider, with no sharing of information. *See id.* ("Each health care provider maintains its own EMRs—physician's offices maintain their EMRs, hospitals maintain their EMRs, and so on.").

149. *See id.* at 2245, 2251–54 ("Until now, patients could request a copy of her [sic] medical records from their health care providers but have not had the opportunity to control them in the way that PHRs offer.").

150. *Id.* at 2258.

151. Health Information Technology for Economic and Clinical Health Act, Pub. L. 111–5, Div. A, Title XIII, Div. B, Title IV, 123 Stat. 226, 467 (2009) (codified in scattered sections of 42 U.S.C.).

and that the HHS has also promulgated a rule that requires PHR vendors to comply with notification requirements if a breach occurs.[152] The increased vulnerability of data in the cloud necessitates strong protections for PHR, like encryption, password protection, and authentication requirements.[153] One of our recommendations for regulating cloud providers focuses on establishing baseline standards for data protection, which could help address some of these issues.

III. Privacy Fundamentals

A. Privacy Theories

"Privacy" is an example of a word that can mean many different things.[154] It can be a handmade sign on the door of a teenager's room prohibiting entry by parents and little brothers. It can be the right to make one's own decisions without undue burden imposed by the government. On the Web, some people might consider social networking posts "private" if they are only viewable by the poster's four hundred closest friends,[155] while others do not consider anything that they do on the Web "private" unless all data is heavily encrypted and all of their traffic is routed through an anonymizer.[156]

---

152. *See* McCarthy, *supra* note 95, at 2263–64 (discussing new federal law governing PHR privacy and security).

153. *See id.* at 2267 ("PHRs should be required to employ best practices in data encryption, password protection, and authentication in order to safeguard PHI stored on their servers.").

154. *See* Anita L. Allen, *Privacy-As-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 864 (2000) [hereinafter Allen, *Data Control*] (noting the wide variation in how "privacy" is defined, even among people who seemingly are talking about the same privacy paradigm of privacy being data control).

155. Some argue, however, that such postings are still functionally private because of the boundaries that exist by making a posting viewable only by certain people. *See* Richards & Solove, *supra* note 1, at 1920–21 (citing Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005)). This view arguably does not consider the potential of screenshots of "friends only" postings being reposted elsewhere.

156. These three categories of privacy have been referred to as physical and proprietary privacy, decisional privacy, and informational privacy. Allen, *Data*

Some view privacy as a negative freedom, providing a freedom *from* something instead of a claim *to* something else.[157] Perhaps the most prevalent view of privacy over the years has been the secrecy paradigm of privacy, where privacy is limited to things that are secret.[158] There is also an "invasion conception" of privacy, where privacy violations are viewed as invasions of an interest.[159] Some view privacy as referring to inaccessibility, when a person or information about her is inaccessible to others.[160] Some also address what sort of harm is necessary to find a privacy violation. Solove asserts that there can be an infringement of privacy "even if no secrets are revealed and even if nobody is watching us," connecting the concepts of privacy and human dignity.[161]

The importance of privacy is sometimes stated in grandiose terms, tying the concept of privacy to democratic ideals like

---

Control, supra note 154, at 865–66.

157. *See* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 747–48 (1999) [hereinafter Allen, *Coercing Privacy*] (discussing conservative and liberal interpretations of the right to privacy).

158. *See* Solove, *Taxonomy, supra* note 111, at 497–98 ("Under the secrecy paradigm . . . if the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information. In many areas of law, this narrow view of privacy has limited the recognition of privacy violations."). This paradigm can be seen in the approach courts have taken to the Fourth Amendment, as well as in the tort of intrusion upon seclusion. *Id.* Solove takes the view that the secrecy paradigm approach to information privacy law is outmoded. SOLOVE, DIGITAL PERSON, *supra* note 2, at 143.

159. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 8 (defining the invasion conception of privacy). Solove says that the Warren and Brandeis theory of privacy falls within this conception of privacy, with a focus on the existence of discrete wrongs to individuals. *See id.* at 93–94 (discussing the two models for the protection of privacy). Solove also criticizes the invasion conception of privacy by arguing that it overlooks the structural nature of certain privacy problems that affect not just an individual, but also society as a whole. *See id.* at 97.

160. *See* Allen, *Data Control, supra* note 154, at 867 ("[O]ther than in contexts in which 'privacy' holds its decisional and proprietary meanings, privacy refers to a degree of inaccessibility of a person or information about her to others' five senses and surveillance devices."); Allen, *Coercing Privacy, supra* note 157, at 724 ("Privacy obtains where persons and personal information are, to a degree, inaccessible to others.").

161. SOLOVE, DIGITAL PERSON, *supra* note 2, at 44, 55.

independent thought and the right to take political actions.[162] Alan Westin, an early information privacy scholar, defined 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."[163] The law has taken a number of approaches to address different concerns associated with privacy. The right to privacy has been recognized in the United States for over a century, though coherent definitions have generally been lacking.[164] Solove views privacy as a concept that encompasses many different kinds of distinct but interrelated issues.[165]

The concept of privacy also overlaps with constitutional protections under the Fourth Amendment, where the focus is on a "reasonable expectation of privacy."[166] This legal concept is connected to several philosophical questions: what is privacy, where does it exist, and is it reasonable to expect a particular action to be private? If the government conducts surveillance somewhere that there is an expectation of privacy, a warrant is

---

162. *See* Allen, *Coercing Privacy, supra* note 157, at 734 ("Liberal theorists claim that we need privacy to be persons, independent thinkers, free political actors, and citizens of a tolerant democracy."); Solove, *Taxonomy, supra* note 111, at 489 (citing Julie Cohen and Paul Schwartz for the argument that "privacy is a constitutive element of a civil society").

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

164. *See* Richards, *supra* note 114, at 1155 (discussing the sometimes uneasy coexistence of privacy and speech); Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CAL. L. REV. 1925, 1963 (2010) ("[I]n their comprehensive work, Privacy, Property and Personality, [the authors] argue that the right of privacy in the United States 'remains somewhat conceptually uncertain and poorly defined.'" (quoting HUW BEVERLEY-SMITH ET AL., PRIVACY, PROPERTY AND PERSONALITY 207 (2005))); Solove, *Taxonomy, supra* note 111, at 562 ("But our understanding of privacy remains in a fog, and the law remains fragmented and inconsistent.").

165. Richards & Solove, *supra* note 1, at 1914–15; Solove, *Taxonomy, supra* note 111, at 562.

166. *See* Rebecca N. Cordero, *No Expectation of Privacy: Should School Officials be Able to Search Students' Lockers Without Any Suspicion of Wrong Doing?*, 31 U. BALT. L. REV. 305, 308 (2002) ("In his concurrence, Justice Harlan coined the term a 'reasonable expectation of privacy' to describe an area subject to the protection of the Fourth Amendment.").

necessary to protect against unreasonable intrusion.[167] Generally, public surveillance is not viewed as an intrusion because behaviors are being exposed to the public, but there may be exceptions when such surveillance is overzealous.[168] As one court said, "The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."[169]

The Fourth Amendment protection against unreasonable searches and seizures, the protections afforded to electronic communications under the ECPA, and privacy torts are three large legal categories for the concept of privacy.[170] As we examine in later sections, the application of the Fourth Amendment and the ECPA to the Information Age is far from clear. Additionally, there is also a sense that privacy tort law is ineffective at addressing these issues.[171] The traditional model for privacy protection simply does not address the sorts of privacy problems that have arisen recently.[172]

The desire for privacy is arguably an innate human trait, and privacy theorists thus often make philosophical or literary allusions when explaining the importance of privacy. One of the most vivid images for the modern information privacy problems is Jeremy Bentham's design for a prison that he called the

---

167. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

168. *See* Solove, *Taxonomy*, *supra* note 111, at 498 ("In some cases, however, courts have recognized a harm in public surveillance.").

169. Sanders v. Am. Broad. Comps., Inc., 978 P.2d 67, 72 (Cal. 1999).

170. Other relevant elements of constitutional law include the freedom of association and the freedom of anonymous speech under the First Amendment. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 64–65 (discussing the right to privacy).

171. *See* Richards & Solove, *supra* note 1, at 1889 ("Today, the chorus of opinion is that the tort law of privacy has been ineffective, particularly in remedying the burgeoning collection, use, and dissemination of personal information in the Information Age.").

172. *See id.* at 1918 ("Tort law has not emerged as the leading protector of privacy."). Solove argues that many of the privacy problems we confront today are systemic in nature, stemming from information flows, with multiple actors being responsible for these problems. Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1232 (2003) [hereinafter Solove, *Architecture*].

Panopticon.[173] In the Panopticon, prison cells are distributed around a central observation tower, and someone placed in the tower can monitor all of the prison cells without the prisoners knowing when they are being observed, and this fear of observation leads to the prisoners behaving better.[174] In the context of the Internet, Schwartz has argued that there is a danger both of a government Panopticon and private Panopticons operated by private entities that collect and use information while resisting attempts at transparency.[175]

Privacy concerns gained more public visibility in the early 1980s, perhaps due to the era's relationship with George Orwell's dystopian novel *Nineteen Eighty Four*.[176] Similar to the Panopticon, the telescreens of *Nineteen Eighty Four* allowed the government to monitor citizens without their knowledge that they were being observed.[177] Perhaps thanks in part to this work of fiction—and the fact that it is required reading for many high school seniors—U.S. citizens are keenly aware when government action has the potential to intrude on privacy and lead to an authoritarian state.[178]

---

173. *See* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 201 (Alan Sheridan trans., 1977) (listing the essential elements of the Panopticon's effectiveness being visibility and unverifiability, visibility referring to that of the tower, and unverifiability referring to the prisoners' inability to know whether they are being observed).

174. *Id.* at 201; Solove, *Architecture, supra* note 172, at 1240. Solove also notes Foucault's argument that the Panopticon represents power relations in society. *Id.* at 1240.

175. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 852–53 (2000) [hereinafter Schwartz, *State*] (discussing the creation of a privately operated Panopticon in the context of Internet privacy).

176. *See* Schwartz & Solove, *supra* note 3, at 1825–26 ("Part of this attention was driven, in turn, by the arrival of George Orwell's titular year, 1984.").

177. SOLOVE, DIGITAL PERSON, *supra* note 2, at 31.

178. *See* James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1 (last visited Feb. 3, 2013) (describing a massive new National Security Agency data collection center under construction) (on file with the Washington and Lee Law Review). Solove takes issue with the frequent comparisons to *Nineteen Eighty Four*, instead arguing that because the privacy threats are distributed across private companies and government bureaucracy, a better comparison would be to Kafka's *The Trial*. SOLOVE, DIGITAL PERSON, *supra* note 2, at 7–9 ("[F]or a more

1. Warren and Brandeis

Theoretical discussions of privacy law often begin in 1890, when Samuel Warren and Louis Brandeis published their article about privacy as a right of personality.[179] Warren and Brandeis were especially concerned about the use of private information by the media and the implications of technological developments like new and cheaper photography technologies.[180] Warren and Brandeis also argued that a person's intellectual property was not a matter of private property, but rather was related to the person's "inviolate personality."[181]

Warren and Brandeis were supportive of the idea of applying the common law to protect a right to privacy, which they famously summarized as a "right to be let alone."[182] In their article, they supported enforcing the right of privacy using tort damages to provide individuals with compensation for the "mental suffering" caused by the privacy invasions.[183] This view

---

complete understanding of the issues, I turn to . . . Franz Kafka's depiction of bureaucracy in *The Trial*."). In *The Trial*, the protagonist is under arrest and does not understand why because the bureaucratic government has a large amount of information about the protagonist that it refuses to share with him. *See id.* at 8–9 (discussing Kafka's novel *The Trial*).

179. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890); *see also* Richards & Solove, *supra* note 1, at 1888 (writing that Warren and Brandeis popularized privacy in American law with their famous article in 1890); Schwartz & Solove, *supra* note 3, at 1819 (recognizing the Warren and Brandeis article as a famous example of privacy's early jurisprudence).

180. *See* Richards, *supra* note 114, at 1198 ("[M]odern thinking about the right of privacy is often traced to Warren and Brandeis's privacy article, in which their concern was not primarily data privacy, but rather media use of private information."); Schwartz & Solove, *supra* note 3, at 1819 ("The paradigmatic privacy invasion for Warren and Brandeis concerned the press intruding on the privacy of individuals by printing gossip about them."). This position leads to a balancing of the interest in privacy against interests under the Freedom of the Press Clause of the First Amendment. Richards & Solove, *supra* note 1, at 1892; Solove, *Architecture, supra* note 172, at 1229.

181. Schwartz & Peifer, *supra* note 164, at 1944.

182. Richards & Solove, *supra* note 1, at 1891.

183. Solove, *Architecture, supra* note 172, at 1229–30. Warren and Brandeis expressed a preference for money damages over injunctions, which they noted may be appropriate in narrow circumstances, and asserted that narrower circumstances would be required for criminal penalties to be appropriate. *Id.* at

of privacy harms focuses on dignitary harms, like harm to reputation, based on the concept that privacy violations are a type of invasion to the victim's dignity.[184]

Case law on privacy was heavily influenced by the Warren and Brandeis article, especially when the dispute involved the use of photographs of ordinary people to promote a company's product.[185] However, by the time the Warren and Brandeis article was fifty years old, privacy was still a very minor doctrine in tort law. Only twelve states recognized the right of privacy by common law, and only two recognized it by statute.[186]

2. Prosser

For modern privacy scholars, the next major development in the privacy law of the United States was the 1960 publication of William Prosser's article, *Privacy*.[187] In this article, Prosser argued that there were four categories within privacy tort law: appropriation privacy, intrusion privacy, unauthorized public

---

1230.

184. *See* Solove, *Taxonomy, supra* note 111, at 487; SOLOVE, DIGITAL PERSON, *supra* note 2, at 93–94 (referring to the privacy theory of Warren and Brandeis as being based on an "invasion conception" of privacy, which turns on the existence of discrete wrongs to individuals).

185. *See* Richards & Solove, *supra* note 1, at 1892–93 ("Warren and Brandeis's approach to privacy was in one sense profoundly conservative, as it was part of a broader legal strategy employed by late-nineteenth-century elites to protect their reputations from the masses in the face of disruptive social and technological change.").

186. *See id.* at 1895 (discussing the number of states that recognize certain common law privacy rights).

187. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960); *see also* Schwartz & Peifer, *supra* note 164, at 1926 ("Today, Prosser's verdict on the momentous article by Samuel Warren and Louis Brandeis can fittingly be applied to his own work: 'It has come to be regarded as the outstanding example of the influence of legal periodicals upon the American law.'" (quoting William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960))).

disclosure of private facts, and false light.[188] In constructing these four categories, Prosser analyzed hundreds of privacy cases.[189]

Prosser's approach was thus fairly comprehensive, but the categories he created were also narrow and rigid.[190] The rigidity was perhaps based on Prosser's concern that privacy torts might swallow up established doctrines like defamation law and intentional infliction of emotional distress.[191] In some ways, Prosser seemed to be skeptical of privacy laws because of their potential to interfere with the flow of information, and he would have been concerned with the balance between newsworthiness and conflicting privacy interests.[192] Unfortunately, this rigidity also makes it difficult to apply these torts to modern information privacy problems.[193]

---

188. Richards, *supra* note 114, at 1198–99; *see also* SOLOVE, DIGITAL PERSON, *supra* note 2, at 58; Schwartz & Peifer, *supra* note 164, at 1941; Schwartz & Solove, *supra* note 3, at 1820.

189. Richards & Solove, *supra* note 1, at 1889.

190. *See id.* at 1890 ("His skepticism about privacy, as well as his view that tort privacy lacked conceptual coherence, led him to categorize the law into a set of four narrow and rigid categories.").

191. *See id.* at 1890, 1900 (describing Prosser's concern that privacy law's "haphazard development threatened to swallow up established doctrines, such as defamation law, as well as new doctrines, such as intentional infliction of emotional distress, that he felt had more promise"). The intrusion into seclusion tort includes, as its main element, intentional infliction of emotional distress, but does not require a showing of extreme outrage, serious mental harm, or a showing that injuries were nontrivial. *Id.* at 1890. Prosser expressed concern that the false light and disclosure of private facts torts involved an examination of reputation, overlapping with defamation law. *Id.* Prosser was also concerned about privacy torts being overbroad and interfering with freedom of speech and of the press. *Id.*

192. *See* Schwartz & Peifer, *supra* note 164, at 1956–57 ("Due to Prosser's strong belief in liberal flows of information, moreover, his article reflects a strong undercurrent of skepticism about the legal protection of privacy.").

193. *See* Richards & Solove, *supra* note 1, at 1904 ("[W]hile Prosser gave tort privacy a legitimacy it had previously lacked, he also fossilized it and eliminated its capacity to change and develop."). *But see* Schwartz & Peifer, *supra* note 164, at 1929 (disagreeing with some of Richards and Solove's criticism of Prosser, asserting that if it had not been for Prosser, privacy would likely be much less protected in the United States); *id.* at 1983 ("Rather than creating an ossified privacy concept, Prosser's contribution generated useful doctrinal categories where there previously had been unclassified cases and a lingering air of skepticism towards the tort.").

Breach of confidentiality has been described as a tort that addresses privacy violations in specific contexts.[194] Though the concepts are related, Prosser did not include breach of confidentiality in his categories of privacy torts.[195] This may be because Prosser drew a line between privacy and what would be addressed under agency or contract law. Compared to Warren and Brandeis, Prosser was also less focused on the idea of personality as a justification underlying privacy protections.[196]

a. Prosser's Privacy Torts and Information Privacy

Prosser's torts differ significantly from each other. In Prosser's article, he points out that intrusion and disclosure both require an invasion into something secret, which is not required of false light or appropriation.[197] Disclosure and false light have publicity as an essential element, while intrusion and appropriation do not (though appropriation usually involves publicity).[198] Additionally, only false light requires falsity, and only appropriation requires that the defendant have gained some advantage from the use.[199]

The tort of appropriation has evolved somewhat from Prosser's time. When Prosser originally wrote *Privacy*, he noted

---

194. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 77 ("The common law tort of breach of confidentiality . . . enables people to sue for damages when a party breaches a contractual obligation (often implied rather than express) to maintain confidentiality.").

195. *See* Richards & Solove, *supra* note 1, at 1909 ("A second notable omission from Prosser's taxonomy was the tort of breach of confidence."). In Prosser's treatise, Prosser addressed this concern by stating, "The right of privacy, as such, is to be distinguished from liability found upon the breach of some confidential or fiduciary relation . . . ." *Id.* at 1910 (quoting WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 1062 (1st ed. 1941)).

196. One of Prosser's contemporaries was Edward Bloustein, who differed from Prosser in the degree to which the former argued for the idea that privacy law protects an "inviolate personality." Schwartz & Peifer, *supra* note 164, at 1945.

197. *See* Prosser, *supra* note 187, at 407 (discussing and defining common facets of privacy).

198. *See id.* (examining false light in relation to privacy generally).

199. *See id.* (discussing false light in detail).

that under the common law, all four of the recognized categories of privacy claims were specific to the individual and were not assignable, though three states at the time did recognize under statute that a publication-based claim could be brought after a person's death.[200] On the other hand, the modern right of appropriation allows a likeness to be treated as descendible property.[201]

These torts have questionable utility in the modern context of information privacy. The privacy tort of invasion typically requires the invasion to be of an offensive nature, but a lot of information collection appears largely innocuous.[202] In *Shibley v. Time, Inc.*,[203] the litigation concerned the magazine's sale of their subscriber information to advertisers, but this sale was found to not meet the injury requirements for Ohio's common law invasion of privacy tort.[204] Courts have also rejected the theory that the tort of appropriation could apply to the data collection problem.[205] Thus, it is likely that addressing personal privacy issues will require either the revision of privacy torts or the introduction of new alternatives.

3. Modern Informational Privacy Theory

While there are many types of privacy, the type that we are most concerned with is informational privacy and the right of a person to keep information about herself from being used by

---

200. *See id.* at 408 (discussing the qualities of invasion that would constitute a tort).

201. *See* Schwartz & Peifer, *supra* note 164, at 1965 ("The overwhelming majority of states in the United States have also recognized a postmortem dimension to the publicity right."). Schwartz and Peifer point to the example of Elvis, whose publicity rights have been sold and resold multiple times since his death. *Id.* at 1966.

202. *See* Richards & Solove, *supra* note 1, at 1919 (stating that many "privacy torts—public disclosure, intrusion, and false light" require a showing that the privacy invasion be highly offensive).

203. Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975).

204. *See* Richards & Solove, *supra* note 1, at 1919.

205. Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1357 (Ill. App. Ct. 1995) (ruling that there was not an appropriation claim when American Express sold customer names to merchants); Richards & Solove, *supra* note 1, at 1919.

others. Our understanding of informational privacy in the modern context also needs to take social norms into consideration. In the United States, the younger generation seems to value privacy much less than the older generations,[206] though some empirical research casts doubt on the idea that there is a meaningful difference between how different age groups view and prioritize privacy.[207] Solove has become a leader in modern informational privacy theory, with some scholars asserting that Solove is Prosser's modern heir.[208] Not entirely dissimilar from Prosser's approach, Solove divides privacy problems into four categories: information collection, information processing, information dissemination, and invasion.[209]

Informational privacy implicates the potentially conflicting interests of content owners and content users. If protections of personal privacy are too strong, businesses that use customer information to target people who would be interested in a new product may be prevented from doing so. There are some First Amendment concerns as well. Chiefly among them is to what extent do I have the right to use the law and the courts to prevent you from speaking about me?[210] There is also a question of accountability to prevent legitimate privacy regulation from applying in ways that are not optimal for society.[211]

Schwartz argues that privacy is a "constitutive value" that is valuable not for its own virtues or effects, but because some degree of protection for personal privacy is a necessary condition

---

206. *See* Allen, *Coercing Privacy, supra* note 157, at 736–37 ("Generational differences in the taste for privacy may be significant in the United States, as younger Americans appear to be learning to live reasonably well and happily without privacy.").

207. Hoofnagle, King, Li & Turow, *supra* note 109, at 20.

208. *See* Schwartz & Peifer, *supra* note 164, at 1940 ("In this sense, Daniel Solove proves the modern heir of the Berkeley Dean.").

209. Solove, *Taxonomy, supra* note 111, at 489.

210. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STANFORD L. REV. 1049, 1049 (2000).

211. *See* Allen, *Data Control, supra* note 154, at 861 (citing Schwartz for two important normative questions facing contemporary privacy theorists: how to protect privacy while preserving accountability, and the appropriate role of the state in regulating personal privacy).

for a society that values individual identities and deliberative democracy.[212] Taking the view that privacy is of vital importance, Allen argues that privacy can be lost through voluntarily giving it up, and that this raises similar moral and policy implications as someone who voluntarily sells himself into slavery.[213] In the same way that people are forced to be free by being prohibited from selling themselves into slavery, Allen argues that people should be forced to be private to better allow them to "reap the full dignitarian and political consequences of privacy."[214]

a. Concepts of Privacy

Different approaches to privacy find the value of privacy in different things. Under a communitarian view of privacy, privacy is valuable because it protects a social good by allowing citizens to more effectively participate in a deliberative democracy.[215] The liberal approach to privacy focuses on the individual and on personal autonomy.[216] A liberal concept of privacy could be

---

212. *See* Schwartz, *State, supra* note 175, at 834 ("Informational privacy, whether on or off the Internet, should not be considered a right of control. Instead, it should be conceptualized as a constitutive value."). A constitutive value is one that derives its value not from the causal effects of the value's existence or from the existence of the value for its own sake, but for its role in "a larger complex that is itself valued." GERALD DWORKIN, THE THEORY AND PRACTICE OF AUTONOMY 80 (1988). The value of privacy is occasionally the subject of discussion, with some scholars asserting that privacy is not generally worth protecting except for people who have something to hide. JEFFREY H. REIMAN, CRITICAL MORAL LIBERALISM: THEORY AND PRACTICE 171 (1997).

