Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery

Derek S. Witte

John Marshall Law School

Follow this and additional works at: https://scholarcommons.sc.edu/sclr

Part of the Law Commons

Recommended Citation


This Article is brought to you by the Law Reviews and Journals at Scholar Commons. It has been accepted for inclusion in South Carolina Law Review by an authorized editor of Scholar Commons. For more information, please contact dillarda@mailbox.sc.edu.
BLEEDING DATA IN A POOL OF SHARKS: 
THE ANATHEMA OF PRIVACY IN A WORLD OF DIGITAL SHARING AND 
ELECTRONIC DISCOVERY

Derek S. Witte*

I. INTRODUCTION .................................................................................................................... 718

II. WE ARE ALREADY BLEEDING PERSONAL DATA .................................................. 722

   A. Individual Consumers Share Their Personal Data Knowingly and
      Unknowingly Through Social Networking Sites like Facebook and
      Web-Based Service Providers like Google ......................................................... 722

   B. Businesses and Consumers Also Share the Contents of Their
      Computers and Digital Devices by Agreeing to Use Cloud Storage... 728

   C. Our Information Is Being Tracked and Stored, Without Our
      Knowledge and Consent, by the Web sites We Visit, Search Engines
      We Use, and the Data-mining Companies Who Profit from Scraping
      Our Data from the Publicly Available Sources .............................................. 731

   D. We Are Constantly Sharing Data About Our Whereabouts Through
      Our Mobile Phones and Personal GPS Devices........................................... 734

III. PRIVACY MATTERS: IF WE CEDE OUR RIGHT TO PRIVACY TO THE

      MARKETING COMPANIES AND DATA MINERS, WE MAY UNWITTINGLY

      loose OUR RIGHT TO PROTECT OURSELVES FROM UNWARRANTED

      GOVERNMENT INTRUSION ........................................................................... 738

IV. LAWMAKERS MUST INTERVENE TO PROTECT U.S. CITIZENS FROM

      COMPLETELY LOSING THEIR FUNDAMENTAL RIGHT TO PRIVACY .......... 742

   A. The Current Laws Do Not Create a Comprehensive Right to
      Privacy for U.S. Citizens ............................................................................. 742

   B. The Stored Communications Act Should Be Amended or Replaced
      Because It Is Ineffective ............................................................................. 748

   C. Congress Should Pass a Comprehensive Privacy Statute, Similar to
      the 2011 Bill Proposed by Senator McCain and then-Senator Kerry.. 750

   D. In Addition, the Judicial Conference of the United States and the
      Committee on Rules of Practice and Procedure Should Propose
      Amendments to the Federal Rules of Civil Procedure to Account for

*Formerly a full-time Professor at the Thomas M. Cooley Law School where he taught E-
Discovery and Contracts, Professor Witte is currently responsible for the Advanced Discovery
Techniques class at the John Marshall Law School in Chicago, Illinois. He also works on an “of

counsel” basis for Talcott Franklin, P.C., where he runs the firm’s e-discovery practice group and

assists with complex commercial litigation out of his Grand Rapids, Michigan office. In addition,

Professor Witte practices as a litigator on an of-counsel basis with local West Michigan firms.

Professor Witte would like to thank Lauren Formica, a J.D. candidate at the Washington & Lee

University School of Law, for her invaluable research assistance on this Article.
In today’s society, many people share their deepest secrets and personal thoughts on Facebook and other social media sites. Most believe that they are only sharing with a private few, but what happens when nearly everyone in a person’s life is on Facebook? In his *Time* article on the “2010 Person of the Year,” Facebook founder Mark Zuckerberg, Lev Grossman eerily predicted:

The bigger social networks get, the more pressure there is on everybody else to join them, which means that they tend to pick up speed as they grow, and to grow until they saturate their markets. It’s going to get harder and harder to say no to Facebook and to the authentically wonderful things it brings, and the authentically awful things too.

It seems the only mistake George Orwell made was in supposing that “Big Brother” would have to take our freedom from us against our will. Facebook believes we will hand it over willingly. If we all entrust our information, thoughts, and personal data to social networking companies and other information hungry Internet sites, we will be sharing not only with our friends but also with our foes.

2. See id.
4. George Orwell is an English author, well known for his novel *Nineteen Eighty-four* (titled 1984 in later collections). See George Orwell, *Biography*, http://www.biography.com/people/george-orwell-942983 (last visited Feb. 10, 2013). *Nineteen Eighty-four* presents a bleak vision of the world, divided into three oppressive nations. *Id.* In the novel, Orwell imagined a world in which the government controlled every detail of a person’s life, down to his private thoughts. See id. “Big Brother” is the face of the oppressive political party, symbolizing the vagueness of authority’s power and its inescapable presence. See GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949).
Many consumers do not realize that the information stored on Facebook’s servers or iCloud is available to third parties. They only vaguely understand that by using Google Maps on their iPhones, they are revealing their location to a third party, or that by using the Internet, they are downloading corporate digital spies in the form of cookies and beacons. Because consumers do not grasp how vulnerable their information is, few have taken measures to safeguard their information. Consumers do not realize they should attempt to bargain for privacy, rather than simply giving it away. Unfortunately, however, consumers have little to no bargaining power with large companies like Apple or Google. Therefore, courts, legislators, and rulemakers should step in to protect consumers from unwanted privacy intrusions, specifically through discovery in litigation.