213. *See* Allen, *Data Control, supra* note 154, at 869 (discussing the moral and political implications associated with privacy loss). Allen has also examined whether people could be forced to be private in the same way they can be forced to be free. *See* Allen, *Coercing Privacy, supra* note 157, at 728 ("We are forced to be free. Liberal governments cannot permit us to sell ourselves into slavery. Are we forced to be private?").

214. Allen, *Coercing Privacy, supra* note 157, at 752.

215. *See* Schwartz, *State, supra* note 175, at 836 ("In searching for ways to construct this strong democracy, these thinkers emphasize common participatory activities, reciprocal respect among political equals, and the development of consensus about political issues.").

216. *See* Allen, *Coercing Privacy, supra* note 157, at 739 ("Liberal moral philosophers maintain that respecting the many forms of privacy is paramount

further broken down into categories including physical privacy, informational privacy, proprietary privacy, and decisional privacy.[217]

Some view control over data as central to privacy.[218] Solove points to the lack of control over data as one of the systemic problems that enables identity theft.[219] One potential privacy right related to controlling data is a right to prevent access to the data.[220] After personal information is collected, the person to whom the information refers typically has no control over future use of the information.[221] Even if courts or policy makers decree that a person has a "right" to control his personal data, he still may lack the ability to meaningfully control his information.[222] Our recommendations address similar issues under the broad label of "data control," including the need for data mobility and a right of data withdrawal.

It is unlikely that an individual will ever be able to exercise absolute control over his data. The government can readily access

---

to respect for human dignity, personhood, moral autonomy, workable community life, and tolerant democratic political and legal institutions.").

217. *Id.* at 723–25. Allen notes that the concept of "private choice" is stronger than the general liberal concept of "privacy." *Id.* at 727–28. Allen defines informational privacy in this way: "Informational privacy obtains where information actually exists in a state of inaccessibility, whether it is locked in a file drawer, computer, or in someone's mind. Anonymity, confidentiality, reserve, and secrecy—not merely having the choice to bring these about—are forms of privacy." Allen, *Data Control, supra* note 154, at 869.

218. *See* Allen, *Data Control, supra* note 154, at 863 (defining privacy as data control, and the right to privacy as the right to control, and asserting that the central aim of privacy regulation should be to promote individuals' right to control their personal data).

219. *See* Solove, *Architecture, supra* note 172, at 1258 ("Therefore, the problem runs deeper than identity theft. It is the fact that we have so little participation in our personal data combined with the fact that it flows so insecurely and carelessly without sufficient control.").

220. *See* Birnhack & Elkin-Koren, *supra* note 108, at 344 ("There are two principal understandings of the right to privacy in personal data: privacy as a right to control data ('privacy as control') and privacy as a right to prevent access ('privacy as access').").

221. *See* Solove, *Architecture, supra* note 172, at 1234 ("[P]ersonal information is not only outside our control but also is subjected to a bureaucratic process that is itself not adequately controlled." (citation omitted)).

222. *Id.*

individuals' financial information, and medical privacy is subject to the sharing of medical information between medical professionals and health insurance companies.[223] It is thus probably fair to say that to the extent that privacy involves the control of data, this control is qualified in certain circumstances. In the online context, Schwartz goes so far as to say that control over personal information on the Internet is an illusion.[224] When consumers are presented with take-it-or-leave-it TOS agreements on websites, there is typically no negotiation of terms, and thus no ability to exercise meaningful control.[225] Schwartz argues that informational privacy is not just a matter of having a right to control, but instead is a matter of line drawing to shape behaviors and thus either encouraging or discouraging the use of certain categories of expression and action.[226]

b. The First Amendment Critique

Some argue that a right of "data privacy" would conflict with the First Amendment by interfering with the dissemination of truthful information.[227] Volokh is the most prominent proponent of the First Amendment critique, arguing that data privacy regulation amounts to "a right to have the government stop you

---

223. *See* Allen, *Data Control, supra* note 154, at 872 (discussing moral accountability, control, and privacy). However, though the federal government may have access to detailed financial records, this does not necessarily mean that the government can then disclose the information. In *Wine Hobby USA, Inc. v. IRS*, the court declined to order the government to disclose registered home wine producers under FOIA, concluding that such a disclosure would violate the registered parties' privacy. Wine Hobby USA, Inc. v. United States IRS, 502 F.2d 133, 135 (3d Cir. 1974); Allen, *Data Control, supra* note 154, at 873–74.

224. *See* Schwartz, *State, supra* note 175, at 832 (arguing that simply declaring a property right in personal information will not resolve any of the major issues relating to information privacy); *see also* Allen, *Data Control, supra* note 154, at 869 (discussing the limits burdening the privacy control paradigm).

225. Solove, *Architecture, supra* note 172, at 1235.

226. *See* Schwartz, *State, supra* note 175, at 858 ("As a result, information privacy should not create data fortresses, but shifting multidimensional data preserves that insulate personal data from different kinds of observation by different parties.").

227. Richards, *supra* note 114, at 1150–51.

from speaking about me."[228] Cate argues that there should be full First Amendment protection for electronic information flows, and that truthful data should be allowed to flow unimpeded to prevent violations of the First Amendment.[229] Richards counters these arguments, arguing that data privacy properly concerns economic rights, and that bringing the First Amendment into the debate wrongly makes it into a civil rights issue.[230] Richards also points out that the First Amendment critique is weak because it does not consider the many types of "speech" that are outside the First Amendment's protection, like fraud, solicitation, antitrust law, threats, and libel.[231]

There is some case law support for the First Amendment critique. In *U.S. West, Inc. v. FCC*,[232] the Tenth Circuit analyzed the constitutionality of the FCC's interpretation of a statutory confidentiality provision, which required customers to opt in before a carrier would be permitted to share the customers' confidential information.[233] In that case, the Tenth Circuit stated that privacy "imposes real costs on society."[234] The court concluded that the opt-in regime for the sharing of confidential

---

228. *See* Volokh, *supra* note 210, at 1050–51; *see also* Richards, *supra* note 114, at 1161 (discussing the First Amendment and privacy regulation (citation omitted)).

229. FRED H. CATE, PRIVACY IN THE INFORMATION AGE 1–4 (1997); Richards, *supra* note 114, at 1161.

230. *See* Richards, *supra* note 114, at 1151 ("This Article takes issue with the conventional wisdom that regulating databases regulates speech, that the First Amendment is thus in conflict with the right of data privacy, and that the Constitution thereby imposes an insuperable barrier to basic efforts to tackle the database problem.").

231. *See id.* at 1171–73 (discussing the fact that much "speech" is outside the scope of the First Amendment and providing an alternative approach).

232. U.S. West, Inc. v. F.C.C., 182 F.3d 1224 (10th Cir. 1999).

233. *See id.* at 1230.

234. *See id.* at 1235 (stating that privacy does not inherently constitute a substantial state interest for First Amendment commercial speech analysis purposes, and further justification is required). As part of its analysis, the court concluded that the FCC's regulation was not narrowly tailored because it did not adequately consider a less restrictive alternative, specifically an opt-out regime. *Id.* at 1238–39.

information promulgated by the FCC violated the First Amendment commercial speech rights of the carriers.[235]

Ultimately, the First Amendment critique has many flaws, but it illustrates the sort of theoretical balancing that Prosser, Warren, and Brandeis were concerned about. Whether informational privacy is truly more of an economic or First Amendment issue is outside the scope of our research. We mention the First Amendment critique here only to emphasize that the balancing of interests is a pervasive theme in discussions of privacy theory.

c. Privacy as a Commodity

Some theorists have suggested understanding privacy as a property right.[236] Property can be described as an interest in an object in which the owner can enforce that interest against all others.[237] To law students, the concept of property is often described as a bundle of rights. A lot of property is freely alienable; that is, it can be sold, traded, and gifted as the owner sees fit.[238] Some property, like human tissue, can be donated but not sold.[239] With regard to privacy, views differ about the extent to which privacy should be alienable at all.[240] Some scholars advocate propertizing personal information, while others

---

235. *See id.* at 1230, 1240.

236. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 77 (noting that Alan Westin took this view). *But see* Schwartz, *State, supra* note 175, at 832 (arguing that simply declaring a property right in personal information will not resolve any of the major issues relating to information privacy).

237. Schwartz, *Property, supra* note 10, at 2058.

238. One scholarly definition of inalienabilities posits that inalienabilities amount to "any restriction[s] on the transferability, ownership, or use of an entitlement." *Id.* at 2095 (citing Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 COLUM. L. REV. 931, 931 (1985)).

239. *See* Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 498 (Cal. 1990) (Arabian, J., concurring) (viewing the question of property rights in human tissue as a moral issue).

240. For example, Allen argues that privacy should not be viewed as optional, and that people should be restrained from trading away their privacy because of privacy's importance in a society that values personal identity. Allen, *Coercing Privacy, supra* note 157, at 729.

advocate an outright ban on data trade.[241] Schwartz suggests a category that he calls "information property," which is itself a bundle of interests made up of five areas: "inalienabilities, defaults, rights of exit, damages, and institutions."[242]

Allen argues that the expectations of people with regard to privacy have been decreasing, with people being willing to prioritize informational privacy lower than they prioritize other goods.[243] There is also some disconnect between what people say they want in terms of privacy, and then what people actually do, often being quick to accept something in exchange for their personal information.[244] Currently, no value is consistently assigned to personal information, and Schwartz suggests that this lack of a value contributes to the lack of appreciation that people have for their private data.[245]

---

241. *See* Schwartz, *Property, supra* note 10, at 2057 (recognizing that "a strong conception of personal data as a commodity is emerging in the United States" but that some legal scholars have been "suspicious of treating personal data as a form of property").

242. *Id.* at 2060. Schwartz suggests implementing a system that has use-transfer restrictions and an opt-in default. *See id.* ("This Article's model of propertized personal data involves the development of a hybrid inalienability consisting of a use-transfer restriction plus an opt-in default.").

243. *See* Allen, *Coercing Privacy*, *supra* note 157, at 729–30 (arguing that consumer behavior and popular culture show that people prefer less privacy when using technology than other goods). Allen also notes that because of the deprioritizing of privacy, people may be more willing to trade privacy for things like entertainment, personal profit, medical care, and access to a certain community. *See* Allen, *Data Control*, *supra* note 154, at 871 (noting that people may disclose private information for various benefits and in doing so either send strong messages to policymakers that people do not value privacy in their technological encounters or stimulate them to paternalistically "coerce" privacy). An antipaternalist approach to privacy would say that privacy is a good if people desire it, but that it should not be forced upon them. On the other hand, the paternalist approach would impose privacy on people who might not want it. There are a number of laws that mandate privacy, like laws requiring people to wear clothes in public and building codes regulating the placement and design of residential housing. *See id.* (noting that the idea of privacy coercion is not foreign in American law).

244. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 80–81 (noting that, despite people's reflexive desire to protect their private data, most people take minimal precautions and would relinquish their data for money).

245. *See* Schwartz, *Property*, *supra* note 10, at 2076 (noting a higher appreciation for one's personal data may accompany higher market value for it).

In their book, Hagel and Singer proposed the use of "infomediaries," a label used to describe companies that would serve as intermediaries between consumers and companies that collect their data.[246] While discussion of this idea has not been pervasive over the last decade, the ideas underlying it form the basis for some start-up companies.[247] Though the impact of such efforts has not yet been seen, infomediaries might be an effective private market solution to the problems related to the decline of privacy on the Internet, provided it does not prove counterproductive to view privacy as a commodity. In a similar vein, Ayres and Funk have suggested implementing a system for telemarketers in which telemarketing is shifted to an opt-in paradigm in which customers can opt in to be contacted and are also compensated for receiving telemarketing calls.[248] Solove argues that compensation for information would not solve the problem, however, arguing that the real problem is a lack of control over data, lack of meaningful participation in the process, and lack of transparency about future data use.[249]

B. Privacy Law

Because intrusions into privacy on the Web are so prevalent, some argue that the government should regulate the Internet to promote consumer privacy, but others worry that this could harm

---

246. *See* JOHN HAGEL III & MARC SINGER, NET WORTH: SHAPING MARKETS WHEN CUSTOMERS MAKE THE RULES 28 (1999) (suggesting a role of intermediaries in helping consumers obtain the most value in exchange for their personal information and also protecting that information from being abused).

247. *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. TIMES, Feb. 12, 2012, at B3 (noting the existence of start-ups that would allow people to control and maybe even profit from their "digital trails").

248. *See* Schwartz, *Property*, *supra* note 10, at 2079 (noting that telemarketing is presently inefficient because it reaches an "excessively broad audience" and suggesting that opt-in programs would "add incentives to target likely customers").

249. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 89–90 (noting that, if people only have the right to sell their data, the result is an "all or nothing" exchange in which the consumer is not left with a viable choice between the two alternatives).

the online advertising industry and other interests.[250] In this subpart, we will first review some of the issues that emerge when discussing privacy regulation, before turning to existing bodies of law to evaluate the extent to which data control issues, like data mobility and data withdrawal, may fall within current law.

1. Steps Toward Regulation of Privacy

When a social issue has to be addressed, there are two primary options: address the problem through the market and self-regulation, or have the government regulate it. The dichotomy of self-regulation versus government regulation also arises in the privacy context. Some say that the government should not regulate privacy, suggesting that it would be too paternalistic to assume that the government knows best, though others argue that self-regulation is not a viable option because of the lack of mechanisms in the market to enable the exercise of informed, meaningful choices by individuals.[251]

There are a number of arguments in favor of self-regulation of privacy issues online. Birnhack and Elkin-Koren concluded from their data that law was not important in the shaping of website behavior and privacy practices, suggesting the market forces may be more effective than law at protecting privacy.[252] Others say that rules to protect privacy could have negative

---

250. *See* Lanois, *supra* note 18, at 34 (noting that Internet tracking and selling of personal data has pushed the government to promote greater consumer privacy and others to seek relief through the courts, resulting in sizable awards).

251. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 90–91 (recognizing that although proponents of market-based solutions to privacy concerns criticize the government for paternalism, the market fails to provide adequate mechanisms for the protection of privacy).

252. Birnhack & Elkin-Koren, *supra* note 108, at 378 (arguing that the "law does not appear to play an important role" in Israeli Internet privacy practices). However, the authors do not think that law is completely irrelevant, arguing that there is a circular relationship between privacy regulations and what amounts to a "reasonable expectation of privacy." *See id.* at 379 ("In the United States, data protection law plays another role. Given . . . the 'reasonable expectations' test within U.S. privacy law, concrete regulations help shape these expectations . . . . The fact that the law requires certain measures has a large effect on data subjects' expectations and . . . the reasonability of expectations.").

effects like decreasing the information available and increasing transaction costs.[253] If the private resolutions to privacy conflicts are preferred, Solove suggests that fiduciary relationships could be recognized under the law when a company collects and uses personal information.[254]

On the other hand, government intervention can be very helpful in advancing change. Consider, for example, the importance of civil rights legislation in ending institutional segregation. If remedying discrimination had been left to the market to self-regulate, improvements may have been much slower. With respect to online privacy, we disagree with the conclusions of Birnhack and Elkin-Koren concerning the value of government oversight, and assert that the enforcement part of the law is of the utmost importance and was not something that these researchers examined in adequate detail.[255] Additionally, while it is true that government regulation might have negative effects, this is just as true of trusting market self-regulation. In virtually any context, when faced with multiple options, there will be potential downsides to every option. Thus, the most important thing is to balance the positive and negative.

Fair Information Practices (FIPs) are often referenced as a guide for privacy regulations. When examining the core principles of privacy regimes of different governments, some patterns emerge, including an emphasis on notice, confidentiality, and data security.[256] These principles also underlie the idea of FIPs, which address how to handle and use personal information,[257] and often focus on responsibility and participation in the collection and use of data.[258] The Federal Trade Commission

253. *See* Richards, *supra* note 114, at 1159–60 (noting that this is the view of some law and economics scholars).

254. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 103 (recognizing that the disparities in knowledge between consumers and market participants of how consumer data is used may support a court's finding of a fiduciary relationship).

255. *See supra* note 252 and accompanying text (discussing Birnhack and Elkin-Koren's views on privacy law and the cloud).

256. *See* Birnhack & Elkin-Koren, *supra* note 108, at 350 (noting that foreign governments, like those of members of the European Union, exhibit data protection standards similar to those contained in U.S. law).

257. *See* Solove, *Architecture, supra* note 172, at 1266 (describing FIPs).

258. *See id.* at 1268 (describing the two focuses of FIPs: responsibility and

(FTC) views FIPs as being based on five core principles: (1) notice and consumer awareness; (2) consumer choice and consent; (3) access and participation in the process; (4) data integrity and security; and (5) enforcement and redress.[259] Schwartz and Solove suggest using FIPs to varying degrees, dependent on whether the personal information is identified or identifiable.[260]

Whether new regulation is needed at all ultimately depends on whether the current regulatory scheme is too flawed to offer meaningful guidance. For this reason, we turn now to an examination of current U.S. privacy law.

2. Federal Privacy Statutes and State Laws

Federal privacy law focusing on consumer protection is typically narrow, often focusing on the type of records in issue or a particular industry.[261] Early congressional action on privacy includes the Fair Credit Reporting Act (FCRA)[262] in 1970 and the Family Educational Rights and Privacy Act (FERPA)[263] in 1974.[264] Other federal statutes addressing specific privacy issues

---

participation); SOLOVE, DIGITAL PERSON, *supra* note 2, at 105 (same).

259. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23.shtm (reporting to Congress on five core principles of privacy protection).

260. *See* Schwartz & Solove, *supra* note 3, at 1880–81 (suggesting that, for example, full notice, access, and correction rights would probably not be necessary if only identifiable data is at issue, whereas FIPs concerning data quality, data security, and transparency should apply to both identified and identifiable data).

261. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 71 ("Thus, the federal privacy statutes form a complicated patchwork of regulation with significant gaps and omissions."); *see also* Birnhack & Elkin-Koren, *supra* note 108, at 349 (describing the focus of U.S. privacy laws in contrast to EU systems).

262. 15 U.S.C. § 168b (2006).

263. 20 U.S.C. § 1232g (2006).

264. *See* Schwartz & Solove, *supra* note 3, at 1821 (explaining the history of congressional action on privacy laws). FCRA applies to consumer reporting agencies that furnish consumer reports about the creditworthiness or personal characteristics of a consumer, and limits the circumstances and purposes under which consumer reports may be provided to other parties. *See id.* (explaining the scope of FCRA). The focus of FERPA is student privacy, and it is the first federal statute that uses the term "personally identifiable information." *See id.* at 1822–23 (explaining the historical context of FERPA).

include the Children's Online Privacy Protection Act (COPPA),[265] the Health Information Portability and Accessibility Act (HIPAA),[266] the Electronic Communications Privacy Act (ECPA),[267] and the Gramm–Leach–Bliley Act (GLBA).[268] Several federal statutes focus on the presence of personally identifiable information (PII),[269] while others focus on transparency and access to information,[270] on protecting consumers from inappropriate use of their personal data,[271] or on imposing duties of confidentiality.[272] Federal statutes often include requirements for administrative agencies to promulgate regulations. HIPAA requires HHS to enact regulations to support the Act.[273] Under

---

265. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2006) (preventing websites from, among other acts, collecting data from children using the Internet without giving notice of the type of data that will be collected, obtaining parental consent, and providing parents with an opportunity to refuse websites' requests to collect data).

266. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of 29 U.S.C., 42 U.S.C.) (providing the laws governing the privacy and security of health data, including guidelines for the collection of data related to electronic healthcare transactions).

267. *See* Electronic Commc'n Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510–2522, 2701–2712 (2006)) (protecting wire, oral, and electronic communications while in transit, extending restrictions on government use of wire taps to computer-based communications, and preventing the government from accessing data on electronic storage devices under some circumstances).

268. *See* 15 U.S.C. §§ 6801–6809 (2006) (protecting financial data).

269. *See* Schwartz & Solove, *supra* note 3, at 1827 (explaining the differing focuses of electronic privacy legislation). Statutes concerned with PII include the Cable Communications Policy Act, the Video Privacy Protection Act, and the Gramm–Leach–Bliley Act. *See id.* at 1824, 1829, 1830 (detailing the characteristics of CCPA, VPPA, and GLBA).

270. *See* Solove, *Taxonomy, supra* note 111, at 525 (listing the Privacy Act, CCPA, FCRA, and COPPA as examples).

271. *See* Richards, *supra* note 114, at 1167 (listing statutes that protect consumers' PII from inappropriate uses); *see also* Kuner, *Part 1*, *supra* note 119, at 176 ("Data protection law gives rights to individuals in how data identifying them or pertaining to them are processed, and subjects such processing to a defined set of safeguards.").

272. *See* Richards, *supra* note 114, at 1196 (listing statutes that impose confidentiality on handlers of PII).

273. *See, e.g.*, Martin, *supra* note 44, at 297 (providing an example of a regulation promulgated under and supporting HIPAA (citation omitted)).

the GLBA, agencies regulating financial institutions are required to promulgate rules setting requirements for safeguarding customers' personal information.[274]

States also adopt their own privacy laws to protect consumers. For example, there is a statute in Massachusetts that requires detailed data security procedures,[275] and forty-five states have statutes requiring customer notification in the event of a security breach.[276] Minnesota has a merchant liability statute, under which a merchant can be held liable if there was a security breach and customer credit card information was insufficiently protected.[277] California's Song–Beverly Act[278] protects PII by prohibiting merchants from requiring customers to give personal information like their address and phone number "as a condition to accepting the [customer's] credit card."[279]

There are several federal statutes aimed at protecting children as a vulnerable population, including COPPA, FERPA, and the Protection of Pupil Rights Amendment.[280] COPPA

---

274. *See* Solove, *Architecture, supra* note 172, at 1274 (explaining the GLBA).

275. *See* Denny, *supra* note 46, at 240 (explaining a Massachusetts Internet privacy law); *see also* Rhodes & Kunis, *supra* note 23, at 50–51 (describing the Massachusetts law as being controversial because of the high bar that it sets as a minimum threshold for security).

276. *See* Rhodes & Kunis, *supra* note 23, at 49–50 (explaining that most states have followed California's passage of laws requiring businesses to notify customers in the event of a security breach); Schwartz & Solove, *supra* note 3, at 1884–85 (noting that forty-four states have enacted laws requiring that businesses notify customers when they experience a security breach).

277. *See* Rhodes & Kunis, *supra* note 23, at 50 (noting the existence of a Minnesota law imposing liability for negligent handling of consumer financial data).

278. Song–Beverly Credit Card Act of 1971, CAL. CIV. CODE § 1747.08 (2009).

279. Schwartz & Solove, *supra* note 3, at 1831. The California Supreme Court also held that asking for a zip code would be sufficient to violate the Song–Beverly Act if the zip code was being requested as a condition of accepting a credit card. *See* Pineda v. Williams-Sonoma Stores, Inc., 246 P.3d 612 (Cal. 2011) ("In light of the [Song–Beverly Act]'s plain language, protective purpose, and legislative history, we conclude a ZIP code constitutes 'personal identification information' as that phrase is used in section 1747.08. Thus, requesting and recording a cardholder's ZIP code, without more, violates the Credit Card Act."); *see also* Schwartz & Solove, *supra* note 3, at 1834 (explaining the outcome of *Williams-Sonoma Stores*).

280. *See* Cascia, *supra* note 17, at 891 (identifying federal laws that protect

imposes limitations on the types of information that a website may collect from children younger than thirteen, and privacy policies must address the website's information collection practices with regard to children.[281] COPPA explicitly spells out what elements are required for notice to be valid.[282] There are also state laws aimed at protecting children's online privacy, like a law in Maine that requires parental consent before someone collects, transfers, or sells a minor's personal or health-related information for product promotion purposes.[283]

Some privacy-related laws do not focus on consumer protection, but on procedural elements of government investigations. The Privacy Act of 1974[284] regulates how federal agencies can collect and use personal records,[285] the USA PATRIOT Act of 2001[286] grants a right to the U.S. government to demand data in the interest of protecting homeland security,[287] and the ECPA sets out conditions under which the government can obtain a variety of electronic communications.[288] Beyond statutes, the Fourth Amendment protects against unreasonable

---

student privacy).