Consumers are not the only ones who should be concerned, however. Corporations are now using cloud storage to store their electronic records. Companies can enter into a contract with a third-party storage company and then house their documents, some of which are highly confidential, on the third-party’s servers for a price. Companies avoid the cost of purchasing and maintaining their own servers, and they save money by agreeing to pay only for the amount of storage used. Individuals who use the cloud can carry lightweight, high-performance tablets and phones that are not bogged down with heavy storage capacity. But there is a catch: customers must hand over custody

7. See generally id. (discussing how Google uses cookies to collect and store information).
12. See Hearing, supra note 11, at 14; Gilbert, supra note 11, at 1.
13. See Hearing, supra note 11, at 14; Gilbert, supra note 11, at 1.
14. See id.
of their precious data. What happens when a third-party data storage company receives a subpoena or an investigatory demand? Worse yet, what happens if a consumer has intentionally or unintentionally agreed to allow the cloud provider unlimited access to his information through the data storage contract?

Whether it is due to consumers’ increasing demand for lightweight and affordable high-performance mobile devices, companies’ hesitancy to invest in their own expensive servers, consumers’ desire for the flexibility of web-based email, such as Gmail or Yahoo! mail, or powerful corporations’ unwillingness to store and dole out data for profit unless we grant them access to our valuable personal information in return, there is no dispute that, as a country, we are bleeding personal data. We bleed data by saving our emails, correspondence, records, songs, and books on other people’s computers. Consumers are giving their information to third parties because it is convenient and cheap to have someone else carry their pile of papers.

Some consumers do not even realize they are forfeiting their personal information. Many fail to question where those emails in their Gmail inbox or photos on their Facebook page actually reside. In the rush to embrace every new piece of hardware and software, people do not consider the unintended consequences—some legal, some practical. Although there may be benefits to allowing Google, Microsoft, or some entrepreneurial storage company to bear the burden and cost of buying the “big iron” (servers as far as the eye can see), most consumers have not paused to consider what might happen after they hand over their data.

If, as a country, we are going to allow third parties to gather, store, and even broker our personal information and documents for a profit, then the law must adapt to protect both individuals and businesses from completely losing their rights to privacy.

15. See generally Alberto G. Araiza, Note, Electronic Discovery in the Cloud, DUKE L. & TECH. REV., no. 8, 2011, at 1, 14 (“Cloud providers are custodians of the ESI they hold in data centers.”).
16. See, e.g., Daniel J. Gervais & Daniel J. Hyndman, Cloud Control: Copyright, Global Memes and Privacy, 10 J. TELECOMM. & HIGH TECH. L. 53, 78–79 (2012) (“The . . . average users do not know how personal information is used after it enters the Cloud . . . .”)
17. See generally id. at 76–77 (posing questions about what happens to information entered online that the average consumer does not consider).
18. See id. at 78–80 (describing both legal and practical consequences of sharing personal information in clouds).
19. “Big Iron” has been described as “high-priced products characterized by heavy-duty packaging, complex interconnections, large scalability, and a multitude of software features such as de-duplication and compression” and is known for doing “its main job well, no question; data rarely gets misplaced.” Jim O’Reilly, The White-Box Threat to Big Iron Storage, DATACENTER ACCELERATION (Oct. 16, 2012), http://www.datacenteracceleration.com/author.asp?section_id=2559&doc_id=252489.
20. See, e.g., Gervais & Hyndman, supra note 16, at 78–79 (“The . . . average users do not know how personal information is used after it enters the Cloud . . . .”)
At their best, those who govern use the rule of law to protect those who cannot protect themselves, to check unchecked power, and to protect our fundamental rights. The fundamental right of privacy is currently under attack. Ordinary citizens seem to be left with no choice but to feed the ever-growing data stream of contemporary commerce and give up any remnants of privacy, all in exchange for an ever-shrinking piece of the pie. If you want a mobile phone, then the mobile phone provider may own the content of your calls. If you want to store information on the cloud, then the storage company can read and maybe even sell your personal information. If you want to use a debit card, then the bank can store and sell your buying patterns. If you want to use the Internet, then each click or scroll is tracked and compiled by strangers. Finally, if the government wants all of the information you have given to Apple and Google and sent to the cloud, they can have it.

This is not the future; this is today. Courts and lawmakers must overcome their Luddite ways and step forward to protect the fundamental right of privacy before it is lost through unconscionable consumer contracts and constant unscrupulous data-mining.