281. *See id.* at 892 (discussing COPPA). COPPA is why the terms of service or privacy policies in our sample typically contained language about not collecting data from or marketing to children under thirteen. FTC, *Frequently Asked Questions about the Children's Online Privacy Protection Rule*, http://www.ftc.gov/privacy/coppafaqs.shtm (last visited Feb. 3, 2013) (answering common questions from website providers about how to keep within COPPA regulations) (on file with the Washington and Lee Law Review).

282. *See* Schwartz, *State*, *supra* note 175, at 855 (describing ways that COPPA changed the previous practices of using data collected from children).

283. *See* Cascia, *supra* note 17, at 899 (discussing laws that states have enacted to support COPPA).

284. 5 U.S.C. § 522a (2006).

285. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 68 (describing the Privacy Act of 1974). The Driver's Privacy Protection Act of 1994 is similar and prohibits states from selling personal information from motor vehicle records to marketers. *See id.* at 69 (describing the Driver's Privacy Protection Act of 1994).

286. Pub. L. No. 107-56, 115 Stat. 272, 367–68 (codified as amended in scattered sections of U.S.C. (2006)).

287. *See* 20 U.S.C. § 1232g(j)(1) (2006); Lanois, *supra* note 18, at 45 (stating that the USA Patriot Act is a "hurdle to the international adoption of cloud computing" and explaining the Act's expansion of federal power to collect data).

288. *See, e.g.*, 18 U.S.C. § 2703 (setting out procedures for compelling providers to disclose information).

searches and seizures.[289] However, Fourth Amendment protection is also likely to be weaker in the cloud than it would be if the same information were stored solely on a personal computer in the suspect's home.[290]

a. Electronic Communications Privacy Act

The ECPA was passed partly in response to the findings of the Office of Technology Assessment that the protections of e-mails were "weak, ambiguous, or nonexistent."[291] The ECPA and a major update to the Computer Fraud and Abuse Act (CFAA) were both passed in 1986, though in subsequent decades, the criminal provisions of the CFAA have been expanded much more than the electronic privacy protection provisions of the ECPA.[292]

The ECPA consists of three federal statutes: the Stored Communications Act (SCA),[293] the Pen Register statute,[294] and the Wiretap Act.[295] Its protections supplement those of the Fourth

---

289. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .").

290. *See* Soghoian, *supra* note 5, at 386–87 (noting that law enforcement agencies have "essentially deputized" technology companies to monitor end-users' use of their applications operating on the cloud).

291. Kattan, *supra* note 8, at 627–28.

292. *See* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 912 (2003) (noting that the CFAA was amended eight times between 1986 and 2003); *see also* Martin, *supra* note 44, at 308 (listing provisions of the Act that criminalize Internet-based conduct); Robison, *supra* note 4, at 1196 (describing the ECPA and one component thereof called the Stored Communications Act (SCA)).

293. 18 U.S.C. §§ 2701–10 (2006).

294. *Id.* §§ 3121–27.

295. *See id.* §§ 2510–22; *see also* Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 167 (2011) (identifying the three parts of the statute and highlighting court decisions that have interpreted the statute); Casey Perry, U.S. v. Warshak*: Will Fourth Amendment Protection Be Delivered to Your Inbox?*, 12 N.C.J.L. & TECH. 345, 349 (2011) (identifying the three parts of the statute and explaining the contents of the SCA). A "pen register" is a device that records phone numbers dialed, though the language of the statute also applies to other technological means. *See "Pen Registers" and "Trap and Trace Devices,"* ELEC. FRONTIER FOUND. SURVEILLANCE SELF-DEFENSE

Amendment.[296] The application of each depends on what type of information is sought and where it is in the transmission process.[297] The Wiretap Act covers interception of wire, oral, and electronic communications.[298] Under the Wiretap Act, obtaining e-mail contents in real time requires a Title III order to be issued with Department of Justice (DOJ) approval and a grant by a federal judge, and the order must be renewed every thirty days.[299] Under the Pen Register statute, obtaining real time subscriber data requires an ex parte pen register order.[300] Stored electronic information and the requirements for obtaining each type are addressed under the SCA,[301] which we analyze in more detail in the section below.

PROJECT, https://ssd.eff.org/wire/govt/pen-registers (last visited Feb. 3, 2013) (defining pen registers and trap and trace devices and explaining how they are used) (on file with the Washington and Lee Law Review).

296. *See* Bagley, *supra* note 295, at 167 (explaining the ECPA's expansion of the Fourth Amendment's general requirement of warranted searches); *see also* Perry, *supra* note 295, at 349 (noting that the ECPA supplements the Fourth Amendment). Congress had two main purposes when it adopted the SCA as part of the ECPA: to address privacy concerns that might hinder technological development, and to apply Fourth Amendment privacy principles to computer networks. Robison, *supra* note 4, at 1224 (identifying the two primary purposes behind the SCA). The legislative history of the SCA indicates that Congress acknowledged that e-mail and computer networks were analogous to first class mail. *See id.* at 1106, 1225 (explaining the legislative history of the Act and noting that Congress analogized e-mail to traditional postal mail).

297. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1231 (2004) (defining the legal difference between stored communications and communications in transit). The Wiretap Act's requirement for a search warrant is stronger than the requirements under the SCA, so law enforcement personnel arguably have incentives to use the SCA's retrospective authority instead of complying with the Wiretap Act for prospective surveillance. *See id.* at 1232 (explaining a possible weakness in the SCA's privacy framework and court action on the issue).

298. *See* Soghoian, *supra* note 5, at 411 (explaining the coverage of the Wiretap Act).

299. *See* 18 U.S.C. § 2518 (2006) (mandating procedures for the interception of electronic communications with a pen register); Bagley, *supra* note 295, at 179 (explaining the procedures provided by the pen register statute).

300. *See* 18 U.S.C. § 3123 (setting out procedures for obtaining pen register or trap and trace device orders); Bagley, *supra* note 295, at 179 (explaining the procedures provided by the pen register statute).

301. *See* Bagley, *supra* note 295, at 179 (explaining the procedures provided

(1) Stored Communications Act

The status of the SCA is problematic because much of the language is very unclear or outdated and interpretations of the statute by courts have varied significantly.[302] The two most important sections for our purposes are: (1) § 2702, which addresses the circumstances under which a provider can voluntarily disclose customer information to others;[303] and (2) § 2703, which addresses how the government can compel a provider to produce stored information.[304] This sounds simple enough, but there are so many exceptions, subcategories, and additional requirements that the statute quickly becomes unwieldy. For example, one commonly referenced exception to the prohibition on disclosure allows for disclosure when the subscriber or customer (depending on the type of service) consents to disclosure,[305] but the question then arises as to what actions can amount to consent. For example, is it consent under

---

by the SCA).

302. *See* Kerr, *supra* note 297, at 1208 (calling the statute "dense and confusing" as well as "outdated"); Perry, *supra* note 295, at 361 n.82 (noting that although most believe that the SCA deals with retrospective surveillance only, the court in *Warshak* stated that the language of the statute on its face does not compel this reading (citing United States v. Warshak, 631 F.3d 266, 290 (6th Cir. 2010))); *see also* Soma, Gates, & Smith, *supra* note 16, at 526–27 (suggesting that incremental changes to the ECPA could help address these issues).

303. *See* 18 U.S.C. § 2702 (establishing prohibitions on the disclosure of customer data and establishing exceptions to these prohibitions).

304. *See id.* § 2703 (outlining cases in which the government can require disclosure of customer communications or records); *see also* Perry, *supra* note 295, at 350–51 (explaining the effect of §§ 2702 and 2703 of the SCA).

305. *See* 18 U.S.C. § 2702(b)(3) (2006) (providing the consent exception). While one might assume that the originator and subscriber would be the same person, this is not always so, such as in the 9th Circuit case of *Quon v. Arch Wireless*, in which the issue was whether the employer-subscriber's consent for Arch Wireless to disclose the contents of text messages was valid, or if the messaging service was an ECS, and thus the originator or recipient (in this case, the employee Quon) would have to consent for the disclosure to be valid under this exception. Quon v. Arch Wireless, 529 F.3d 892, 900 (9th Cir. 2008) (ruling that summary judgment for Arch Wireless on employee-plaintiffs' claim of nonconsent was improper because a genuine dispute of material fact existed as to whether Arch was a "remote computing service" as opposed to an "electronic communication service" under SCA Sections 2701–2711).

the SCA to accept the terms of a very broad privacy policy without reading these terms? Another exception in § 2702 that raises new questions in the cloud computing context is the exception for disclosure to persons who provide the service.[306] The definition of remote computing service in the Wiretap Act supplements this exception, permitting service providers to monitor activities on their networks in real time.[307] This exception allows private employers to internally share information about the online activities of employees when the employer provides these services in-house,[308] but will employers lose the right to monitor their employees' online activities if they outsource IT to a cloud service provider? There is also some possible overlap between compelled and voluntary disclosures, such as when the government merely tells the provider about an ongoing investigation, and then the provider gives the government relevant information without a formal request being made for the information.[309] In such circumstances, which set of exceptions or requirements should apply?

To determine the propriety of a disclosure under the SCA, the government must first determine whether the sought information is stored as part of an electronic communications

---

306. *See* 18 U.S.C. § 2702(b)(4) (providing the service provider exception).

307. *See id.* § 2711(2) (defining RCS and excluding from limitations on interception devices such as those "being used by a provider of wire or electronic communication service in the ordinary course of its business"); Kerr, *supra* note 297, at 1226–27 (explaining the advantages of a narrow definition of RCS for nonpublic service providers that want to monitor their networks); *see also* Soma, Gates, & Smith, *supra* note 16, at 516 (noting problems with the ECS/RCS dichotomy when applied to service providers that outsource their communications services).

308. *See* Soma, Gates, & Smith, *supra* note 16, at 516, 521 ("The key to legal [e-messaging] monitoring by closed community service providers, such as employers, is providing notice and [obtaining] consent." (internal quotations and citation omitted)).

309. *See* Kerr, *supra* note 297, at 1224–25 (calling this overlap a "gray zone"). Kerr offers up these examples: If an ISP finds files and contacts law enforcement pursuant to one of the exceptions in § 2702, but the ISP requests a subpoena before turning over the files so that it has a paper trail, is that voluntary or compelled? On the other hand, if the police contact an ISP and ask the ISP if they would like to help in the investigation of a child molester, and the ISP says yes and turns over its files, is that voluntary or compelled? *See id.* (providing examples of the gray zone).

service (ECS) or a remote computing service (RCS). An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[310] while an RCS is defined as a "provision to the public of computer storage or processing services by means of an electronic communications system."[311] In the provisions prohibiting voluntary disclosure, ECS providers are prohibited from knowingly disclosing communication contents that the provider holds in "electronic storage,"[312] and RCS providers are prohibited from knowingly disclosing communication contents that the provider maintains for the sole purpose of providing the subscriber or customer with "storage or computer processing services."[313] Some cases have thus turned on a party's ability to establish the difference between when communications are in "electronic storage" and when communications are just in "storage."[314]

The process required to obtain information also varies with the type of information sought, with notice required prior to the disclosure of some information types, some of which require a warrant, while others require a special court order under § 2703(d), and still others require only a subpoena.[315] These three

---

310. 18 U.S.C. § 2510(15).

311. *Id.* § 2711(2).

312. *Id.* § 2510(17) (defining "Electronic storage" as: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication"). Intermediate storage is thus covered by the ECS rules, while long-term storage is covered by the RCS rules. Kerr, *supra* note 297, at 1216 (noting that intermediate storage is covered under the ECS rules and long-term storage is covered by the RCS rules).

313. *See* 18 U.S.C. § 2702(a) (2006) (mandating restrictions on providers of RCS). Insofar as RCS providers are prohibited from disclosing contents held for "storage or computer processing" purposes, these protections go away if the provider is authorized to access the communication contents for any purpose other than "storage or computer processing." *See id.* § 2702(a)(2)(B) (delineating the scope and context of the prohibition).

314. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004) (reversing dismissal of plaintiff's claim that an Internet service provider disclosed e-mails in violation of the SCA on the grounds that the e-mail messages were in "electronic storage" and therefore afforded SCA protections); *see also* Kerr, *supra* note 297, at 1229 (discussing the *Theofel* case).

315. *See* 18 U.S.C. § 2703 (requiring, for example, a warrant for disclosure of

methods of compelling information are listed in descending order of the strength of the showing required to obtain them. To obtain a § 2703(d) court order, the governmental entity must show "specific and articulable facts" establishing "reasonable grounds" to believe that the information sought is "relevant and material to an ongoing criminal investigation."[316] This standard is less than the "probable cause" standard for obtaining a warrant, but greater than the "reasonable relevance" standard for obtaining a subpoena.[317] The type of information sought also determines whether a § 2703(d) order or subpoena must be accompanied by prior notice to the target.[318] For example, the statute explicitly states that only a subpoena, and no prior notice to the customer, is required to compel an ECS or RCS provider to disclose noncontent, basic subscriber information, including the customer's name, address, phone records (including session times and durations), length and type of service, phone number, and how the customer pays for the service.[319] Most of this same noncontent subscriber information, it should be noted, can be freely disclosed

---

contents of electronic communications in storage or a subpoena with prior notice from the governmental entity seeking disclosure, a court order for disclosure of electronic communications in an RCS, and a subpoena for disclosure of records concerning an ECS or RCS).

316. *Id.* § 2703(d).

317. *See* U.S. CONST. amend. IV; Kattan, *supra* note 8, at 631 (discussing the reasonable relevance standard); Kerr, *supra* note 297, at 1218–19 (discussing the specific and articulable facts requirement).

318. *See* Kattan, *supra* note 8, at 629–30 (noting that different requirements pursuant to a demand for disclosure exist depending on the way information is stored). The SCA also permits notice to be delayed in certain circumstances. *See* 18 U.S.C. § 2705(a)(2) (allowing the delay of notice when prompt notice would "[endanger] the life or physical safety of an individual; [risk] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or otherwise seriously [jeopardize] an investigation or unduly [delay] a trial").

319. *See* 18 U.S.C. § 2703(c) (2006) (detailing instances when the government has the power to require a provider of ECS or RCS to disclose records related to a subscriber or customer of its services); Kerr, *supra* note 297, at 1219 (explaining the disclosure rules that cover records). Information about how a customer pays for the service can include disclosure of the customer's credit card or bank account numbers. *See* 18 U.S.C. § 2703(c) (allowing a government entity to compel disclosure of credit card information).

to nongovernmental entities pursuant to an explicit exception in the voluntary disclosure provisions.[320]

Considering the many avenues for uncertainty within the SCA, it should come as no surprise that disclosures under the SCA are often a source of contention. A disclosure in violation of the SCA may give rise to a civil cause of action.[321] However, good faith reliance on a seemingly lawful document compelling disclosure acts as a complete defense to a civil action against a provider who is compelled to disclose communications.[322]

(2) Applying the SCA to the Cloud

Orin Kerr has written a very detailed and well-received article analyzing and explaining the SCA.[323] The SCA is a complex statute that Congress wrote based on how early computer networks operated.[324] The category of RCS provider was intended to address the business model in which companies

---

320. *See* 18 U.S.C. § 2702(c) (permitting disclosure to the National Center for Missing and Exploited Children). The SCA thus leaves a hole for the disclosure to private parties of personally identifiable information, so the privacy policies of these providers would thus be more applicable to the protection of PII than the SCA. Because there is no explicit exception for subpoenas in civil litigation, courts interpret this omission as meaning that private litigants cannot obtain data other than noncontent information from ECS and RCS providers. *See* Robison, *supra* note 4, at 1208–09 (citing a number of cases that have so decided). However, because of the importance of civil discovery, courts may promote alternative methods of obtaining information held by an ECS or RCS provider, such as a Rule 34 motion to compel the party to produce data held by these providers. *See, e.g.*, Flagg v. City of Detroit, 252 F.R.D. 346, 349–55 (E.D. Mich. 2008) (concluding that the SCA does not preclude civil discovery for electronic stored communications that are maintained by a nonparty service provider because the other party has control over that information and thus can be compelled to produce it under Rule 34).

321. *See* 18 U.S.C. § 2707(a) (creating a private cause of action for knowing or intentional violations of the law).

322. *See id.* § 2707(e)(1) (extending the good faith exception to "a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization").

323. *See* Kerr, *supra* note 297, at 1213–33 (analyzing and explaining the SCA).

324. *See* Robison, *supra* note 4, at 1205 (explaining the legislative history of the SCA).

outsourced a lot of storage and processing functions due to the high cost of doing this in-house.[325] It is thus likely that the RCS category would easily apply to commercial cloud services that provide options for outsourcing IT, but in most other contexts, there is substantial overlap between RCS and ECS. In part because of the rigid language of the statute and the substantial changes that have come about in the electronic communications field, it is unclear how the privacy protections of the SCA apply to other communications in the cloud.[326] Kerr suggests eliminating the categories of ECS and RCS to address some of the confusion.[327]

Currently, the degree of privacy in an e-mail likely depends on whether it is stored on a hard drive or in the cloud.[328] E-mails downloaded from a service provider are easily covered by the requirement in the SCA that requires a warrant to obtain unopened e-mails fewer than 180 days old, but it is unclear whether a webmail provider would be considered an "electronic communication service" or a "remote computing service."[329] Some industry actors seem to oppose the 180-day rule because people now leave information on webmail services for long periods of time.[330] Generally, many support the proposal to revise the SCA to better address cloud computing.[331]

Some question whether the SCA would protect free cloud services at all because advertising-supported business models

---

325. *See id.* at 1206–07 (explaining the legislative history of the SCA).

326. *See* Kattan, *supra* note 8, at 619 (recognizing the uncertainty of the SCA's protections of cloud-based electronic communications).

327. Kerr, *supra* note 297, at 1209 (calling the categories "confusing" and suggesting their removal); *see also* Kattan, *supra* note 8, at 653 (echoing this recommendation and suggesting that Congress consider whether it even makes sense to continue to distinguish between ECS and RCS).

328. *See* Lanois, *supra* note 18, at 45 (discussing cloud privacy issues).

329. *See* Bagley, *supra* note 295, at 167–68 (noting the SCA's ambiguous relationship to webmail services).

330. *See* Kattan, *supra* note 8, at 642–43 (noting Microsoft's objections to the 180-day rule).

331. *See id.* at 645 (noting that Digital Due Process, a consortium of privacy advocates, are lobbying for amendment of the ECPA); *see also supra* Part II.E (discussing the need for legislative reform to create adequate privacy protections for the cloud).

often give the providers access to communication contents for targeted advertising purposes.[332] This may prevent these services from being considered RCS providers because the provider is authorized to access communication contents for purposes other than rendering storage and computer processing services.[333] TOS agreements and privacy policies thus have potentially significant effects on the extent to which the SCA protects the customer's privacy because these terms may give the provider explicit authority to take actions that would disqualify the provider from being considered a provider of RCS.[334]

3. Case Law

While there is not an explicit clause in the U.S. Constitution that states the existence of a general right to privacy, courts have held that such a right exists and is protected by the Constitution. Much discussion of Supreme Court privacy jurisprudence focuses on decisional privacy; that is, the right of individuals to make decisions free of government intervention.[335] In *Whalen v. Roe*, the Supreme Court recognized "the individual interest in avoiding disclosure of personal matters,"[336] which has influenced many lower courts in recognizing a constitutional right to information privacy.[337]

---

332. *See* Kattan, *supra* note 8, at 638–40 (arguing that Gmail might not be considered an RCS provider because the privacy policy allows Google to access user communications for advertising purposes); Robison, *supra* note 4, at 1196 (noting that this quid pro quo violates the SCA's provisions).

333. *See* Robison, *supra* note 4, at 1213 (noting that cloud services may not qualify as RCS because these services allow advertisers access to customer data).

334. *See id.* at 1215, 1220–21 (identifying three varieties of terms-of-service agreements and explaining how courts have interpreted terms-of-service agreements).

335. Some of the best known examples of decisional privacy cases in the Supreme Court over the last fifty years concern contraception and abortion. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 153 (1973) (citing a right to privacy under the Constitution in prohibiting states from outright banning abortion); Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (ruling unconstitutional a Connecticut law that prohibited the use of contraception).

336. Whalen v. Roe, 429 U.S. 589, 600 (1977).

337. *See* Solove, *Taxonomy, supra* note 111, at 558 (discussing the privacy

U.S. courts have often examined the distinctions between the public and private spheres. The public-disclosure-of-private-facts tort, for example, has been found to not apply to the republication of public postings on the web, even when the original posting is deleted a few days after it was first posted.[338] In contrast to public postings, courts may be more protective of seemingly nonsensitive private data, like search queries.[339]

Courts have also examined privacy in the context of the Fourth Amendment and statutes that relate to privacy, like the ECPA. Also relevant to our research, some courts have examined the implications of TOS agreements and privacy policies. It is to these topics we now turn.

a. Fourth Amendment

The Fourth Amendment declares that people have a right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[340] The Fourth Amendment also applies to seizure of digital evidence, though seizing digital evidence stored in the cloud is likely to be much easier than seizing identical data that is stored solely on a suspect's personal computer within the suspect's home.[341]

---

doctrine's effect in lower federal courts).

338. *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Cal. Ct. App. 2009) (concluding that initial publication was not sufficiently obscure or transient). The *Moreno* court concluded this in spite of the fact that the public backlash did not rise to unacceptable levels until after the college student's MySpace posting about the town was republished in the local newspaper. *See id.* at 861–62.

339. *See, e.g.*, Gonzales v. Google, 234 F.R.D. 674, 687–88 (N.D. Cal. 2006) (declining to compel disclosure of 5,000 search queries and noting the potential privacy concerns of such disclosures).

340. U.S. CONST. amend. IV. Typically, this protection requires a search warrant to be issued, though in some circumstances it is acceptable for the warrant to be executed by parties other than law enforcement. *See* United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) (permitting an ISP's technicians to execute a search warrant outside the presence of law enforcement).

341. *See* Soghoian, *supra* note 5, at 386–87 (noting that digital search and seizure is far easier because of the development of the cloud).

Fourth Amendment cases often focus on the need for a warrant, the issuance of which requires a finding of probable cause by a judicial officer.[342] When searches are executed without a warrant, Fourth Amendment jurisprudence requires courts to decide if the target of the search had a subjective expectation of privacy that society recognized as reasonable.[343] Much turns on the existence of this "reasonable expectation of privacy" (REOP). Courts recognize a REOP in papers and effects sent in the mail, and some courts have held that e-mail is analogous to postal mail and thus a sender has a REOP in e-mail.[344] A REOP might not exist, for instance, in a library's shared computers that are available for public use, but may exist in a personal Yahoo! webmail account.[345] A REOP is generally recognized in locked containers, and password protected computers may be considered analogous to locked containers.[346] On the other hand, a public employee may have a reduced REOP in equipment provided by

342. *See* United States v. Leon, 468 U.S. 897, 923 (1984) (ruling that a warrant is deficient for failure to show probable cause if the facts articulated on the face of the warrant are "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"); *supra* note 340 and accompanying text (discussing the Fourth Amendment).

343. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (espousing the reasonable expectation of privacy doctrine).

344. *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (extending Fourth Amendment protections to e-mail). *But see* Rehberg v. Paulk, 611 F.3d 828, 847 (11th Cir. 2010) (ruling in favor of immunity because there is not a "clearly established" constitutional right to privacy in e-mail content "voluntarily transmitted over the global Internet and stored at a third-party ISP").

345. *See* Wilson v. Moreau, 442 F. Supp. 2d 81, 104, 108 (D.R.I. 2006) (citing cases that declared a lack of reasonable expectation of privacy when using public library computers); *see also* United States v. D'Andrea, 648 F.3d 1, 5–14 (1st Cir. 2011) (analyzing a government search of a password protected website used to store private images). On the other hand, courts might not find a REOP in information disclosed in a chatroom with other individuals. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997).

346. *See* United States v. Lifshitz, 369 F.3d 173, 193 (2d Cir. 2004) (ruling that a probation condition allowing for frequent or random monitoring of probationer's computer use may be overbroad and violate a Fourth Amendment interest); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (concluding that a third party's authority to consent to search of shared spaces did not extend to the defendant's password protected files).

his employer.[347] On this point, the Supreme Court recently examined the issue of a public employer-issued pager and the extent to which the Fourth Amendment protected text messages sent over this pager, concluding that a search that is justified by noninvestigatory work-related purposes is reasonable.[348] In *City of Ontario v. Quon*,[349] the Court assumed, but did not conclusively determine, that there was otherwise a REOP in text messages.[350]

If a warrantless search is conducted where a REOP exists, a court will examine if one of the exceptions to the warrant requirement applies, and if one does not, the evidence derived from the violation may be suppressed at trial. One of the exceptions is when the party with a REOP is the object of the search, or a third party with adequate authority, gives consent to the search.[351] The scope of the permission is also important. Suppression may be an option when investigators seize more than permitted under the warrant, which is an especially big danger with e-discovery.[352] However, suppression might not be an available remedy in the case of evidence that was within the

---

347. *Compare* United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (noting that a public employer's computer use policy may reduce an employee's REOP in the employee's office computer), *with* Maes v. Folberg, 504 F. Supp. 2d 339, 347 (N.D. Ill. 2007) (finding a REOP in a public employee's work laptop computer).

348. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2632–33 (2010) (holding that the city's review of a police officer's text messages did not violate the officer's Fourth Amendment rights).

349. *See id.* at 2619.

350. *See id.* at 2630 ("Even if Quon had a reasonable expectation of privacy in his text messages, petitioners did not necessarily violate the Fourth Amendment by obtaining and viewing the transcripts.").

351. *Compare* United States v. Andrus, 483 F.3d 711, 721 (10th Cir. 2007) (holding that a cotenant had apparent authority to consent to a search of the computer in defendant's room when police used forensic software to bypass possible password protection), *with Trulock*, 275 F.3d at 402–03 (holding that third-party consent does not extend to the defendant's password protected files).

352. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177 (9th Cir. 2010) (emphasizing the importance of procedures to segregate data covered by the warrant from data that is not covered, including the need to have disinterested computer technicians go through the information to separate covered data).

scope of the warrant, even if the seizure of evidence was outside the warrant.[353]

There is also an important distinction between "content" and "noncontent" information, with the latter category including things like addresses on the outside of an envelope and phone numbers dialed on a phone. In the cloud context, a person is likely to not have a REOP in subscriber information provided to an ISP.[354] Other noncontent information, like e-mail addresses in the "To" field of an e-mail or IP addresses of visited websites, are likely to not be protected by the Fourth Amendment.[355]

The third-party doctrine of Fourth Amendment jurisprudence is the focus of much discussion in the online privacy context, because the doctrine prevents a REOP from being found in papers and effects turned over to a third party.[356]

---

353. *See* United States v. Hill, 459 F.3d 966, 973–76 (9th Cir. 2006) (declining to suppress evidence found on storage media seized pursuant to a warrant that only addressed the seizure of a computer). If digital evidence within the scope of the warrant has been deleted by the computer owner, it is not outside of the warrant's scope for police to restore deleted files when executing the warrant. *See* United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) ("The seizure of unlawful images is within the plain language of the warrant; their recovery, after attempted destruction, is no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note.").

354. *See* United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (finding that the defendant had no REOP for subscriber information given to ISP).

355. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (holding that it is not a Fourth Amendment search to use computer surveillance techniques to obtain only information concerning the to/from fields of e-mails and website addresses visited); Viacom Int'l, Inc. v. Youtube, Inc., 253 F.R.D. 256, 261–62 (S.D.N.Y. 2008) (stating that privacy concerns of disclosing noncontent information like data logs and IP addresses were only "speculative"). The *Perrine* court also suggested that the defendant's use of peer-to-peer software also decreased the defendant's expectation of privacy, especially as to the files shared over the P2P service. *See Perrine*, 518 F.3d at 1205 (ruling that Perrine's use of peer-to-peer software, which allowed other Internet users to access files on his computer, partially reduced the expectation of privacy that he would otherwise enjoy in his computer, therefore leaving Perrine with no Fourth Amendment interest in subscriber information he gave to Yahoo! and Cox).

356. *See* United States v. Miller, 425 U.S. 435, 436–40 (1976) (finding no reasonable expectation of privacy in financial records disclosed to a financial institution in the ordinary course of business); Couch v. United States, 409 U.S. 322, 335–36 (1973) (finding no reasonable expectation of privacy in financial

Bailments of concealed items, however, might not be limited by the third-party doctrine because the bailee entrusted with concealed items does not necessarily have the authority to view the items or to consent to the search of the items by others.[357] Thus, much will turn on the authority that the third party has with respect to the entrusted items. If a private carrier's terms retain the right to inspect a package for any reason, acceptance of these terms by a customer of the private carrier may also result in a loss of a REOP in packages sent using this private carrier.[358]

Information privacy scholars often argue that this third-party doctrine will prevent Fourth Amendment protections from applying in the cloud because users must inherently reveal their information to third parties in order for it to be transmitted or processed.[359] On the other hand, recent case law casts doubts on this view. In the Sixth Circuit case *United States v. Warshak*,[360] the court distinguished e-mail interception from other third-party doctrine cases by holding that the e-mail provider was an intermediary in the communication, not a recipient.[361] However, the *Warshak* court also noted that if an agreement with a service provider gave the service provider the authority to "audit, inspect, and monitor" the e-mails of its subscribers, that might cause the subscriber to lose a REOP in those e-mails.

---

records turned over to an accountant for tax return purposes).

357. *See* United States v. James, 353 F.3d 606, 613–15 (8th Cir. 2003) (overturning a child pornography conviction because the police obtained the evidence from a person entrusted with computer disks with specific instructions to not use the disks).

358. *See* United States v. Young, 350 F.3d 1302, 1307–09 (11th Cir. 2003) (finding no REOP when a private carrier retained the right to inspect packages for any reason and when defendant also violated other terms set out by the carrier). The court in *Young* also held in the alternative that reserving a right to inspect gave the carrier the ability to later consent to a search of the package by law enforcement. *See id.* at 1308 ("Just as the 'right to inspect' notice defeated Young's privacy interest, we believe it also served to defeat Young's Fourth Amendment challenge because it authorized Federal Express, as a bailee of the packages, to consent to a search.").

359. *See, e.g.*, Bagley, *supra* note 295, at 173–74 (arguing that Fourth Amendment protections should be extended to data that is revealed involuntarily and incidentally to using a service).

360. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

361. *See id.* at 288 (distinguishing *Miller*).

For Fourth Amendment protection to apply to a search, it must be executed by a state actor because the Fourth Amendment only protects against intrusions by the state.[362] Searches conducted by a private party thus do not inherently raise Fourth Amendment concerns unless the private party is behaving as a state actor,[363] an analysis that often turns on state entanglement with the private party's business.[364] Under the Supreme Court's holding in *United States v. Jacobsen*,[365] if the papers or effects are secured such that it is clear that the nonstate-actor searcher does not have a right to look at the contents, but the searcher executes a private search anyway, a REOP might not protect the owner of the contents if law enforcement then duplicates the private search.[366] The *United States v. D'Andrea*[367] case suggests a narrow interpretation of *Jacobsen*, however, with the former court implying that a private search of password protected online storage would not validate a subsequent warrantless search unless the content owner was careless with his password security.[368]

---

362. *See* U.S. CONST. amend. 4 (providing protections against unreasonable and warrantless searches); United States v. Jacobsen, 466 U.S. 109, 113 (1984) (stating that the Fourth Amendment is construed as "proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official'" (citation omitted)).

363. *See* United States v. Richardson, 607 F.3d 357, 365–66 (4th Cir. 2010) (holding that an ISP was not turned into a state actor by a statute that required ISPs to report to law enforcement if the ISP found child pornography on its network).

364. *See* Burton v. Wilmington Parking Auth., 365 U.S. 715, 716–17 (1961) (finding state action sufficient to implicate the Equal Protection Clause of the Fourteenth Amendment when a restaurant in a city-operated parking garage denied service to a customer because of his race).

365. *See Jacobsen*, 466 U.S. at 109.

366. *See id.* at 126 (holding that if a third party violates the person's expectation of privacy, the government may use that information to the same extent, but cannot exceed the scope of the private search). *But see* United States v. D'Andrea, 648 F.3d 1, 8 (1st Cir. 2011) (ruling that the private search doctrine would not apply when the property owner did not give the private searcher permission or means to search the property, unless the property owner was very careless about security of the property).

367. *See D'Andrea*, 648 F.3d at 1.

368. *See id.* at 8 (noting that the private search doctrine might apply if the

b. Stored Communications Act

As discussed above, the ECPA includes the Wiretap Act, the SCA, and the Pen Register statute.[369] The SCA is a complicated statute that courts often interpret differently. The Ninth Circuit, for example, adopted a broad interpretation of the phrase "for backup purposes" within the definition of "electronic storage." The *Theofel v. Farey Jones*[370] court held that a provider was holding e-mails in "electronic storage," and thus the ECS terms applied rather than the RCS terms that would apply if the e-mails were merely in "storage."[371] Kerr criticizes the Ninth Circuit's interpretation of "electronic storage" under the SCA,[372] specifically its broad interpretation of "backup purposes" that may permit more frequent findings that a service is acting as an ECS provider.[373]

It is unclear how the SCA will apply to webmail. The *Theofel* court itself suggested that storage would not be for "backup

property owner was careless about the security of the property).

369. *See supra* note 295 and accompanying text (discussing the ECPA's three components). When applying the Wiretap Act, courts require the interception to be contemporaneous with transmission in order to find a violation. *See* United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (concluding that the Wiretap Act is violated if a provider intercepts electronic communications that are in transient electronic storage as part of the communications process); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) (discussing the contemporaneity requirement). The *Steve Jackson Games* court also acknowledged that it is unlikely that Congress intended for a Wiretap Act violation to also violate the SCA. *See Steve Jackson Games, Inc.*, 36 F.3d at 461–63 (discussing the legislative history of the Wiretap Act and the SCA).

370. *See* Theofel v. Farey Jones, 359 F.3d 1066 (9th Cir. 2004).

371. *See id.* at 1075 (concluding that "backup purposes" can include when an ISP keeps a copy of an e-mail on its server in case the user needs to download the e-mail again later, thus broadening the category of communications to which the stronger requirements for ECS can apply).

372. *See* Kerr, *supra* note 297, at 1218 (criticizing the Ninth Circuit's interpretation).

373. *See id.* at 1218 n.61 (providing reasons for the author's labeling of the Ninth Circuit's analysis in *Theofel* as "implausible and hard to square with the statutory text"); *see also Theofel*, 359 F.3d at 1075 (providing a broad definition of "backup purposes"); Quon v. Arch Wireless, 529 F.3d 892, 902–03 (9th Cir. 2008) (concluding that by archiving text messages, Arch Wireless was providing backup protection instead of storage services, and thus was an ECS provider).

purposes" if the information were not stored anywhere else.[374] In *United States v. Weaver*,[375] the court held that Hotmail was an RCS provider, so only a trial subpoena would be required to compel Hotmail to produce previously accessed e-mails under 181 days old.[376] It is also unclear the extent to which the SCA would prevent a party in civil litigation from seeking records maintained by a cloud service provider during discovery.[377] Even if a provider does violate the SCA, the remedy for such a violation is not suppression, as it would be with a Fourth Amendment violation because the available remedies are explicitly limited under § 2708.[378]

The intersection of the SCA and the Fourth Amendment may also raise issues of the ultimate constitutionality of the SCA. Because the e-mail acquisition actions of law enforcement in *Warshak* relied on the SCA, and the *Warshak* court viewed e-mail as having the same Fourth Amendment protection as postal mail, the *Warshak* court ultimately concluded that insofar as the SCA permitted law enforcement to obtain e-mails without a warrant,

---

374. *See supra* note 371 and accompanying text (discussing the *Theofel* court's interpretation of the "backup purposes" language contained in the SCA).

375. *See* United States v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009).

376. *See id.* at 771 (interpreting 18 U.S.C. § 2703(b)(2)'s subpoena requirements and ruling that e-mails under 181 days old must be seized using a subpoena).

377. On its face, the SCA does not include an exception for disclosure for civil discovery purposes, so adverse parties may be precluded from requesting stored information directly from service providers. However, because of the importance of civil discovery, courts are likely to find other avenues for allowing such information to be compelled, such as by compelling the opposing party to produce it directly under Rule 34 of the Federal Rules of Civil Procedure. *See* Flagg v. City of Detroit, 252 F.R.D. 346, 352–53 (E.D. Mich. 2008) (concluding that the SCA does not preclude civil discovery for electronically stored communications that are maintained by a nonparty service provider because the other party has control over that information and can be compelled to produce it under Rule 34). Thus, because the subscriber requests the information from the nonparty service provider, the information is being disclosed consistent with the statutory exceptions.

378. *See* 18 U.S.C. § 2708 (2006) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."); United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) (ruling that violations of 18 U.S.C. § 2708 do not warrant exclusion of evidence).

the SCA was unconstitutional.[379] Accordingly, if more courts adopt the reasoning of *Warshak*, the influence of the SCA in the e-mail search context may be significantly reduced.

c. Contracts and Privacy

In the cloud context, one should also consider case law precedent concerning contract law and agreements between consumers and service providers. As the *Warshak* court noted, excessively permissive TOS agreements may deprive a customer of a REOP in contents stored or transmitted using a service,[380] so the validity of these contracts has implications for privacy law. Additionally, privacy policies and TOS agreements have implications for SCA cases because one of the most important exceptions under the SCA is for information obtained after the subscriber or customer has given valid consent.[381] Thus, a privacy policy that reserves a license to use the customer's information and content for business or marketing purposes may be read as consent to disclosure under the SCA.[382] To the extent that the consent applies to communications stored for computer storage and processing purposes, consent renders the SCA completely inapplicable if the service otherwise only qualified as an RCS instead of an ECS.

Contract law is typically state law, so standards will vary across cases. Generally, contracts can be invalidated if they are found to be unconscionable. Some courts have invalidated excessively one-sided TOS agreements on unconscionability

379. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (ruling that the portion of the SCA that allows the government to obtain e-mails without a warrant is unconstitutional).

380. *See id.* at 287 (noting that "if the ISP expresses an intention to 'audit, inspect, and monitor' its subscriber's emails, that might be enough to render an expectation of privacy unreasonable" (citation omitted)).

381. *See* 18 U.S.C. §§ 2702(b)(3), 2703(c)(1)(C), 2703(c)(2) (explaining the consent exceptions to the SCA).

382. However, this may be limited to content for which the customer does not elect stronger privacy protections. Viacom Int'l, Inc. v. Youtube, Inc., 253 F.R.D. 256, 264–65 (S.D.N.Y. 2008) (concluding that acceptance of Youtube's TOS and privacy policy does not amount to consent to the disclosure of private content).

grounds, often when the customer was seeking to avoid mandatory arbitration provisions.[383] Courts have also examined terms not related to arbitration, and may also invalidate terms that the court finds to be excessively unfair.[384]

At least one court has held that privacy policies are purely aspirational, and thus not contracts that are enforceable at law, when they do not afford any rights or remedies to the customer.[385] However, this position does not take into account recent actions by the FTC to enforce privacy policies against companies on the grounds that violating its own privacy policy amounts to an unfair business practice.[386] Thus, we do not anticipate that this "purely aspirational" characterization of privacy policies will be adopted.

---

383. *See* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 35 (2d Cir. 2002) ("Reasonably conspicuous notice of the existence of contract terms and unambiguous manifestation of assent to those terms by consumers are essential if electronic bargaining is to have integrity and credibility."); Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 611 (E.D. Pa. 2007) (finding procedural and substantive unconscionability sufficient to invalidate an arbitration provision that was part of a TOS that amounted to a very one-sided adhesion contract); People v. Network Assocs., Inc., 758 N.Y.S.2d 466, 470 (N.Y. Sup. Ct. 2003) (holding that some terms of a software license were unenforceable due to their unfairness when the provisions included terms prohibiting customers from publishing reviews of the product or benchmark test results without the company's permission).

384. *See Network Associates*, 758 N.Y.S.2d at 470 (holding that some terms of a software license were unenforceable due to their unfairness when the provisions included terms prohibiting customers from publishing reviews of the product or benchmark test results without the company's permission). Courts value the rights of parties in contracts, however, so perhaps they are likely to only invalidate unfair terms that pass a certain threshold. *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 955–56 (9th Cir. 2010) (acknowledging the contract claim that arises when a user violates a game's prohibition on the use of "bots" to automatically play a game); Bowers v. Baystate Techs., Inc., 320 F.3d 1317 (Fed. Cir. 2003) (enforcing a shrinkwrap agreement that prohibited reverse engineering).

385. *See* Freedman v. Am. Online, 325 F. Supp. 2d 638, 640 (E.D. Va. 2004) (finding that a subscriber agreement "is plainly aspirational only . . . and is not intended to confer any rights and remedies upon the subscriber").

386. *See infra* note 465 and accompanying text (discussing FTC enforcement actions).

4. European Privacy Law

The United States and the European Union take very different theoretical approaches to privacy. In the United States, the idea of privacy is often related to concepts like secrecy and intrusions.[387] In the United States, privacy is viewed as an aspect of liberty, with the goal of protecting against intrusions by the state.[388] The European approach, however, views privacy as a right of human dignity, with a focus on an individual's personal autonomy in deciding how his personal data will be used by anyone, including the free market.[389]

European privacy law is very complicated, and a detailed examination is outside of the scope of this Article. However, because we now live in a global information economy, cloud providers must inevitably consider how their services and practices will need to be altered for a European market. For this reason, we will give a fairly brief introduction to this complicated topic.

In the European Union, privacy is considered to be a fundamental right.[390] The first European data protection laws were enacted in the 1970s, followed by the adoption of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[391] in 1981, and the enactment of the EU Data Protection Directive 95/46 (DPD 95/46)[392] in 1995.[393]

---

387. *See supra* Part III.A (discussing fundamental privacy theories).

388. *See* Birnhack & Elkin-Koren, *supra* note 108, at 341 ("In the American model, privacy is understood as a liberty, protecting citizens against the State.").

389. *See id.* ("[T]he common European understanding is of a right to human dignity—an individual right to determine the end uses of our personal data—in which threats to privacy arise from both the State and the free market.").

390. Lanois, *supra* note 18, at 37 (stating that "the European Union has enshrined the status of privacy as a fundamental right").

391. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. no. 108, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

392. Council Directive 95/46, art. 2(a), 1995 O.J. (L 281) 31 (EU).

393. *See* Kuner, *Part 1*, *supra* note 119, at 176–77 (providing a discussion of the early data protection laws in Europe).

DPD 95/46 focuses on the protection of "personal data," which it defines as "information relating to an identified or identifiable natural person."[394] By its terms, it applies EU law to data controllers that use "equipment" within the EU for the processing of personal data, but the term "equipment" has been read broadly to apply to things like cookies and JavaScript.[395] Other provisions that U.S. cloud providers must comply with include DPD 95/46's requirements for robust authentication and access safeguards.[396]

a. The Safe Harbor Framework

DPD 95/46 also governs the transfer of data, permitting data transfers only to other countries with adequately protective privacy laws.[397] The United States does not have sufficient privacy laws, but the data of European users can nonetheless be transferred to the United States if the company handling the transfer complies with the Safe Harbor agreement between the

---

394. *See* Council Directive 95/46, *supra* note 392, at 38; *see also* Schwartz & Solove, *supra* note 3, at 1873–74 (comparing the reduction in privacy law in the U.S. to its expansion in the EU).

395. *See* Kuner, *Part 2*, *supra* note 126, at 228–29 (explaining the controversy over the use of the term "equipment" to encompass things such as "cookies"). Other EU regulations also restrict the use of cookies and similar technologies, requiring the informed consent of a user to be obtained prior to the provider commencing to store and access information that is on the user's computer. *See* Lanois, *supra* note 18, at 40 (discussing the consent requirement under the EU Data Protection Directive and both the 2002 and 2009 ePrivacy Directives). Because cookies involve information that is considered personal data under the Data Protection Directive, which includes IP addresses, a company that uses cookies in the EU must comply with the terms of both the Data Protection Directive and the more recent ePrivacy directive of the EU. *See id.* at 41 ("[T]he use of cookies or similar devices involving a unique user ID or an identifier will result in the application of both the Data Protection and the ePrivacy Directives.").

396. *See* Lanois, *supra* note 18, at 47 ("[D]ata may only be transferred outside of the EU if that country provides an 'adequate' level of protection . . . .").

397. *See* Stylianou, *supra* note 44, at 596 (noting that "[t]he gravest expression of the implications of different levels of privacy protection occurred when the European Union . . . passed the Data Protection Directive, which allows the transfer of data intended to undergo processing to third countries only if they ensure an adequate level of protection").

United States and the European Union.[398] Because of the limits of DPD 95/46 on transferring personal data, some cloud providers have also established segregated EU clouds.[399]

The Safe Harbor framework provides a method for companies to certify compliance with European privacy standards without necessarily using segregated clouds. Under the Safe Harbor Privacy Principles, organizations must: (1) provide *notice* about data collection; (2) give individuals a *choice* to opt out of the disclosure of their personal information to third parties or before their information is put to a secondary use (or to opt in to sharing if the personal information is considered sensitive); (3) extend these standards to *onward transfers*—that is, ensure that third parties to whom personal information is transferred also adhere to the Safe Harbor Privacy Principles or have comparable controls in place; (4) provide individuals with *access* to their personal information held by the organization; (5) take reasonable *security* precautions to protect personal information; (6) take reasonable steps to protect *data integrity*; and (7) provide adequate measures for *enforcement* of the principles.[400]

Adhering to the Safe Harbor Privacy Principles provides a mechanism for companies in the United States to preserve the

---

398. *See* Lanois, *supra* note 18, at 48 (discussing how the Safe Harbor program works between the United States and the European Union); Stylianou, *supra* note 44, at 597 (explaining the Safe Harbor agreement, "according to which American companies could transfer data from Europe as long as they abided by a commonly agreed upon privacy framework set by the United States Department of Commerce and the European Commission"). The European Commission has found that membership in the U.S. Safe Harbor system provides an "adequate level of data protection," but the Commission suggests that further transfer of the data beyond the Safe Harbor member must comply with EU privacy law as well. *See* Kuner, *Part 2*, *supra* note 126, at 231 (discussing personal data protection concerns regarding "onward transfers of data" from U.S. Safe Harbor members to third parties).

399. *See* Lanois, *supra* note 18, at 48 ("The most simple and obvious way to comply with the EU Data Protection Directive is to ensure that personal data does not leave the EU . . . which is why certain cloud vendors offer segregated EU clouds that keep personal data from being transferred outside of the European Union.").

400. *See Safe Harbor Overview*, EXPORT.GOV (Apr. 26, 2012, 3:08 PM), http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Feb. 3, 2013) (providing an overview of the U.S.–EU Safe Harbor program) (on file with the Washington and Lee Law Review).

status quo of a self-regulatory approach to privacy while still being eligible to serve customers in the European Union.[401] We note that these principles also resemble many of the ideas underlying FIPs, and that the Safe Harbor Privacy Principles might provide another model for how companies should handle personal information belonging to customers located in the United States.

IV. Companies, Customer Data, and Customer-Company Interactions

A. Companies and Customer Data

In this Article, we examine the interaction between privacy theories, privacy law, and the relationships between consumers and the companies that serve them in the cloud. These relationships are largely defined by TOS agreements and privacy policies, and these agreements typically enumerate what a consumer can expect concerning the use of his personal information. The concerns about how companies handle customer data go beyond these agreements, however, and include issues like data security, identity theft, and behavioral marketing.

1. Terms of Service Agreements

TOS agreements set forth terms governing the relationship between a service provider and its customers.[402] Generally, cloud-based services targeted at individual users are accompanied by non-negotiable TOS agreements that favor the service provider

---

401. *See* James T. Sunosky, *Privacy Online: A Primer on the European Union's Directive and United States' Safe Harbor Privacy Principles*, 9 CURRENTS: INT'L TRADE L.J. 80, 85 (2000) (explaining the benefits of the Safe Harbor Privacy Principles).

402. *See* Joshua A.T. Fairfield, *Contemporary Issues in Cyberlaw: Nexus Crystals: Crystallizing Limits on Contractual Control of Virtual Worlds*, 38 WM. MITCHELL L. REV. 43, 44 (2011) (referring to terms of use and EULAs as the "social contract of the new millennium," setting forth the rights and redresses of citizens).

over the end user.[403] TOS agreements will generally address things like metering, monitoring, and data backup,[404] and often include clauses in which the provider disclaims liability for harm and forbids customers from using the company's intellectual property without authorization.[405] Some also include terms concerning the retention, control, and ownership of a user's information.[406] TOS agreements take a variety of approaches to customer information. Some include terms that allow providers to access customer information for advertising and other purposes relating to the business, while others are less transparent about what the company may do with customer information, and still others make explicit promises in their TOS agreements that the companies will not access customers' data.[407]

The terms of TOS agreements can have a significant impact outside the context of the provider–customer relationship, potentially affecting the consumer's legal rights. The DOJ has recently argued that violating a website's TOS agreement amounts to unauthorized access under the CFAA,[408] and courts

---

403. *See* Bagley, *supra* note 295, at 163 ("Google's profit model is based on offering free services to consumers in exchange for their consent to non-negotiable terms of service."); Wittow & Buller, *supra* note 7, at 7 ("The SLAs of cloud-based applications and services generally are non-negotiable and much more favorable to the provider than to the end user.").

404. *See* Martin, *supra* note 44, at 311 (noting the difficulties of providing good customer service because of the lack of standards to measure a cloud's performance).

405. *See* Bagley, *supra* note 295, at 178 ("[L]anguage in a TOS agreement merely disclaims liability for any damage to a user's computer data and forbids unauthorized use or redistribution of intellectual property.").

406. *See id.* (explaining that TOS clauses "also dictate the terms by which the entity will retain, control, and own a user's information"). Google's TOS agreement includes a provision giving the company a license to use the customer's data in ways that would otherwise violate the customer's copyright. *See Google Policies and Principles, Terms of Service*, GOOGLE (Mar. 1, 2012), http://www.google.com/policies/terms/ (last visited Feb. 3, 2013) (providing that Google may use personal data in accordance with their privacy policies) (on file with the Washington and Lee Law Review).

407. *See* Robison, *supra* note 4, at 1215–17 (providing an examination of existing cloud providers).

408. *See* Declan McCullagh, *DOJ: Lying on Match.com Needs to Be a Crime*, CNET (Nov. 14, 2011, 11:58 PM), http://news.cnet.com/8301-31921_3-57324779-281/doj-lying-on-match.com-needs-to-be-a-crime/ (last visited Feb. 3, 2013) (discussing the DOJ's stance on CFAA violations in the context of popular

have also examined whether agreeing to an expansive TOS agreement or a broad privacy policy may cause a person to lose a reasonable expectation of privacy.[409] As discussed above in Part III.B.2.a, the terms of TOS agreements may also impact the application of the SCA.[410]

It is very important that consumers read and understand the terms of cloud services' TOS agreements because of the large amounts of sometimes sensitive information stored with these services.[411] Consumers should pay special attention to how the TOS agreements address customer data, including the information that the company claims rights in, and how the consumer can terminate his relationship with the cloud provider.[412] Consumers might be storing information solely in the cloud, making it very important for the TOS agreements to

---

websites such as MySpace and Match.com) (on file with the Washington and Lee Law Review). The Ninth Circuit, however, recently rejected the DOJ's argument on the reach of the CFAA in *United States v. Nosal*. *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (holding that the language "exceeds authorized access" in the CFAA should be narrowly interpreted and is therefore limited to violations of restrictions on access to information, and not restrictions on its use); Richard Santalesa, *Ninth Circuit Narrows Reach of CFAA in* En Banc U.S. v. Nosal *Decision*, INFO. LAW GROUP (Apr. 13, 2012), http://www.infolaw group.com/2012/04/articles/computer-fraud-and-abuse-act-c/ninth-circuit-narrows-reach-of-cfaa-in-en-banc-us-v-nosal-decision/ (last visited Feb. 3, 2013) (discussing the decision in *United States v. Nosal*) (on file with the Washington and Lee Law Review).

409. *See* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (stating that such protections likely would not apply to content stored with a provider that includes terms in an agreement reserving the right to "audit, inspect, and monitor" e-mail content); Bagley, *supra* note 295, at 181 (discussing cases examining the Fourth Amendment in the context of Terms of Service agreements).

410. *See supra* Part III.B.2.a (discussing the Electronic Communications Privacy Act).

411. *See* Soma, Gates, & Smith, *supra* note 16, at 534 (examining the "blurred lines" between work and home life that e-technology has created and suggesting that "users must make a good faith effort to read, understand, and ask questions about service provider privacy and terms of use policies"); *see also* Stylianou, *supra* note 44, at 593 (noting that such terms attract greater scrutiny because of the large amount of data stored with these providers).

412. *See* Wittow & Buller, *supra* note 7, at 7 (asserting that cloud service TOS agreements should address data migration issues to assure business continuity and to protect the customer's continued access to data after the customer's relationship with the provider is dissolved).

include provisions protecting customers' ability to retrieve their content if, for example, a service is shut down.[413]

a. TOS Agreements as Contracts of Adhesion

Under the common law of contracts, forming a contract requires mutual assent.[414] When a contract is not subject to negotiation and is offered by the more powerful party on a "take it or leave it" basis, the contract is often referred to as a contract of adhesion.[415] Privacy policies and TOS agreements typically meet this definition for an adhesion contract.[416] Such contracts are not automatically invalid, but they may be subject to greater scrutiny.

Excessively oppressive TOS terms may be invalidated if the court concludes that the terms are unconscionable.[417] Unconscionability analysis often has two prongs, and courts evaluate the circumstances for both procedural and substantive unconscionability.[418] Courts might be more willing to find

---

413. This issue has come up recently in the context of the shutdown of Megaupload. Megan Geuss, *Megaupload User Asks for His Perfectly Legal Videos Back*, ARS TECHNICA (Mar. 21, 2012, 10:10 PM), http://arstechnica.com/tech-policy/news/2012/03/megaupload-user-asks-for-his-perfectly-legal-videos-back.ars (last visited Feb. 3, 2013) (discussing the shutdown of the file-sharing locker Megaupload and the inability of customers to access their legally stored videos) (on file with the Washington and Lee Law Review).

414. *See, e.g.*, 1 RICHARD A. LORD, WILLISTON ON CONTRACTS § 4:1 (4th ed. 2012) ("[M]utual assent is essential to the formation of informal contracts . . . .").

415. *See Nolo's Plain-English Law Dictionary*, NOLO, http://www.nolo.com/dictionary/adhesion-contract-(contract-of-adhesion)-term.html (last visited Feb. 3, 2013) (providing the definition of an adhesion contract) (on file with the Washington and Lee Law Review); *see also* Bagley, *supra* note 295, at 183 ("[E]lectronic contracts of adhesion are limiting the private rights of an individual to protect their privacy in services so vital to daily life.").

416. Solove, *Architecture, supra* note 172, at 1235 (arguing that the idea that users give informed consent to these terms is a fiction, due to the total lack of negotiation).

417. *See* Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 605 (E.D. Pa. 2007) (finding an arbitration provision to be both procedurally and substantively unconscionable).

418. *Id.*

unconscionability when there are no market alternatives, but the diverse reality of the cloud market makes it unlikely that a lack of market alternatives will be a persuasive argument.[419]

The unequal bargaining power between the provider and its customers means that providers often subject customers to terms that are more favorable to the provider.[420] At least one court has looked favorably on a provider prohibiting the use of "bots" with its service,[421] and Martin expresses concern that this opens the door for "predatory software vendor[s]" to prohibit customers from using third party software with the vendor's projects, thereby eliminating beneficial effects of innovation by third parties.[422]

2. Privacy Policies

Privacy policies and TOS agreements often overlap, though for our purposes we consider privacy policies to be more focused on making the customer aware of the company's policies regarding their data instead of the customer's obligations concerning the service. Terms in a provider's privacy policy might address things like the quantity and nature of collected data and the company's policies on data retention and customer control over data.[423] Privacy policies often also address data security issues, like the use of SSL encryption during data transmission.[424] However, many of these providers insert

---

419. *See* Bagley, *supra* note 295, at 179 (discussing the difficulty of demonstrating unconscionability "in the search engine, e-mail, and digital media services market, where there are many companies even though only a few giants dominate").

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

421. *See* MDY Indus., LLC v. Blizzard Entm't, Inc., 629 F.3d 928, 950 (9th Cir. 2010) (finding that the prohibition of the use of "bots" was permitted under the Digital Millennium Copyright Act).

422. Martin, *supra* note 44, at 312.

423. *See* Stylianou, *supra* note 44, at 599, 602 (discussing the quantity and nature of collected data as well as data retention policies and data storage location).

424. *See id.* at 603 (providing a discussion of data safety, security, and integrity).

provisions in their privacy policies or TOS agreements that repudiate any liability for data loss, and reserve to the provider the right to discontinue the service at the provider's sole discretion.[425]

Privacy policies typically consist of information provided by the service provider about how the provider may gather, use, disclose, and manage the personal information of its customers.[426] Privacy policies, like TOS agreements, are often adhesion contracts marked by significant advantages being reserved for the service provider, such as the right to amend its privacy policy unilaterally with little notice to its customers.[427] Privacy policies may include broad permissions to allow the provider to access information for its own marketing purposes and to disclose customer information to its business partners for business-related purposes.[428] Privacy policies also might not be considered contracts at all, but purely as notices about a company's policy. However, few consumers actually read a company's privacy policy, and even fewer understand it.[429] Solove criticizes many

---

425. *See id.* at 604 (examining Amazon's, Mozy's, and Apple's data protection disclosures).

426. *See* Cascia, *supra* note 17, at 888 ("A privacy policy is a legal agreement between the user and the provider that discloses some or all of the ways the provider gathers, uses, discloses and manages a customer's personal information.").

427. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 82–83 (arguing that privacy policies are not a meaningful contract, with no bargaining over terms and containing mostly unreliable, vague promises); Cascia, *supra* note 17, at 889–90 (discussing Google's privacy policy and noting that "Google reserves the right to unilaterally amend its privacy policy leaving it essentially meaningless"). Birnhack and Elkin-Koren argue that if such a term is included, user privacy is not being effectively guaranteed by upfront notice and consent. *See* Birnhack & Elkin-Koren, *supra* note 108, at 365 (arguing that "if the user agrees upfront to any use of data as detailed by an adjustable privacy policy, the user does not exercise real control over the collection and use of personal data").

428. *See* Soma, Gates, & Smith, *supra* note 16, at 532 (noting that providers often include terms in e-messaging policies and usage agreements permitting the provider to access the systems for "routine monitoring purposes" and to comply with lawful requests by the government or litigants); *infra* Part V (providing an empirical analysis of agreements and policies in the cloud).

429. *See* Schwartz & Solove, *supra* note 3, at 1856 ("[S]tudies have shown that few consumers read privacy policies, and that those who do frequently fail to understand them.").

privacy policies as being "written in obtuse prose," containing large amounts of extraneous information.[430]

Cloud services collect a lot of data, both through the customer's voluntary disclosure of data and through the provider's automatic collection of information through its operations or advertising policy.[431] Many privacy policies assure limited use of customer information.[432] Some, however, are vague, leaving ambiguities and loopholes. Transparency in privacy policies is very important, and consumers should be informed about how their data will be collected and used.[433] In this Article, we posit that reserving explicit rights for consumers to control their data will raise consumer awareness of privacy issues. We anticipate that this raised awareness, combined with the increased control that an individual has over the use of his data, will have a positive effect on the market for cloud services.

a. Sharing Information with the Government

Consumers will often encounter inherent limitations in how much control they can exercise over their data because of common policies permitting the sharing of data with government entities. Privacy policies typically contain provisions reserving to the provider the right to disclose customer information pursuant to lawful government requests.[434] Companies like Google and AT&T

---

430. SOLOVE, DIGITAL PERSON, *supra* note 2, at 82.

431. *See* Stylianou, *supra* note 44, at 599 (examining the quantity and nature of collected data by cloud services). Some companies may also collect information from other sources that pertains to the user indirectly. *See id.* at 601 (using Microsoft as an example to demonstrate that the practice of indirect data collection is increasing).

432. *See id.* at 601, 604 (discussing Microsoft's, IBM's, and Amazon's privacy and data protection policies).

433. *See* Birnhack & Elkin-Koren, *supra* note 108, at 353 (explaining the importance of user consent to data collection).

434. *See Google Privacy Policy*, GOOGLE (July 27, 2012), http://www.google.com/policies/privacy/ (noting that Google may share user data for legal reasons) (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review); *see also* Soghoian, *supra* note 5, at 393–94 (citing a public statement by the CEO of Google in which the CEO listed assisting with lawful investigations as being one of the main reasons that Google keeps detailed data of the online

collect large amounts of personal user data from customers.[435] This sort of information was formerly used for marketing and research purposes, but recently the U.S. government has been building national security databases that contain personal user data provided by cooperating telecommunications companies like AT&T.[436] Sometimes, providers may voluntarily provide data to government entities to improve the provider's own security.[437]

Governments have requested personal user information from various companies for a variety of purposes over the years.[438] This is not limited to the United States. For example, the government of the United Kingdom is considering using data obtained by social networking sites for the purpose of monitoring users to prevent terrorism and crime.[439] Generally, private companies that turn over information to the government are not considered state actors by doing so.[440] Cloud providers sometimes also are required

---

activity of its customers).

435. *See* Bagley, *supra* note 295, at 155–56 ("[T]hird parties such as information service provider, Google, and telecommunication giant, AT&T, amass large amounts of personal user data.").

436. *See id.* at 156 (noting that "in recent years the United States government has built national security databases with personal user data allegedly obtained from cooperating telecommunication companies" that has resulted in Fourth Amendment litigation); Soghoian, *supra* note 5, at 385–86 (discussing wiretaps obtained through telecommunication companies and Internet providers working with law enforcement officers). Bagley cites the wiretapping controversy as an example that did not involve warrants or subpoenas, but instead relied on voluntary agreements with private companies. *See* Bagley, *supra* note 295, at 156–57 (criticizing that the "traditional legal process was evaded" in this situation because "private companies did the data gathering and managed the phone calls" and the companies involved waived their Fourth Amendment rights).

437. *See* Bagley, *supra* note 295, at 154 (citing the example of Google voluntarily providing data to the NSA).

438. *See id.* at 161–62 (noting that the government sought user information from airlines after the September 11th attacks and from hotels and car rental agencies in 2003 to thwart terrorist threats against Las Vegas).

439. *See id.* at 164 (discussing the United Kingdom's potential plan to use data collected by social networking sites).

440. *See id.* at 162 ("[P]rivate companies are not restrained as state actors when they voluntarily hand consumer data to the government . . . they are treated as a third party in whom a consumer is placing their trust."). *But see id.* at 188 (arguing that there may be entwinement sufficient to find state action if a communication provider assigns employees to work with government agencies

to comply with certain content laws of other countries, like Skype's Chinese counterpart that was required to implement a filter to prohibit text messages that included phrases like "Falungong" and "Dalai Lama."[441] There are also some concerns about the U.S. government's ability to exploit software vulnerabilities or even enable the microphones of cellular phones remotely as part of criminal investigations.[442]

There are a number of other reasons why government officials might request information. The federal government recently used data associated with customer shopping cards to trace the source of salmonella poisoning.[443] The DOJ has also requested search records from companies like Google and Microsoft in the course of its investigation into the effectiveness of child protection legislation.[444] However, the court in that case did not compel Google to turn over actual search queries, noting in dicta that there may be an expectation of privacy in such queries.[445]

In addition to requesting the cooperation of private companies, the government itself has been collecting personal information for many years. Solove notes in his book that there are almost 2,000 databases of personal information maintained

---

and respond to government requests).

441. Soghoian, *supra* note 5, at 408. Skype denied allegations that its Chinese software contained a backdoor to allow surveillance by the Chinese government, but it came out in 2008 that when text messages using this software were filtered, the offending message and the identities of the sender and recipient were forwarded to a publicly accessible server in China. *See id.* at 408–09 (providing a discussion of the TOM-Software).

442. *See id.* at 400–02 (discussing the FBI's use of "roving bug" software).

443. *See* Martin, *supra* note 44, at 299 (examining use of consumer data by the federal government).

444. *See* Gonzales v. Google, 234 F.R.D. 674, 679 (N.D. Cal. 2006) (examining a subpoena by the U.S. Attorney General to Google to compile and produce information from the search engine's index and search queries); Bagley, *supra* note 295, at 165 (discussing litigation involving subpoenas for online user data).

445. *See Gonzales*, 234 F.R.D. at 684 (denying the motion to order Google to disclose search queries of its users); Bagley, *supra* note 295, at 165 (noting that, "[i]n the end, Google was compelled only to generate a list of URLs, rather than actual user search queries").

by the federal government.[446] Personal information collection as part of the census began in 1790, with the questions becoming more personal until the 1890 census, which included questions about things like diseases, disabilities, and finances.[447] The massive databases that are already maintained by the government and over which citizens have no control might appear to threaten any attempts to improve informational privacy. Requiring data control protections in the private sector may seem like a relatively small issue compared to government databases. However, private data held by governments generally do not leave the government's possession, and thus the circulation of this information is not as problematic as the circulation of information collected in the private sector.

3. Effects of Security Breaches

A major reason that we argue for consumers to be in control of their data is that we think consumers should be empowered to take proactive steps to protect their information. Consumers, in our view, should be free to withdraw their data from a service if they learn of security failings in that service. One of the dangers of insufficient data security for data in the cloud is the risk of identity theft as a result of data breaches.[448] According to the Identity Theft Resource Center, in 2009 there were at least 498 publicly reported data breaches, impacting 222 million total

---

446. SOLOVE, DIGITAL PERSON, *supra* note 2, at 15. Richards also notes that the government has huge databases of information about citizens. *See* Richards, *supra* note 114, at 1156 (discussing the history of personal data collection by the federal government that began as early as the nineteenth century).

447. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 13 (providing a historical look at the collection of public data by the federal government). The public outcry in response to the intrusiveness of the questions in the 1890 census eventually led to legislation to ensure the confidentiality of census data. *See id.* ("When the 1890 census included questions about diseases, disabilities, and finances, it sparked a public outcry, ultimately leading to the passage in the early twentieth century of stricter laws protecting the confidentiality of census data.").

448. *See* Lanois, *supra* note 18, at 44 (discussing the increasing amount of "commercial, personal, and even secret data and other sensitive information . . . flowing around the globe in the cloud").

records.[449] A single data breach of a credit card processing company in 2012 may have resulted in 1.5 million credit card accounts being compromised.[450]

Identity theft is a federal crime and has been referred to as the most rapidly growing white collar crime,[451] though some criticize the law as not being adequately supported by resources or sufficient criminal sentences.[452] Approximately half a million people are victims of identity theft every year.[453] Twenty-six percent of consumer complaints submitted to the FTC in 2008 concerned identity theft.[454]

But identity theft is not the only risk related to data breaches.[455] Some breaches can involve very personal and embarrassing information, such as when a firm accidentally posted to the Internet the names, addresses, phone numbers, credit card information, and details of the sex lives of ninety psychotherapy patients.[456] Sometimes, breaches are due to a serious failing in a company's procedures. In one instance, Metromail Corporation hired prison inmates to enter personal information into Metromail's databases, and one inmate started sending sexually explicit letters with information about the recipients' lives.[457] In another more troubling instance, the

---

449. Wittow & Buller, *supra* note 7, at 9.

450. *Credit Card Data Breach Contained, Says Global Payments*, BBC NEWS (Apr. 3, 2012, 5:59 ET), http://www.bbc.co.uk/news/technology-17596394 (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review).

451. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 110 (stating that the FTC estimated that 10 million Americans were victims of identity theft in 2003).

452. *See* Solove, *Architecture, supra* note 172, at 1248 (noting the problems with viewing identity theft as an exclusively criminal matter).

453. *Id.* at 1244.

454. Wittow & Buller, *supra* note 7, at 9.

455. *See* Solove, *Architecture*, *supra* note 172, at 1258 ("With ever more frequency, we are hearing stories about security glitches and other instances of personal data being leaked and abused.").

456. *See id.* (providing examples of instances of security breaches of personal information in recent years).

457. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 53 (discussing "irresponsible and careless uses of personal information"). In another Metromail incident, a reporter contacted Metromail and successfully purchased a list of 5,000 children after giving the name of the buyer as a known child molester and murderer. *See id.* at 53–54 (illustrating a lack of care and accountability in

company Docusearch provided a man with information about a woman named Amy Lynn Boyer, which the man then used in finding and murdering Boyer.[458]

Cloud providers might not bear the risk of loss due to fraud, but companies have many incentives to secure data and prevent security breaches because large-scale breaches often result in negative publicity. Security breaches can destroy consumer confidence and devastate a company's bottom line.[459] However, this decrease in consumer confidence may not effectively incentivize the creation of stronger security protocols if cloud service providers store data in proprietary formats, making it difficult for current customers to leave. Thus, we argue that data control and format transparency could have benefits for security in the cloud by giving providers incentives to keep data secure in order to retain customers.

4. Protecting Consumer Data—Who Watches the Watchers?

Currently, consumers have fairly little control over their data, but there are other entities to help address data security issues. Several private bodies have set standards enabling companies to either seek certification as to the adequacy of their privacy practices, or otherwise measure their own actions against industry standards. These options include SAS 70 certification, which involves audits of firms' control mechanisms to protect information;[460] the Payment Card Industry Data Security

---

corporate data collection).

458. *See* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1009 (N.H. 2003) (finding that Docusearch owed a duty of reasonable care when the company disclosed Boyer's information to Liam Youens); SOLOVE, DIGITAL PERSON, *supra* note 2, at 54 (providing the facts of the *Docusearch* case); Richards & Solove, *supra* note 1, at 1923 (discussing the holding in *Docusearch* and noting duty of care issues arising from computer databases).

459. *See* Rhodes & Kunis, *supra* note 23, at 26 ("A security breach affecting a corporation can destroy consumer confidence and be devastating to the bottom line."). There was recently a breach at Heartland Security, leading to a loss of 130 million credit card numbers. *Id.* at 45. Heartland has suffered major financial damages since the breach, including a $60 million settlement with Visa over the breach. *Id.*

460. *See SAS 70 Overview*, SAS 70, http://sas70.com/sas70_overview.html

Standard, which created IT guidelines for the credit card industry aimed at reducing the risk of a security breach;[461] and the Financial Industry Regulatory Authority (FINRA), which requires members to have policies and procedures addressing customer record safety, protecting against unauthorized access, and protecting against relevant anticipated threats.[462] Companies on the Web may also seek TRUSTe certification for their privacy practices.[463] These organizations are elements of the self-regulatory framework that U.S. businesses currently use with regard to privacy. However, these certification authorities are largely sector-specific, and thus we recommend broader protections that do not rely on sector-specific self-regulatory bodies.

When the sector-specific self-regulatory framework fails, there are sometimes other private solutions available. Customers may, for example, sue companies in the event of a database security breach, though courts disagree about whether a customer has standing based on a mere risk of future identity

---

(last visited Feb. 3, 2013) (providing an overview of the standards) (on file with the Washington and Lee Law Review); *see also* Martin, *supra* note 44, at 297 ("[P]ublic companies that fail to obtain SAS 70 qualification by adhering to certain procedures and controls can easily lose the confidence of investors and customers.").

461. *See PCI SSC Data Security Standards Overview*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/security_standards/ (last visited Feb. 3, 2013) (providing an overview of the "comprehensive standards and supporting materials to enhance payment card data security") (on file with the Washington and Lee Law Review); *see also* Rhodes & Kunis, *supra* note 23, at 44 (discussing the PCI DSS guidelines). Rhodes and Kunis note that there is a lack of direct enforcement of the PCI DSS, but argue that companies have incentive to enact the standards on their own. *See id.* at 45 (discussing the financial incentive to enact standards with the example of a breach at Heartland Security that resulted in a $60 million settlement with Visa).

462. *See About the Financial Industry Regulatory Authority*, FINRA, http://www.finra.org/AboutFINRA/ (last visited Feb. 3, 2013) (providing FINRA's mission and message statement) (on file with the Washington and Lee Law Review); *see also* Rhodes & Kunis, *supra* note 23, at 46 (providing background on FINRA).

463. *See Protecting Consumer Information Online*, TRUSTE, http://www.truste.com/why_TRUSTe_privacy_services/privacy_best_practices (last visited Feb. 3, 2013) (providing examples of the best privacy practices that businesses can utilize to build trust with their customers) (on file with the Washington and Lee Law Review).

theft or if standing requires actual identity theft to have occurred.[464] There are also other organizations that focus on online consumer protection issues, including the Electronic Privacy Information Center (EPIC) and Digital Due Process (DDP). These organizations are more policy-oriented and may do things like filing privacy-oriented amicus briefs in relevant litigation.

In terms of government intervention, the FTC has also become involved with personal data security and other privacy issues, using its authority to challenge unfair or deceptive practices.[465] The first FTC action that primarily concerned a company's data security practices was in 2004 against BJ's Wholesale Club after hundreds of instances of identity theft arose due to BJ's data security failings.[466] An advantage to FTC involvement over private litigation by consumers is the ability of the FTC to bring an action against a company in the absence of identity theft. For example, the FTC fined Choicepoint in 2006 after a breach resulted in 163,000 private financial records being compromised, citing Choicepoint's privacy policy as containing "inaccurate and misleading assertions about its security procedures."[467] The FTC may also bring an action when a company fails to adequately secure its data, even if there has not

---

464. *See* Jonathon J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?": Data Collection Practices in the Digital Age*, 10 N.C. J. L. & TECH. 1, 30 (2008) (discussing the issue of standing in consumer data breach cases).

465. *See* Rhodes & Kunis, *supra* note 23, at 36 (discussing the FTC's jurisdiction and enforcement authority); Wittow & Buller, *supra* note 7, at 9 (noting that, as of the time of the authors' writing, the FTC had filed twenty-seven enforcement actions concerning the data security practices of companies). The FTC requires companies to institute "reasonable safeguards" to protect information, and what is "reasonable" depends on factors like how sensitive the data is and how costly it would be for the company to avoid potential risks. *See* Rhodes & Kunis, *supra* note 23, at 36 (discussing the "reasonableness" standard applied by the FTC beginning in 2006 to bolster the enforcement of data security risks).

466. *See* Rhodes & Kunis, *supra* note 23, at 37 (noting the FTC's conclusion that the security failings amounted to an unfair practice in violation of federal law).

467. *Id.*

actually been a data breach.[468] The FTC could also potentially bring an action against a business that uses deceptive practices to obtain information.[469]

As an alternative to extending current regulations to new data issues in the cloud, some argue that the FTC and its current authorities could be used to enforce a company's privacy policy against it.[470] However, after examining a number of privacy policies, we argue that this approach would not be wise given the reality that many companies adopt vague privacy policy language regarding the company's own obligations.[471] It is also unclear whether the FTC would be the appropriate regulatory body in all instances because the FTC usually regulates e-commerce issues, but providers whose services count as telecommunications or information services would also be governed by FCC regulations.[472] We also assert that relying on government

468. *See* Schwartz & Solove, *supra* note 3, at 1856–57 ("[T]he [FTC] has taken actions against companies that fail to provide adequate data security . . . even in the absence of a data breach, though more typically it acts only once a data spill has occurred."). The FTC also settled an enforcement action against Sears in 2009, based on Sears's practice of tracking customers without adequately disclosing details of the tracking program to the customers, and another action against EchoMetrix in 2010 concerning parental control software that also provided information to marketers about children's computer activity. *See id.* at 1858 (discussing the "more substantive approach to disclosure of company behaviors" taken by the FTC in enforcement actions).

469. *See* Richards, *supra* note 114, at 1185 ("The use of fraud or other deceptive practices in obtaining consumer data could also constitute a violation of the Uniform Deceptive Trade Practices Act (UDTPA), and would fall within the powers of the Federal Trade Commission (FTC) to deter and punish unfair trade practices . . . .").

470. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 72 (noting that the FTC has recently brought actions for "unfair or deceptive acts or practices" against companies that violate their own privacy policies); McCarthy, *supra* note 95, at 2260 (discussing the possibility of enforcing PHR vendors' privacy policies against them). McCarthy argues, however, that HIPAA would be a stronger way to address privacy issues with personal health records. *See id.* at 2261 (contrasting HIPAA and the FTC by stating that "HIPAA mandates that covered entities take constant concern over privacy and security by continually auditing, monitoring, and augmenting security when necessary").

471. *See infra* Part V.C (providing an analysis of and statistical information on privacy policies).

472. *See* Soma, Gates, & Smith, *supra* note 16, at 490–91 (suggesting the possibility of a joint rulemaking between the FTC and FCC to address these issues).

agencies to address the failure of companies to give consumers meaningful control over their data would be ineffectual because the most likely approach would be through adjudication, in which individual consumers would not be clearly represented, in an adjudicatory process that by definition would only address problems on an ad hoc basis. On this point, we argue that regulating this behavior in advance would be more beneficial to consumers than case-by-case adjudication.

5. Tracking Technologies and Behavioral Marketing

Another element of privacy policies that is relevant to the issue of data control is the use of technologies to track consumer behavior. Privacy policies typically address the tracking technologies that a website uses for advertising or other purposes. When tracking users, advertisers may use technologies like cookies, flash cookies, and Web beacons. The degree to which companies disclose the use of these tracking technologies varies.[473] The information collected using these tracking technologies can then be used by companies to profile consumers.[474] Consumers typically have the option to decline some tracking technologies, often by adjusting the settings of their Web browsers to decline all cookies. However, we suggest that this option does not represent a meaningful exercise of

---

473. *See* Birnhack & Elkin-Koren, *supra* note 108, at 372 (providing data comparing actual privacy practices to declared privacy practices of numerous websites); Lanois, *supra* note 18, at 34 (referencing a study that found that the top fifty websites installed, on average, sixty-four pieces of tracking technology when a visitor loaded the site, and usually did not provide a warning that they were doing so).

474. *See* Richards, *supra* note 114, at 1157 (discussing the "profiling industry" and noting that the profiles may include "a person's social security number, shopping preferences, health information . . . financial information, race, weight, clothing size, arrest record, lifestyle preferences, hobbies, religion, reading preferences, homeownership, charitable contributions, mail order purchases and type, and pet ownership"); *see also* SOLOVE, DIGITAL PERSON, *supra* note 2, at 50 (noting private companies' recent use of information to categorize people as either angel customers or demon customers, and the practices of some banks to deny credit card applications from college students majoring in liberal arts).

control because many websites require cookies to be enabled for website functionality.

A cookie is a text file that is downloaded to a user's computer when she accesses a website, and it acts as an identifier for the computer on which it is stored.[475] Cookies by themselves do not contain a user's personal information under most definitions of the term,[476] but a company called DoubleClick provides a service to websites, connecting cookies to personal information to enable more targeted advertising.[477] Flash cookies have a similar effect to text cookies, but some flash cookies may be able to reconstruct previously deleted browser cookies and cannot be controlled by the user.[478] Recent research revealed that out of the one hundred most popular websites, fifty-four used flash cookies, but only four sites mentioned the use of flash cookies in their privacy policies.[479] Web beacons, the third type of tracking technology noted above, permit the advertiser to observe a user's website activity in real time.[480]

Behavioral marketing is advertising that is targeted at individuals based on their past behavior patterns.[481] The environment of behavioral marketing has developed substantially

---

475. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 24 (referring to cookies as "a form of high-tech cattle-branding"); Lanois, *supra* note 18, at 33 (explaining how cookies work and why they are useful for both advertising and consumers).

476. However, because cookies typically collect a user's IP address, this is sufficient to find that cookies collect "personal data" for purposes of the EU's Data Protection Directive. *See* Lanois, *supra* note 18, at 41 ("In practice, almost all cookies involve the processing of personal data because even if the user's real identity remains anonymous, cookies typically involve the collection of the user's IP address, the processing of unique identifiers, or both which are personal data within the scope of the Data Protection Directive.").

477. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 24–25 (explaining how DoubleClick functions).

478. *See* Lanois, *supra* note 18, at 35 (discussing a lawsuit that involved the distinction between flash cookies and traditional cookies).

479. *Id.* at 36.

480. *See* Schwartz & Solove, *supra* note 3, at 1851 ("Some technology, particularly the beacon, or 'Web bug,' permits real-time observation of a user's activity on an Internet page, including where one's mouse moved and the information that one typed, such as search queries or personal information that an individual filled into a form.").

481. *See id.* at 1849 (introducing the concept of behavioral marketing).

over the last century, becoming more effective as marketers have gained access to more detailed information.[482] Behavioral marketing has led to advertisers buying access to individuals who match a particular consumer profile.[483] There is a market for consumer data that is collected and can be used for targeting advertisements, with information about an individual's browsing habits selling for a fraction of a cent on the data exchange.[484]

Because declining all cookies would likely lessen a user's Web browsing experience, researchers have worked to develop a technology that focuses on collection by third parties, like third-party advertisers that collect data for behavioral advertising. Concerns over such data collection and the possible privacy implications thereof have led to calls for a "Do Not Track" (DNT) standard, similar to a "Do Not Call" registry, that would allow users to opt out of tracking by third parties.[485] Mozilla's Firefox already includes DNT capabilities.[486] Additionally, Microsoft made DNT the default setting for Internet Explorer 10, and Google announced that Google Chrome would have DNT capabilities by the end of 2012.[487]

---

482. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 19 (noting that direct mail has a yield-per-cost ratio double that of television advertisements).

483. *See* Lanois, *supra* note 18, at 34 (noting that user profiles are bought and sold on exchanges that resemble the stock market); Schwartz & Solove, *supra* note 3, at 1851 ("Marketers draw on extensive databases . . . . They are able to cross-reference online activity with offline records including home ownership, family income, marital status, zip code, and a host of other information, such as one's recent purchases as well as favorite restaurants, movies, and TV shows.").

484. *See* Richards, *supra* note 114, at 1157–58 (noting that in some places, consumer profiles can be bought for $65 for a thousand names); Schwartz & Solove, *supra* note 3, at 1852 (explaining that browsing information sells for as little as a tenth of a cent but that it adds up to a billion-dollar industry).

485. *See Do Not Track, Universal Web Tracking Opt Out*, http://donottrack.us/ (last visited Feb. 3, 2013) (providing an overview of the "Do Not Track" policy proposal) (on file with the Washington and Lee Law Review).

486. *See Do Not Track*, MOZILLA FIREFOX, http://www.mozilla.org/en-US/dnt/ (last visited Feb. 3, 2013) (providing answers to frequently asked questions about the "Do Not Track" preference) (on file with the Washington and Lee Law Review).

487. *See* Kate Solomon, *Chrome Adds Do Not Track, Rolling Out by End of the Year*, TECHRADAR (Sept. 24, 2012), http://www.techradar.com/news/internet/web/chrome-adds-do-not-track-rolling-out-by-end-of-the-year-1099241 (last

Modern consumers are often uneasy about the pervasiveness of behavioral advertising,[488] and some research questions the ultimate value of targeted advertising.[489] However, there is currently not much recourse available to consumers whose data is mined. The privacy torts typically require an invasion to be of an offensive nature, but most of the time, information collection is of largely innocuous information.[490] For these reasons, one of our proposals relevant to data control focuses on the possibility of withdrawing data that was mined using these technologies. A DNT system, as described above, may also assist with limiting future unauthorized collection, provided that most websites eventually adopt it. At the time of this writing, however, many websites and advertisers have not adopted a DNT-friendly implementation.[491] Even if the market solutions become more viable, our proposed data withdrawal and data portability rights are designed to inform and empower consumers, enabling more meaningful participation in the vigorous market for cloud services. In our view, such rights would be complementary to, and not supplanted by, an effective opt-out DNT regime.

---

visited Feb. 3, 2013) (explaining the DNT option that will be added to the Google Chrome browser) (on file with the Washington and Lee Law Review).

488. *See* Schwartz & Solove, *supra* note 3, at 1854 (suggesting that consumer objections to behavioral advertising should be addressed through policy).

489. Aleecia M. McDonald & Lori Faith Cranor, *The Cost of Reading Privacy Policies*, 4 J.L. & POL'Y INFO. SOC'Y 540, 541 (2008) (concluding that targeted advertising "may have negative social utility" after taking into account the opportunity costs required if everyone read and understood privacy policies).

490. *See* Richards & Solove, *supra* note 1, at 1919 (citing *Shibley v. Time, Inc.* for its holding that disclosure of subscriber information did not meet the requirements of causing "mental suffering, shame or humiliation to a person of ordinary sensibilities." (citing Shibley v. Time, Inc., 341 N.E.2d 337 (Ct. App. Ohio 1975))).

491. *See* Solomon, *supra* note 487 ("The main problem with DNT, though, is that not all that many websites and advertisers actually abide by it, since it's more of a guideline than an actual rule."). In fact, some critics say that DNT simply does not work and, in addition, that advertisers are adopting an interpretation of DNT that is contrary to the intent of those promoting DNT. *See* Ed Bott, *Why Do Not Track is Worse Than a Miserable Failure*, ZDNET (Sept. 21, 2012, 12:35 GMT), http://www.zdnet.com/why-do-not-track-is-worse-than-a-miserable-failure-7000004634/ (last visited Feb. 3, 2013) (criticizing DNT and arguing that it does not work) (on file with the Washington and Lee Law Review).

6. Personally Identifiable Information and "Anonymous" Information

The final concept that we will address in the context of privacy policies is the treatment of certain types of information. Arguments about the degree of protection to which information is entitled often turn on the type of information being protected. In the context of information privacy, the focus is often on personally identifiable information (PII), and on information that is considered sensitive. Computer use in the 1960s led to PII becoming more of an issue because companies and government entities were processing a lot of personal data.[492] PII is a term that is often used to describe information that is clearly connected to a specific person, though there is no uniform definition of the term.[493] Service providers often focus on assuring customers that their PII will be kept safe.

Regulatory intervention is often focused on protecting PII, in part because of the threats posed by identity thieves. Statutes define PII in several different ways. Some define PII as information that is personally identifiable, some define PII as information that is not public, and some define it by providing specific examples of information that is PII.[494] With PII, the question is often whether information is identified or identifiable, which respectively refers to whether information immediately connects to an identified person or can be used to lead to an identified person, given more information.[495] In the United States, the concept of PII is largely limited to identified data, whereas the European Union takes an expansionist view of PII that treats identified data the same as data that is only identifiable.[496] Schwartz and Solove argue that the European

---

492. *See* Schwartz & Solove, *supra* note 3, at 1820 (explaining why the PII became an issue in the 1960s).

493. *See id.* at 1816 ("Given PII's importance, it is surprising that information privacy law in the United States lacks a uniform definition of the term.").

494. *See id.* at 1828 (identifying the competing definitions of PII).

495. *See id.* at 1817 (setting forth a "PII 2.0" model that proposes "two categories of PII, 'identified' and 'identifiable' data," and treats them differently).

496. *See id.* (comparing the United States and European models); *see also id.*

Union's expansionist approach is more consistent with the technology than a reductionist approach that limits PII protections to identified personal data.[497]

The idea of categorizing information as PII, however, has become more problematic over the years. The line between identified and identifiable has become increasingly blurred, as has the line between sensitive and nonsensitive. A social security number is generally viewed as very sensitive information, but date of birth may be considered less so. However, computer science has shown that a person's social security number can be estimated to some degree of accuracy if one knows the person's date of birth and the city in which they were born.[498] If a database contains a very large amount of nonsensitive information, the aggregation of the information can track a person's whole existence.[499] A person's search queries are an example of seemingly anonymous information that could nonetheless lead to an identifiable person, especially considering common behaviors like searching for local businesses, information on particular medical diagnoses, and vanity searches when an individual will often search for her own name to see what results emerge.[500]

---

at 1875 (noting that Canada takes a similar approach to that of the European Union).

497. *See id.* at 1875 ("The European Union's expansionist approach to PII is more in tune with technology than is the United States' reductionist approach.").

498. *See id.* at 1846 (citing a recent study by Alessandro Acquisti and Ralph Gross).

499. *See* Bagley, *supra* note 295, at 164 ("The synthesis of data from a user's web search history coupled with email, photos, documents, voicemails, phone logs, and location, creates a profile of an individual that serves as behavior modeling for advertisers. This same data could just as easily be disclosed to law enforcement officials for criminal profiling."); *see also* Richards, *supra* note 114, at 1158 (acknowledging the privacy concern that "uber-databases can be created, composed of nonsensitive information in such enormous quantities that the database constitutes a highly detailed dossier of a person's entire existence").

500. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1717–18 (2010) (providing an example of AOL search queries being used to identify individuals); Schwartz & Solove, *supra* note 3, at 1848 (explaining that "if the user has engaged in a highly specific search, or multiple searches, she becomes more

Even if identifying information is removed, that does not necessarily solve the privacy problems. Reidentification science is a new field in computer science research that reattaches anonymized information to identified individuals.[501] Researchers may reidentify a dataset by, for example, comparing two databases, one anonymized and one containing PII and some information fields in common with the anonymized database.[502] The FTC has recently acknowledged that the distinction between PII and de-identified information is often blurred.[503] Because of the ease with which data can be reidentified, Ohm suggests rejecting the concept of PII entirely, though Schwartz and Solove instead suggest a reunderstanding of what information should be considered PII.[504]

---

identifiable" and "[a]t some point, a search allows a person to be readily identifiable").

501. *See* Ohm, *supra* note 500, at 1704 (arguing that the science of reidentification should be of more concern to policymakers than PII).

502. *See id.* at 1725–26 (explaining the basic principles of how reidentification functions). One potential source of databases containing PII is public records, which many times may be obtained upon a showing that the request is not for an improper purpose. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 133 (discussing the history of public record disclosure laws). Public records that may be so obtained include a person's vital records and records of a person's interactions with government. *See id.* at 128–29, 134 (demonstrating the breadth of personal information contained in public records). When a person makes a state or federal Freedom of Information Act (FOIA) request, the state may redact private personal information, but the person to whom the information corresponds cannot object to a disclosure if the state does not redact such information. *See id.* at 135 ("The federal FOIA doesn't require that a person be given notice that his or her personal information is encompassed within a FOIA request. Even if an individual finds out about the request, she has no right under FOIA to prevent or second-guess an agency's decision . . . .").

503. *See* Schwartz & Solove, *supra* note 3, at 1828 (discussing the core conceptual problems with PII recently identified by the FTC). The Seventh Circuit has also noted the problem of reidentification, holding that redacting patient identities in a series of records about recipients of partial birth abortions was not sufficient to avoid violating the patients' privacy rights. *See id.* at 1844 (recognizing that "de-identified data can readily be re-identified" (citing Nw. Mem'l Hosp. v. Ashcroft, 362 F.3d 923, 929 (7th Cir. 2004))).

504. *Compare* Ohm, *supra* note 500, at 1742–45 (arguing that the concept of PII must be replaced to allow for privacy law to move forward), *with* Schwartz & Solove, *supra* note 3, at 1817 (arguing that "PII must be re-conceptualized if privacy law is to remain effective in the future").

Considering the technological issues, theorists who urge government regulation should evaluate which approach to PII should be taken. Reidentification science should be examined by policymakers to determine whether the concept of PII should be expanded to include both identified and identifiable information. Schwartz and Solove propose a model in which information is considered identified when the person's identity is ascertained, identifiable when there is a nonremote possibility of future identification, and nonidentifiable when the risk of identification is remote and the information is not relatable to a person.[505] We argue that limited government intervention would be beneficial to set a baseline for protection of PII to mitigate threats to identity security, but we do not take a position on the identified–identifiable dichotomy. The existence of such regulations would likely raise consumer awareness of these threats. Once informed, we expect that consumers will express a preference for exercising meaningful control over their PII, whether identified or identifiable.

V. Empirical Analysis of Agreements and Policies in the Cloud

In the interest of empirically establishing a baseline for the current status of "data control" terms in contemporary agreements, we examined the privacy policies and TOS agreements of several different cloud providers. Our sample size is fairly small, consisting of twelve TOS agreements and nineteen privacy policies, but because so many companies use boilerplate language for these agreements, even though they may include different types of provisions, our small sample size is nonetheless very likely to be fairly representative of the industry. In fact, insofar as our sample emphasizes several enterprise-oriented companies with fee-based structures, in addition to consumer-oriented companies that rely on advertising revenue, our findings may provide a more generous estimate of the degree to which the terms of agreements favor the customer.

---

505. *See* Schwartz & Solove, *supra* note 3, at 1878 (discussing their proposed model of PII).

A. Methodology

In collecting the privacy policies and TOS agreements, we first used a report by BTC Logic that identified thirteen companies that are viewed as leaders in cloud computing.[506] In addition to the BTC Logic report, we also collected TOS agreements and privacy policies for six additional consumer-oriented cloud services whose information was available through Quantcast's website.[507] Most of these companies made their privacy policies available on a company website. In addition to privacy policies for all nineteen companies, we collected twelve separately labeled TOS agreements and one set of disclaimers from EMC that did not include other terms commonly found in TOS agreements.[508]

---

506. *See BTC Logic Ranks: Top 10 Cloud Companies*, BTC LOGIC (2010), http://www.btclogic.com/documents/BTCLogic_TopTen_Q22010.pdf (providing a ranking and report of the top ten cloud computing companies). Based on their appearances in the list of the top thirteen cloud companies, we included in our sample: Google, Amazon, Microsoft, Cisco, Citrix, EMC, Level 3, Oracle, Red Hat, Sales Force, Symantec, VMWare, and IBM.

507. The additional six companies whose agreements we analyzed were: Carbonite, Dropbox, Flickr, Facebook, GoDaddy, and Apple. For Apple, we specifically looked at the TOS agreement and privacy policy for Apple's new iCloud service. Quantcast is a company that is very active in the Web advertising arena, with a website that provides detailed information about services on the web. Quantcast also provides a list of the top 100 websites in terms of visits. *Top Sites*, QUANTCAST, http://www.quantcast.com/top-sites (last visited Feb. 3, 2013) (providing a ranked list of websites based on the number of people in the United States who visit each month) (on file with the Washington and Lee Law Review).

508. Some companies declined to disclose sample TOS agreements. We attribute this in part to the different business models of the companies. If a product is anticipated to be widely deployed to a large number of people, such as Amazon's AWS or Google's ad-supported services, the TOS will most likely be standardized to address the company's relationships with a large population. When a service provider is contracting with an established enterprise that is paying a large sum for these services, we anticipate that the contracting is likely to be more balanced, with TOS agreements being tailored to the specific customer. Some companies such as IBM focus on very customer-specific services with a target audience of large enterprises, and the terms will change based on the specific needs of the customer. In those situations, the TOS will be more like a standard contract between two parties than the click-wrap agreements that individual consumers are familiar with through installing software on their systems.

Table 1

Company	**Privacy Policy**	**Disclaimers/ Warranties Separate from TOS**	**TOS Agreement**
Amazon	X		X
Microsoft	X		
Cisco	X		
Citrix	X		
EMC	X	X	
Level 3	X		X
Oracle	X		
Red Hat	X		
Salesforce	X		X
Symantec	X		X
Vmware	X		X
IBM	X		
Carbonite	X		X
Dropbox	X		X
Flickr	X		X
Facebook	X		X
iCloud	X		X
GoDaddy	X		X
Google	X		X

The remaining six companies, all from the BTC Logic sample, did not make a boilerplate TOS agreement available to noncustomers, and these companies often targeted their services at enterprise customers. In these situations, TOS agreements may be closer to a traditional contract. However, consumers with fewer resources, like end users and small businesses, are likely to have no bargaining power. These consumers are the anticipated beneficiaries of the changes we suggest. Currently, small businesses and end users are simply not given reasonable alternatives for controlling their data. Thus, the current market

is inefficient, notwithstanding the availability of more involved contracting when the customer is a wealthy enterprise.

One of the challenges of educating the public about privacy policies and TOS agreements is that many times, people assume that these agreements are all the same. We posit that a detailed, side-by-side comparison of agreement provisions based on provision categories would prove the most helpful in noting both similarities and differences between these provisions. Thus, once we had collected the privacy policies and TOS agreements, we first carefully read the language of the agreements with an eye to creating categories and subcategories to permit us to compare the language of several agreements from a top-down perspective. We then categorized the different provisions and noted in our research whether certain provisions were present or absent in a given company's available policies.

The purposes of privacy policies and TOS agreements are very different. Privacy policies generally focus on information that can identify the individual, whereas TOS agreements generally focus on matters relevant to potential conflicts between a company and its customers. Both types of agreement reflect a company's policies with regard to data control. Privacy policies are more directly relevant to data control issues relating to the control of personal information. TOS agreements, on the other hand, often address matters like the ownership of intellectual property and the processes to be followed to obtain stored data upon termination of service.

Analyzing a collection of nineteen privacy policies and twelve TOS agreements applicable to cloud services, a number of patterns emerged. The following subparts will first give a brief overview of our findings with respect to TOS agreements and privacy policies, and then discuss the implications of these patterns.

B. Terms of Service Agreements

TOS agreements typically address potential legal conflicts in advance. These agreements may use choice of law and venue provisions to state where litigation must take place, indemnify the company against third parties, limit damages either by type

or by setting a cap for damage awards,[509] and disclaim warranties to the extent permitted by law.[510] The TOS agreements in our sample addressed major topics like these. Seven of the twelve noted that the company might alter the services offered, but only two of the twelve stated that they would give notice to customers of such changes. This is significant because that means that most of the companies in our sample provide little information upfront about the degree to which customers will be notified of service changes.

For our purposes, one relevant aspect of this relationship is the issue of exercising control over data upon termination. Within our sample, eleven of the twelve TOS agreements set out conditions for account termination. Ten of the twelve set out conditions in which the company is authorized to terminate an account for cause, and two of the twelve set out conditions in which either party to the contract can terminate an account for cause, including a breach of the agreement between the parties. Six of the twelve also include provisions allowing customers to terminate their accounts for any reason.

Only five of the twelve, however, address the issue of data access after an account is terminated, and how and when a customer may access the provider's servers to back up their files and delete them from the servers. The removal of information from the company's servers also implicates document retention policy, which is sometimes addressed in a company's privacy policy. Eleven of our full sample of nineteen companies address document retention to some extent, and refer to the company's possible limitations under the law concerning permanent deletion of a customer's data.

---

509. *See, e.g.*, Amazon Web Services, *Customer Agreement*, AMAZON (Mar. 15, 2012), http://aws.amazon.com/agreement/ (last visited Feb. 3, 2013) (disclaiming liability in paragraph eleven for "direct, indirect, incidental, special, consequential, or exemplary damages") (on file with the Washington and Lee Law Review).

510. States following the Uniform Commercial Code will often not recognize a contractual waiver of certain implied warranties unless the waiver is conspicuous within the written contract. *See* U.C.C. § 2-316 (1977).

Table 2

TERMINATION OF ACCOUNT (out of 12)	
Lists when company may terminate for cause	10
Lists when either may terminate for cause	2
Permits customer to terminate without cause	6
Includes provisions for temporary account suspension	1
Specifies time period for former customer to access and delete information*	4
TOS does not address	2
* However, 11 of the 19 in our full sample also refer to the possibility that they may be required by law to retain customer information.	

In TOS agreements, we were especially concerned about the extent to which the information remains the property of the customer. All twelve companies in our TOS sample included statements asserting the company's rights in its own intellectual property that it was licensing to its customers, though only six of the twelve included a provision reiterating that the customer's intellectual property remains his own. Three of the twelve (Amazon, Flickr, and Apple) reserve a license in the customer's IP to the company limited to the purpose for which the customer submitted the content. Another set of three companies in the sample (Facebook, GoDaddy, and Google) also address the granting of a license to the customer's IP, but these latter three do not include explicit restrictive language that would limit the scope of the license to the customer's initial purposes. Eleven of the thirteen companies for which we had TOS agreements or sets of disclaimers also include provisions whereby the company retains full rights in suggestions or ideas submitted by customers, and can therefore use or implement these suggestions as they see fit without giving the submitter of the idea any form of credit or acknowledgment.

Table 3

INTELLECTUAL PROPERTY (out of 12)	
The company retains full rights in its intellectual property that it is licensing to the customer	12
The customer retains full rights in his intellectual property that is maintained on the company's servers	6
The company obtains a license to use the customer's content, not explicitly limited to purpose for which it was originally submitted	3
The company obtains a license to use the customer's content for marketing purposes	1
The company owns all rights in any e-mails, suggestions, or ideas that the customer sends to the company	11

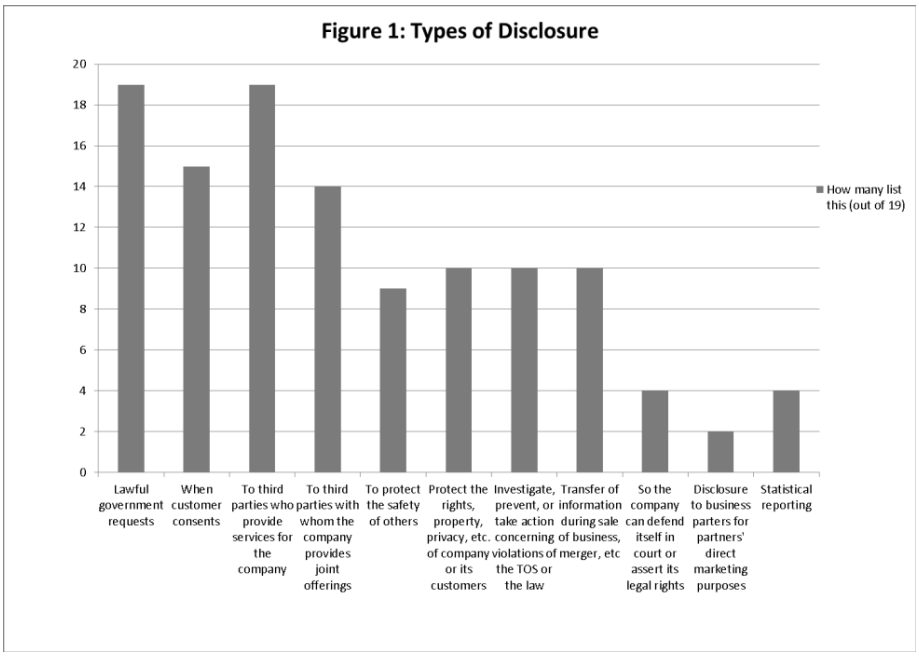
C. Privacy Policies

There are some things that all or almost all of the policies in our sample addressed. All of the companies that we examined gave examples of situations in which they would gather users' personal information and how they would make use of it, such as obtaining the user's name, e-mail address, and other contact information in order to register the user's account and process the user's requests. Eighteen of the nineteen companies in our sample also purport to give their customers some control over the collection of their personal information, which may include the ability to opt out of data collection or the ability to access and edit personal information already on file with the company. Eighteen of the providers in our sample also addressed compliance with either TRUSTe or Safe Harbor, security concerns, changes to the privacy policy, and included a section about the use of tracking technologies.

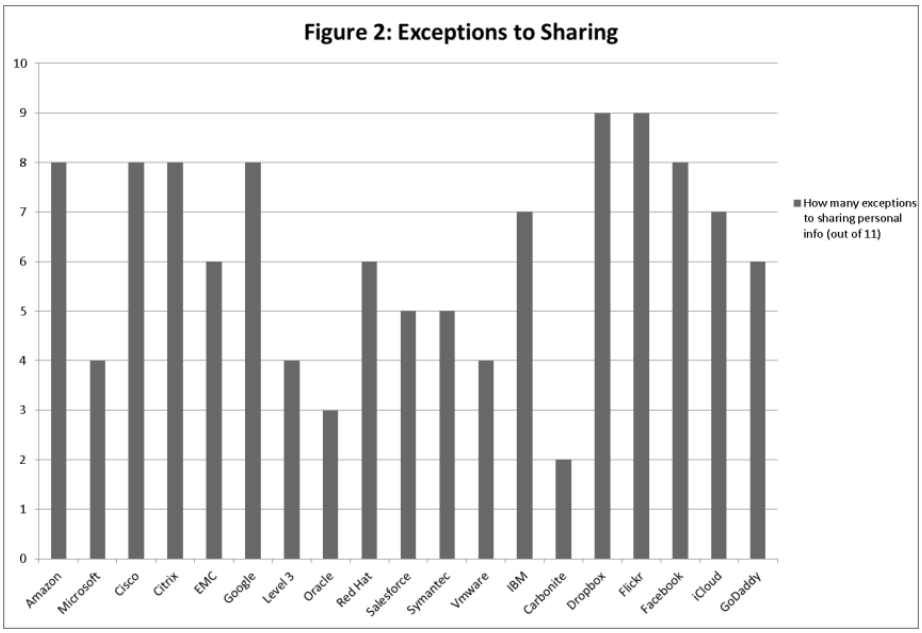
Table 4

19 out of 19 Privacy Policies included:	**18 out of 19 Privacy Policies included:**
Data gathering by the company	Customer control over information
How the company uses that data	Security of user information
When may customer data be disclosed to third parties	Changes to privacy policy
	Complies with TRUSTe or Safe Harbor
	Use of tracking technologies

All of the providers in our sample also included information about sharing customer information with third parties. When the question turned to with whom and when a user's personal information would be shared, however, the differences between the agreements began to stand out. For example, all nineteen companies included lawful government requests as a condition for disclosing customer information, ten said customer information may be disclosed in order to investigate, prevent, or take action concerning violations of the law or the company's TOS, and four said that customer information may be disclosed so that the company can defend itself in court or assert its legal rights. Generally, the enumerated situations in which user information can be disclosed are fairly rational, with an eye to protecting customers' privacy interests. However, two companies noted in their privacy policies that they may disclose customer information to the company's business partners for the partners' direct marketing purposes.



We identified eleven total categories of situations for information disclosure, and noted that out of our nineteen privacy policies, the companies listed between two and nine of these when describing information disclosure. Listing more categories of disclosure does not necessarily mean that a company is less protective of privacy, but it does underscore the variety and complexity inherent in analyzing these agreements.



People have been told for years to be careful of how much they disclose about themselves online in public forums,[511] so it is not a surprise that many of the companies that provide chat forums and bulletin boards for their customers also include disclaimers in their privacy policies that information disclosed in these forums is not protected by the company's privacy policy. Another fairly common-sense provision that fifteen of the nineteen providers include in their privacy policies is a disclaimer that the company does not control the privacy policies of third parties whose websites the customer may access through links on

511. *See, e.g.*, David Gregorio, *Be Careful What You Post Online, Career Counselors Warn*, REUTERS (Aug. 6, 2009, 1:53 PM), http://www.reuters.com/article/2009/08/06/us-careers-socialmedia-tech-life-idUSTRE5754U220090806 (last visited Feb. 3, 2013) (describing how online interactions "present numerous opportunities to sabotage [one's] hunt for a job or promotion") (on file with the Washington and Lee Law Review); Michelle Singletary, *Be Careful Online: Not Everyone Is a True 'Friend'*, THE COLOR OF MONEY (May 14, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/05/13/AR2009051303439.html (last visited Feb. 3, 2013) ("Like a pickpocket working a crowded public venue, cyber thieves may be collecting information that makes victimizing you so much easier with all the personal data you provide.") (on file with the Washington and Lee Law Review).

the company's website. These provisions usually advise the customers to read the privacy policies of the third-party websites.

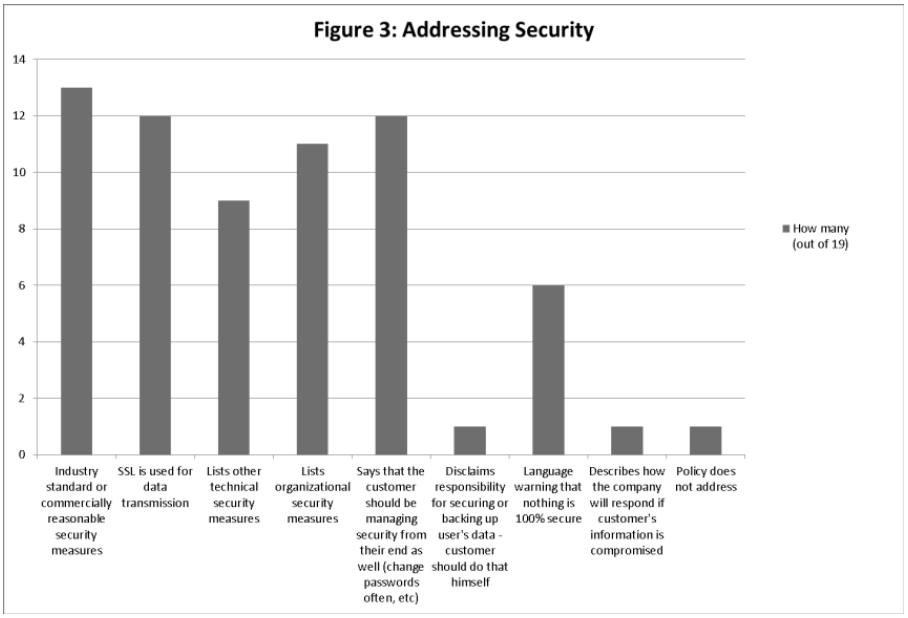
Of the nineteen, only Symantec and Citrix explicitly stated that their customers' information may be disclosed to the company's business partners for direct marketing purposes. Fifteen of the nineteen policies state that the company will not step outside the language of the privacy policy unless the customer gives consent. Disclosure to business partners is generally covered by another button on a form that a customer either checks or unchecks to give permission to the company to share information with these business partners for marketing purposes. Generally, the companies in this sample seem very aware of the negative press associated with selling user information to data farming firms.[512] Four companies in our sample note that they may disclose aggregated information for statistical purposes. Red Hat is one of the four, but its privacy policy also assures that once this information is aggregated, it is no longer traceable to the original individual.

Another element found in all but one of the privacy policies was a discussion of security measures to protect customer data. Data security is not directly related to data control, but as we noted above in Part IV.A.3, giving customers the power to withdraw and move their data may result in security-driven decisions to change services, thus giving companies incentive to implement stronger security measures to retain customers. Thirteen of the nineteen companies in our sample referred to their use of industry standard or commercially reasonable security measures. Some of these companies also listed specific technological or organizational measures in place, but others

---

512. *See, e.g.*, Mitch Lipka, *Twitter Is Selling Your Data*, REUTERS (Mar. 1, 2012, 11:35 AM), http://www.reuters.com/article/2012/03/01/twitter-data-idUSL2E8DTEK420120301 (last visited Feb. 3, 2013) ("Twitter users are about to become major marketing fodder, as two research companies get set to release information to clients who will pay for the privilege of mining the data.") (on file with the Washington and Lee Law Review); Jason Morris & Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN (Aug. 23, 2012 3:42 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html (last visited Feb. 3, 2013) ("Acxiom . . . is just one of hundreds of companies who are peering into your personal life, collecting data that is generated from everything you do online . . . .") (on file with the Washington and Lee Law Review).

simply included a vague statement about implementing industry standards. Another common element of security is encryption, and twelve of the nineteen stated that they use SSL encryption during the transfer of data. Twelve of the nineteen also stressed the importance of customers being proactive with the security of their own systems, and six emphasized that no electronic storage or transmission would ever be 100% secure. Only one company, Oracle, gave any information about what steps would be taken in the event that a customer's user information was compromised.



Because information will be governed by different laws when it is located in different countries, companies also must keep jurisdictional issues in mind when describing their privacy practices. A majority of the companies (fifteen of nineteen) include a provision in the privacy policy notifying the customer that their data may be transferred to and processed in other countries. Only Amazon appears to give customers a meaningful choice of where their information is stored and processed, with its privacy policy stating that data will not be moved to other regions without the customer's consent.

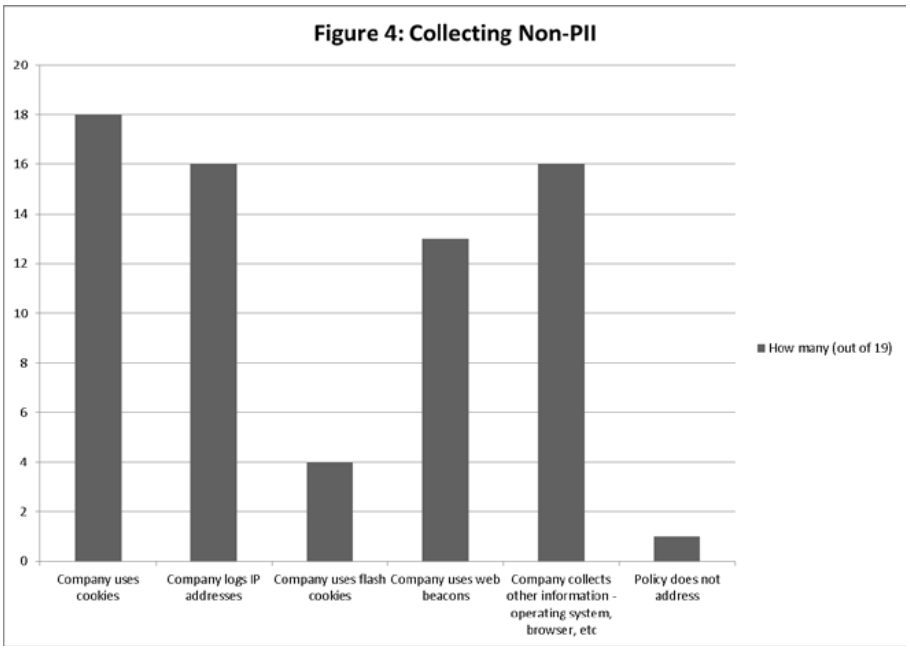
The question of where data is stored is significant, especially when the company has customers within the European Union. Because the European Union has strict privacy requirements,

U.S. companies that wish to transfer personal information from the European Union to the United States must certify compliance with the Safe Harbor program.[513] Sixteen of the nineteen companies in our sample certify in their privacy policies that they are in compliance with this program. Two of the three companies that do not state compliance with Safe Harbor do, however, certify compliance with TRUSTe standards. Of the nineteen companies, eight certify compliance with both Safe Harbor and TRUSTe. Only one company, Citrix, does not refer to either the Safe Harbor program or adherence to TRUSTe standards in its privacy policy.

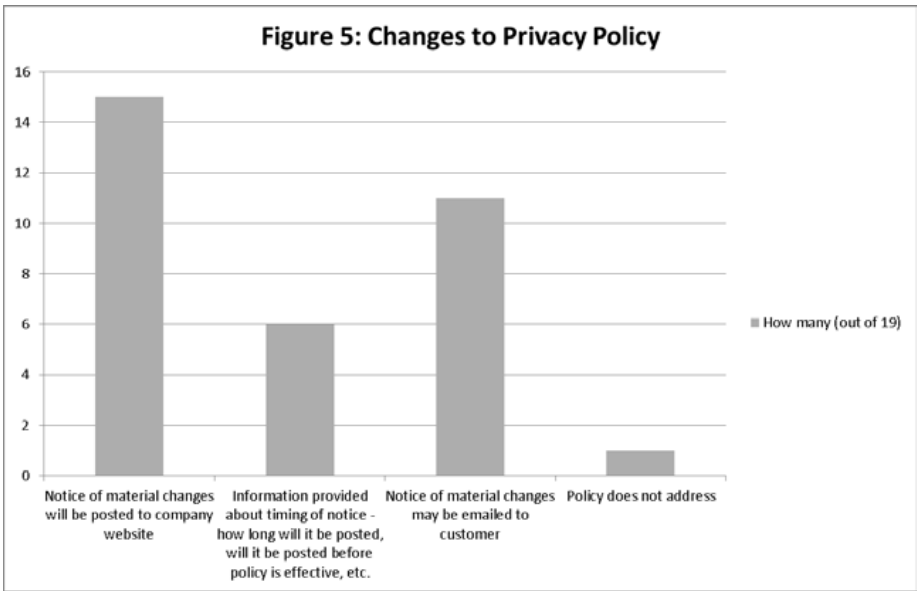
To exercise meaningful data control, consumers should be informed about how data is collected. Most of the companies in our sample detailed their use of Web tracking technologies within their privacy policies. Eighteen of the nineteen companies disclosed their use of cookies on their websites, sixteen of the nineteen disclosed that they used IP logs to track user behavior, and thirteen of the nineteen indicated that they used Web beacons to track user behavior. Sixteen of the nineteen also listed other information that they collected from users, including information on the user's browser and operating system, and other information that can be obtained using Javascript. Only four of the nineteen companies include flash cookies in the list of technologies utilized. However, as earlier research has noted, the use of flash cookies is sometimes unreported by companies.[514]

513. *See* Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC, 2000 O.J. (L 215) 7 (EC); *see also* EXPORT.GOV, *supra* note 400.

514. *See supra* note 473 and accompanying text ("The degree to which companies disclose the use of these tracking technologies varies.").



Privacy policies and TOS agreements for services in the cloud may also change periodically to reflect new priorities or activities on the part of the provider. When companies are empowered to change the terms of agreements unilaterally in material ways, this can undermine user efforts to control data at the outset of the contractual relationship. The privacy policies of eighteen of the nineteen companies in our sample addressed changes to the privacy policy. All eighteen indicated that notice of material changes would be posted on the company's website. Only six of those, however, gave any indication of either how long the notice would be posted or whether it would be posted before the changes went into effect. Eleven of the eighteen also indicated that the company might contact the customers directly to notify them of material changes to the privacy policy. These varying approaches to keeping consumers informed of changes are troubling, and are also reminiscent of our findings in the TOS agreement portion of this study, where we found that of the seven companies that discussed changes to the service, only two indicated that the company would notify current customers of the changes.



D. Analysis and Discussion

In analyzing these documents, we placed the provisions into broad categories. For privacy policies, the categories included provisions listing how and why personal information would be gathered, when and with whom it would be shared, security of information, whether personal information is transferred to other jurisdictions, the collection of non-personally identifying data, provisions addressing third party content and advertisements, and provisions addressing customer control over information. In terms of these larger categories, the companies that we looked at generally have similar priorities. With respect to security, the companies that we examined were more likely to speak in vague terms, with little specific detail (with the exception that most companies referenced SSL encryption). The TOS agreements that we analyzed tended to be more detailed, but this may be because TOS agreements are designed to protect specific rights of the companies. In a TOS agreement, a company will generally address the company's liability for harms to the customer and what recourse a customer may have. A company is also likely to address intellectual property issues, though their primary

interest is typically on protection of the company's rights rather than the customer's rights.

As noted above in Part IV.A.4, consumers are likely to be unable to enforce a company's privacy policy against it. Under § 5 of the FTC Act,[515] however, the FTC is empowered to take action against companies that engage in unfair or deceptive trade practices,[516] and the FTC has a precedent of using this authority to take action against companies that fail to comply with their own privacy policies.[517] Given the possibility that a company could face legal problems for failing to comply with its own privacy policy, this gives a perverse incentive for a company to commit to as little as possible and inform its customers of as little as possible within its privacy policy. This threat of legal recourse may provide a partial explanation for why the companies that we examined are generally vague with respect to the rights of their customers and the methods used to protect their data.

In general, the privacy policies and TOS agreements that we have examined are much more protective of the company that wrote them than of the customer that agrees to them. This is not much of a surprise, especially considering the literature about asymmetric "click wrap agreements" that customers are often required to agree to in order to install software or use services online.[518]

---

515. *See* 15 U.S.C. §§ 41–58 (2006).

516. *See id.* § 45.

517. *See supra* Part IV.A.4 (describing FTC enforcement efforts).

518. *See, e.g.*, Jared S. Livingston, Comment, *Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting*, 21 ALB. L.J. SCI. & TECH. 591, 625 (2011) ("There are several kinds of asymmetric information in this market: (1) failure to read provided information about the agreement; and (2) failure to appreciate the risk of loss of private information."); Lucille M. Ponte, *Getting a Bad Rap? Unconscionability in Clickwrap Dispute Resolution Clauses and a Proposal for Improving the Quality of These Online Consumer "Products,"* 26 OHIO ST. J. ON DISP. RESOL. 119, 119 (2011) ("In undertaking these online transactions, millions of consumers each day simply click on 'I Agree' to a site's standard terms of use, often without reading or understanding the terms and conditions of their purchases.").

E. Implications

Publicly traded companies respond to public demand. As long as consumers ignore privacy policies and TOS agreements, accept that their control over their own data is subject to the will of the service provider, and remain uninformed about existing privacy threats, the companies have little incentive to write privacy policies and TOS agreements with their customers' best interests in mind. On the other hand, if a data control policy became a legal mandate, the customer service experience of various cloud providers could see a marked improvement as providers compete to retain customers. Our research of the literature and our own analysis of the terms of TOS agreements and privacy policies lead us to conclude that there is currently a significant failure on the part of the market to ensure that consumers have sufficient control over their data in the cloud. We argue that this market failure is something that must be remedied to ensure the protection of personal privacy in the cloud.

Given the prevalence of the data trade and the value of profiles to marketers, consumers who are willing to trade personal information and privacy for free services are not just using their own data as currency; to some extent, it could even be said that they are becoming a commodity themselves. This commodification is part of a trade-off, and consumers may even be trading some of their legal rights in exchange for services in the cloud. Currently, a company that provides services to individuals and small businesses can demand any number of allowances as to the use of customer data in its privacy policy, and can substantially limit customers' permissible actions in its TOS agreement. The customer has no bargaining power to challenge these terms. These terms, in turn, can affect the customer's legal rights, limiting the extent to which the Fourth Amendment and the SCA protect data that the customer entrusts to the company, and potentially even making the customer vulnerable to liability under the DOJ's current interpretation of the CFAA.

Throughout this Article, we promote the idea that consumers should have the ability to exercise meaningful control over their own data, including the ability to withdraw their personal information and move their data from one provider to another. If

a regulatory intervention like we propose in this Article gives consumers the power to exercise control over their data, but the consumers *choose* to not exercise these data control rights and still choose to trade their information for various services, such informed decisions may indicate that there is not a systemic flaw in this approach to personal data. However, we argue that the current utter lack of meaningful control prevents us from determining if the current data trade business model can be optimal.

VI. Recommendations—Building a Baseline for Facilitating Transactions in the Cloud

In the United States, privacy is largely protected using narrow laws that apply only to specific categories of information. To the extent that laws of general applicability apply to privacy in the cloud, like the Fourth Amendment and the SCA, customers may inadvertently remove their own privacy protections by agreeing to excessively broad terms in a cloud service's privacy policy. Even though the FTC has brought actions against companies that violate their own privacy policies, these actions arguably serve only to give the providers incentives to write privacy policies that are as vague about the providers' obligations as possible.

After examining the privacy policies and TOS agreements in our sample and analyzing a variety of legal issues and privacy theories, we have arrived at a series of recommendations to what we see as the failure of the contractarian paradigm to adequately protect parties that indicate agreement with these terms. We recommend a new legal regime that would emphasize empowering consumers by setting a baseline of protection to ensure that a consumer has control over her own data. The baseline would be designed to protect the most sensitive information without hindering market development.

A. Building the Baseline

One of our foundational arguments is that relatively modest regulatory intervention into the relationship between providers

and consumers could support positive social change with regard to privacy protections. To some extent, legal regulations can provide structure for social interactions, and the strength of the legal control can affect perceptions of social control and personal freedom.[519] Regulating privacy would involve the regulation of relationships, perhaps by placing limits on organizational power.[520]

When implementing a legislative system to address problems, policy makers can either choose to implement rules, which tend to focus on strict requirements, or standards, which tend to be more flexible and open-ended. In regulating technologies, standards may be superior to rules because standards are more adaptable to further technological change.[521] Detailed and inflexible sets of rules can either chill technological development, or in the alternative can quickly become obsolete if the progress of technology continues unimpeded.[522] On the other hand, if the implemented regulations are too open-ended and vague, they can end up being entirely ineffective.[523] A study by Birnhack and Elkin-Koren questions the very idea that regulation of personal data collection and use would be effective at all.[524] While we do not suggest specific language for regulations

---

519. *See* Solove, *Architecture, supra* note 172, at 1240–41 (explaining his use of the term "architecture" to describe the protection or diminishing of privacy in our society).

520. *See id.* at 1242 ("Protecting privacy thus depends upon regulating relationships, often by enforcing limits on the power of bureaucratic organizations.").

521. *See* Schwartz & Solove, *supra* note 3, at 1871–72 (describing how "standards are generally the superior choice for dealing with situations of rapid change because . . . rules can become obsolete").

522. *See* Solove, *Architecture, supra* note 172, at 1275 (summarizing research that shows how regulations, "if too specific, can quickly become obsolete, discourage innovation, and be costly and inefficient").

523. *See id.* ("However, rules that are too open-ended and vague can end up being toothless. Although security standards must not be overly specific, they must contain meaningful minimum requirements.").

524. *See* Birnhack & Elkin-Koren, *supra* note 108, at 343 (noting a low level of compliance with information privacy laws across several categories of websites in Israel). The authors noted that popular websites were more likely to comply with the privacy protection laws, perhaps because popular websites were likely to be maintained by organizations with the resources to have legal departments, and perhaps because complying with the law also serves as a

in this Article, we encourage policy makers to construct a regime that strikes a balance between rules and standards to make the new data protection regime specific enough to address discrete problems and open-ended enough to allow it to evolve.

1. Baseline Regulation

We recommend a regime that includes baseline privacy protections that would set a floor for the permissible approaches of companies that handle consumer information. The variation in the approaches taken by companies in our relatively small sample underscores the need for more uniformity.

Many questions exist about the appropriate levels of baseline protections, posing interesting questions for future research. Baseline regulations should first identify minimum requirements in order to protect certain types of sensitive information. Such regulations should explicitly address the protection of personal health information, social security numbers, and financial information like bank account numbers and credit cards. The baseline regulation could also include a provision that places the risk of loss for online fraud on a cloud provider.[525] Opponents of our approach may point to the results of the Birnhack and Elkin-Koren study, an empirical study of Israeli websites that suggests that regulations setting a baseline for privacy agreements are not truly effective due to low compliance rates.[526] But the authors of that study failed to focus on enforcement, and more effective enforcement would likely improve the efficacy of such regulations.

After establishing categories of sensitive information that must receive special protection, the next question concerns what minimum requirements should be included to protect consumer information. Baseline regulations might, for example, include

---

signal to consumers that the company is more reliable. *See id.*

525. *See* Soghoian, *supra* note 5, at 378–79 (noting that cloud computing providers do not have the same incentive as banks and online merchants to protect customers from online fraud because the banks and online retailers legally bear the risk of loss instead of the consumer).

526. *See* Birnhack & Elkin-Koren, *supra* note 108, at 383 (describing how the authors "found that some areas of the law are simply irrelevant in the daily practices of websites").

requirements for data security. End users are generally ignorant of many data protection issues, so there is not sufficient market demand for firms to pay more attention to security issues like the need to encrypt information.[527] This could be addressed using regulations that require data to be encrypted.[528] We envision two primary options for security baseline regulation: language requiring the use of "best available security technology," or language requiring the use of "industry standard security technology." The comparison of these two options is another possible direction for future research.

We further suggest that baseline regulations should also address issues related to data breaches. First, the regulation should include security breach notification requirements in order to give users the information necessary to assess the negative consequences of a cloud vendor's security failures.[529] Second, there should be viable private causes of action for data breaches to address the current problem of consumers not having standing to sue a company after a breach in the absence of a distinct injury like identity theft. Some scholars have suggested finding companies strictly liable for data leaks,[530] creating a new common law tort based on the use of Fair Information Practices,[531] and

---

527. *See* Soghoian, *supra* note 5, at 380 (stating that many consumers know very little about data encryption and describing how this provides "no incentive to [devote resources] to something for which most customers have not expressed a want").

528. *See id.* at 382–83 (proposing that government regulators require cloud service providers to use encryption just as this has already been done in the banking and health industries).

529. Martin suggests a similar approach. *See* Martin, *supra* note 44, at 313 ("Congress should create new breach notification requirements that allow users to assess the exposure, damage, and operational costs of any security failures on the part of a cloud vendor.").

530. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 245 (2007) (suggesting "a Rylands strict-liability model to address the hazards of leaking databases").

531. *See* Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 140 (2006) (suggesting "a new common law tort . . . to force reform and accountability . . . and to provide remedies for individuals who have suffered harm to their core privacy interests" and stating that this tort "borrows from . . . the Fair Information Practices from the Privacy Act of 1974").

imposing liability for breach of trust if a company misuses information.[532] Imposing fiduciary obligations in some circumstances may also provide adequate private causes of action in response to security breaches. It is possible that some of the issues relating to information privacy could be resolved through the common law, such as if privacy tort law were expanded to take intangible harms into account, including the harm from the disclosure of data that is not embarrassing.[533] We argue that an emphasis on private enforcement options would preserve the viability of the market by limiting excessive legislative oversight of business practices.

B. Data Control

The most important part of our proposal for a new legal regime that sets a floor for the use of data by private companies concerns data control, which we have defined in this Article as encompassing the ideas of data mobility and data withdrawal. In the cloud context, there are two sets of information that we are concerned about: PII, and what we call "course-of-business" data that is stored as part of the customer's use of the service. Related to the use of PII, we are also concerned about secondary use of such information, including secondary use by third parties. We further argue that data mobility and data withdrawal provisions as described below would attract consumers who are more risk averse and who would not use these services in the absence of these protections, thus leading to a net benefit to the industry.

---

532. *See* Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1288 (2000) ("[A] rubric based loosely on breach of confidence might persuade courts to recognize at least limited data privacy rights.").

533. *See* Richards & Solove, *supra* note 1, at 1922–23

> Courts can readily understand the harm caused by the disclosure of a naked photograph of a person, but they struggle in locating a harm when non-embarrassing data is disclosed or leaked. A broader understanding of harm is needed in order for the privacy torts to apply to the extensive gathering, dissemination, and use of information by various businesses and organizations.

Thus, these provisions should be mandatory, and the regulations should prevent parties from contracting around these terms.

1. Personally Identifiable Information

Baseline privacy regulations should protect the ability of consumers to control the use of their PII in the cloud. The security of PII should be paramount to prevent fraud and identity theft. This part of our recommendation is by no means revolutionary, however, because privacy policies are centered on protection of PII, and most privacy theorists focus on PII as the class of information that must be afforded the most protection.

We also encourage discussions of PII to consider the commodification of data. If consumers are free to use their PII as a form of currency, disclosing it to obtain desired services, should there be limits on what information consumers can trade? If privacy is viewed as property, and property itself is really a bundle of rights, there may be some types of information where it would be against the best interest of society to permit the free trade thereof. For example, the relationship between doctors and patients is typically viewed as sacrosanct. We thus suggest that personal health information is one category of information that service providers outside this circle would not be able to seek under our proposed legal regime.

The problem of reidentification raises additional issues because it can lead to anonymized, descriptive information about the consumer being reattached to the consumer's identity. While we would not recommend a regime that stifles innovation and academic creativity, a legal regime to protect PII in the cloud also needs some forward-looking provisions addressing the possibility that reidentification science could lead to threats to personal privacy in the future. These provisions, for example, might prohibit the use of public records for reidentification purposes unless the user certifies compliance with some form of privacy standard.

2. Secondary Use

Secondary use of PII is another very important consideration. Those who argue for limitations on secondary use suggest that the use of data should be limited to the purpose for which it was initially collected, absent further consent being obtained.[534] Existing rules prohibiting secondary use include legal ethics rules that prohibit a lawyer from using client information for a purpose unrelated to the interests of the client, and restrictions in the Fair Credit Reporting Act that prohibit an employer who obtains an employee's credit report from using this information for nonemployment purposes.[535]

Once PII is properly collected, we suggest imposing further limits on secondary use of the PII. One option is to give the consumer the ability to restrict secondary use of her PII. Privacy policies often give the customer the ability to access and amend PII stored on the collecting company's system, so requiring these provisions to address secondary use would likely not be excessively burdensome.

However, privacy policies do not give consumers control over PII given to third parties unconnected to the consumer. To address this third-party problem, the baseline regime should guarantee consumers a right of data withdrawal. By permitting data withdrawal when a consumer's information is being used in a way that goes against the wishes of the consumer, we secure the right of consumers to control their data and feel more secure.[536] To solidify this data withdrawal right, we recommend

---

534. *See* Richards, *supra* note 114, at 1190 (defining secondary use prohibitions as "the requirement that data collected for one purpose may be used for that purpose only, absent consent"); Solove, *Taxonomy, supra* note 111, at 521 ("'Secondary use' is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent.").

535. *See* Richards, *supra* note 114, at 1190–91. However, Solove argues that the restrictions in the Fair Credit Reporting Act do not adequately restrict secondary uses of covered information. See SOLOVE, DIGITAL PERSON, *supra* note 2, at 67–68 (describing how effective lobbying by the credit reporting industry led to an exemption for "names, addresses, former addresses, telephone number, SSN, employment information, and birthdate").

536. Our proposed right of data withdrawal is ideologically similar to the proposed "right to be forgotten" in European privacy law, which is supported by the European Commission, though many worry that a right to be forgotten is

giving consumers the ability to serve a notice-and-takedown order on third parties to require the removal of the consumer's PII from the third party's system. We recognize that consumers may have difficulty obtaining information about the secondary use of their PII, but argue that combining a notice-and-takedown regime with controls to enable meaningful informed choices could potentially address some of the problems relating to the secondary use of PII by third parties. Designing controls to enable meaningful informed choices is outside the scope of this Article, but it is an important and related issue that should be the subject of further study.

Under a regime allowing for notice and takedown of PII, a party who wants his PII removed from a specific service could contact the operator of that service to (1) assert his rights in the PII, and (2) request that the PII be taken down. At that time, the operator would have to comply and notify the original submitter of the information about the takedown. The original submitter would then have an opportunity to contest the takedown and assert that the PII was not wrongfully made available. This proposal of a notice-and-takedown approach is patterned after the procedures of the Digital Millennium Copyright Act (DMCA),[537] which permits copyright owners to serve a notice on a website when infringing material has been posted.[538] Our notice-and-takedown proposal would permit consumers to request that entities take down information that was either posted by the consumer and then republished elsewhere, or that was derived from information posted by the consumer. The notice and

---

impossible to enforce. *See* European Comm'n, *Commission Welcomes European Parliament Rapporteurs' Support for Strong EU Data Protection Rules* (Jan. 8, 2013), http://ec.europa.eu/commission_2010-2014/reding/pdf/m13_4_en.pdf (last visited Feb. 3, 2013) (on file with the Washington and Lee Law Review). Our proposed model for a right of data withdrawal, however, operationalizes this difficult concept by drawing from the notice-and-takedown procedures of the Digital Millennium Copyright Act (DMCA).

537. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

538. *See* 17 U.S.C. § 512(c)(3) (2006) (establishing a "notice and takedown" procedure to handle allegations that content on a host website infringes an owner's copyright).

takedown approach could apply to secondary use by the original entity entrusted with the information, as well as to third parties.

Another option we suggest is for the baseline regulation to declare that some information, like personal health information, should never be tradable. Thus, someone within the necessary circle encompassing the doctor–patient relationship would not be able to trade health information, even if it is anonymized, to marketers seeking to create profiles based on health needs. If some information is not tradable but others are, this can still leave room for many different business models to survive, as long as a minimum level of privacy and security are provided.

3. Course-of-Business Data

Recommendations about PII are very common in the privacy literature, but the information disclosed to cloud providers goes far beyond PII. One of the elements that we think deserves more discussion is the control of what we call "course-of-business" data, which consumers store with cloud providers as part of the service. Many cloud services permit customers to store photos, writings, and business data in the cloud. The storage of this information is often the customer's purpose for using this service to begin with, whereas the transfer of PII is typically incidental to the rendering of service. Because the storage of this information is essential to the service, the terms relating to such storage should be explicit as a condition of the contract between the parties.

In Part II, we noted that many private actors have called for improved transparency and control in the cloud. In the cloud context, the question of data control does not only involve targeted advertising, but also the importance of data mobility so that customers would not lose everything if a service provider became inoperable or if the data had to be moved to a new service provider.[539] However, as our analysis of TOS agreements and privacy policies showed, companies often do not address the handling of such data after the contract has terminated.

---

539. Martin, *supra* note 44, at 286 ("Any solution needs to incorporate guarantees that data owners would be able to gain control of their data in a usable form should their service providers become inoperable.").

Above we emphasized the data withdrawal aspect of data control. The right of withdrawal may have less application to course-of-business data like writings and photos because such data may be protected by intellectual property law (IP law), and therefore a right of withdrawal may be duplicative of IP law protection. However, for course-of-business data entitled to lesser IP law protection, like databases, the right of withdrawal via notice and takedown should be available.

More importantly, the baseline regulations must require a minimum level of protection to ensure data mobility. This means that data must be converted to an acceptable format before being delivered to a departing customer, such that the customer is not locked in to a particular service provider, and could easily move their data from one provider to another. Data mobility focuses on the access and consumer choice aspects of data control and would facilitate market transactions by enabling customers to move their data freely between competing services. What happens if the customer decides for any reason that she wants to use the cloud services of a competing provider? Is a user's course-of-business data stored in a proprietary format such that the user encounters a "lock-in" problem if she decides she wants to change providers? Currently, privacy policies and TOS agreements often may not address these issues at all. As part of the legal regime that we propose, format transparency would be required, and providers would also be required to include terms addressing end-of-relationship handling of course-of-business data. Under our proposed regime, a company could still store the data in a proprietary format, but would be required to convert the data to a generally accepted format upon account termination to enable the data to be easily moved to a competing service.

Data mobility is important because it allows consumers to more fully participate in the features and services that cloud providers offer. The importance of data mobility in the cloud can be emphasized by analogizing to mobile phone numbers. In November 2003, an FCC regulation became effective that required cell phone carriers to allow numbers to be ported from one carrier to another.[540] There was a great deal of resistance on

540. *See* Telephone Number Portability, First Report and Order and Further

the part of service providers that claimed that this rule would be too costly to carriers and might not be beneficial to consumers.[541] The FCC, however, concluded in 2006 that the number portability requirement did not significantly increase "wireless churn," and did in fact have a positive impact on service quality due to the need that it created for carriers to devote extra effort to customer retention.[542] We expect that a data mobility requirement may be met with the same initial resistance as the wireless number portability requirement, but that like wireless number portability, data mobility requirements will have a net positive effect on both the industry and on consumers. By allowing consumers to "port" their phone numbers into another provider's system, cellular subscribers are better equipped to participate in the market because such porting greatly reduces costs that might otherwise be associated with switching mobile service providers.[543] Similarly, data mobility in the cloud would facilitate consumer participation and reduce transaction costs for consumers when moving from one provider to another.

Protection of course-of-business information could also be achieved through some application of the principles surrounding

---

Notice of Proposed Rule, 11 FCC Rcd. 8352 (1996). The first compliance date was set for June 30, 1999, but after two requests for forbearance, the agency pushed the deadline for compliance to November 24, 2003. *See* Cellular Telecommunications & Internet Ass'n v. F.C.C., 330 F.3d 502, 503–04 (D.C. Cir. 2003).

541. *See* Caron Carlson & Carmen Nobel, *Carriers Resist Porting Numbers*, EWEEK, Apr. 21, 2003, at 20 (describing how "[w]ireless carriers [were] looking for relief from a requirement that would . . . allow cell phone customers to keep their numbers when they change phone companies").

542. Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, 21 FCC Rcd. 10,947, 11,006 (2006)

> [T]he advent of porting . . . did not lead to a significant increase in wireless churn, but did appear to have had a positive impact on service quality by inducing carriers to engage in aggressive customer retention efforts . . . . Significantly improved retention efforts (better deals on upgrade handsets, incentives for signing longer contracts, better customer service, and higher network spending) following the implementation of local number portability . . . have led to lower churn rates . . . (citations and internal quotations omitted).

543. *See* Carlson & Nobel, *supra* note 541 (noting that the extra cost associated with changing a cellular phone number was sometimes viewed as the most important reason to stay with the same provider).

the law of confidentiality. Confidentiality as a concept is related to privacy, but primarily arises in the context of contracts between private parties. When fiduciary relationships exist, the law often recognizes obligations to keep information confidential. Solove has pointed out the potential application of fiduciary relationships in the privacy context.[544] If elements of fiduciary relationships were integrated into the customer–cloud provider relationship, this would impose on the providers an obligation to keep not only the customer's PII secure, but other data stored on the provider's servers as well. Consumers could obtain stronger protections by opting into a fiduciary relationship with the service provider for a price. The consumer would thus get a guarantee that if the service provider acts badly, the consumer has a right of action against them. This differs from Solove's proposal because we are more focused on consumer choice than on making fiduciary relationships into a default rule.

VII. Conclusion

Privacy issues online are not going to disappear overnight. Changes to the law are necessary to facilitate optimal market development that takes into consideration the autonomy of consumers in controlling their personal information. Foucault's view of Bentham's Panopticon as a metaphor for power relations in society is even more apt today than when Foucault was originally writing. The market forces peering into private lives may not be doing so with malicious intentions, but the corresponding decrease in consumer control of their personal information is nonetheless harmful.

In this Article, we have examined issues relating to cloud computing through the lens of privacy theories and privacy law. In analyzing a sample of terms of service agreements and privacy policies, we have concluded that these documents have potentially serious implications for the rights of consumers who agree to them without reading the terms.

---

544. *See* SOLOVE, DIGITAL PERSON, *supra* note 2, at 103 (making the "radical proposal" that the law should recognize a fiduciary relationship when a company collects and uses personal information).

Ultimately, we recommend the implementation of baseline regulations to guarantee some minimum level of protection for consumers in the cloud. These regulations should emphasize the importance of preserving consumer control of their data, and these control mechanisms should focus on data mobility and a right of data withdrawal. Data mobility will require cloud providers to make consumer data available in a generally acceptable format such that consumers can freely move their own data from one provider to another in the interest of maintaining a healthy, competitive marketplace. For data withdrawal, we propose a notice-and-takedown approach patterned after similar provisions in the DMCA, which would permit a consumer to request that entities take down his personal information.

Our proposal raises a number of interesting new research questions. One of the most interesting problems is the effect that our proposals would ultimately have. Once the efficiency of the market is protected and consumers are in control of their data, would there actually be any statistically significant changes in consumer behavior? At the end of the day, if consumers are empowered to control their data, but behavior is largely unaltered, this may indicate that the current state of the market is actually optimal for society. However, the uncertainty that currently exists with regard to data ownership is harmful to consumer autonomy and makes it impossible to conclusively determine the optimality of the current regime. Thus, reduction of this uncertainty is essential to protecting the interests of consumers, and sufficient reduction will likely require some degree of regulatory intervention. We posit, however, that the degree of this regulatory intervention could be very modest, with narrow goals focusing on minimum protections and consumer choice, thus balancing the need to protect consumers with the need to preserve market vitality.