This Article will discuss how we are already bleeding personal data. Specifically, Part II explores how individual consumers share their personal data knowingly and unknowingly through social networking sites like Facebook and web-based service providers like Google. It analyzes how both businesses and consumers also share the contents of their computers and digital devices by agreeing to use cloud storage. Furthermore, it discusses how we are constantly sharing data about ourselves and our whereabouts through mobile phones and personal Global Positioning System (GPS) devices.

Part III of this Article suggests that if we are to cede our right of privacy to the marketing companies and data miners, we may unwittingly lose our right to protect ourselves from unwanted government intrusion. Because the current laws do not create or protect a comprehensive or coherent right to privacy, Part IV argues for lawmaker intervention to protect United States citizens from losing their right to privacy in life and in the courtroom. Specifically, Part IV argues


22. See, e.g., Eric Lichtblau, More Demands on Cell Carriers in Surveillance, N.Y. TIMES, July 9, 2012, at A1 (describing how cell carriers turn over upon request “text messages, caller locations and other information”).

23. See, e.g., iCloud Terms and Conditions, supra note 5 (“You [the user] further consent and agree that Apple may collect, use, transmit, process and maintain information related to your Account . . . .”).


25. See Privacy Policy, supra note 6.

that the Stored Communications Act is ineffective and should be amended or replaced.

I will conclude with two rational solutions: First, for Congress to pass a comprehensive privacy statute, similar to the 2011 bill Senator McCain and then-Senator Kerry proposed to define our privacy rights. Second, the Judicial Conference of the United States, through amendments to Federal Rules of Civil Procedure 26 and 45, should implement a contemporary discovery rule safeguarding private information in litigation.

II. WE ARE ALREADY BLEEDING PERSONAL DATA

Acclaimed social-data expert, Andreas Weigend, Ph.D., recently stated, "Now, many of us reveal on Facebook what the KGB couldn’t get out of us with torture." Individuals are sharing that data with one another with greater and greater frequency. Thus, before analyzing a legal framework for contemporary privacy, it makes sense to first understand the types of personal data being created and how individuals and corporations are sharing that data.

A. Individual Consumers Share Their Personal Data Knowingly and Unknowningly Through Social Networking Sites like Facebook and Web-Based Service Providers like Google

Today, individuals commonly share data about themselves through the various services and applications of social networking and Internet productivity sites, like Facebook and Google. Because people voluntarily sign up for these services and intentionally decide what to share and with whom, it would seem that Facebook and other similar sites should not be a threat to privacy. However, due to Facebook’s misleading privacy settings and ever-changing privacy policy, its customers are often confused about what they are actually sharing and exactly with whom they are sharing it.

This problem has reached epic proportions. Recently, the Federal Trade Commission (FTC) threatened an enforcement action against Facebook, which Facebook, in turn, agreed to settle. Negotiations began in November 2011.

29. See id.
30. See, e.g., Fowler, supra note 1 (describing two Facebook users as “casualties of a privacy loophole”).
and culminated in an August 2012 settlement. The FTC required Facebook to create a “comprehensive privacy policy” and prohibited it from making any changes that would overrule a user’s personal privacy preferences. The FTC’s decision does not bar Facebook from creating a personal privacy policy that allows it to use its customers’ personal data; it only requires that Facebook be transparent and consistent. Thus, this decision promises to be no more than the opening salvo over Facebook’s bow.

Likewise, Google reached a compromise with the FTC under a similar threat of an enforcement action. As a result, Google revised its privacy policy and consolidated over sixty disjointed policies into one. The synthesized policy, effective March 1, 2012, reveals that Google has no interest in maintaining consumer privacy. The new policy may be easier to read and understand, but the message Google sends is frightening: if you use Google, then Google owns your information and will use it how they see fit and profitable. Both the director of the FTC and over half of the state attorney generals are highly critical of Google’s new policy.

The FTC’s criticism was validated. On August 8, 2012, the FTC charged Google with misrepresenting privacy features. Google settled the case for $22.5 million. Jon Leibowitz, Chairman of the FTC, commented,
The record setting penalty in this matter sends a clear message to all companies under an FTC privacy order. . . . No matter how big or small, all companies must abide by FTC orders against them and keep their privacy promises to consumers, or they will end up paying many times what it would have cost to comply in the first place.44

Google’s privacy-agreement breach is a warning that despite what the black letter privacy setting says, an entity may not be in compliance. Furthermore, the FTC’s sanction is minuscule in comparison with Google’s net worth.45 The FTC’s efforts at cutting back against Big Brother may be a needle prick in a giant’s side.

Yet, despite the abundance of privacy breaches, millions of people continue to share information voluntarily with third-party information brokers, including Facebook, Google, Yahoo!, and Twitter.46 These third parties are not keeping this data private; they are sharing it with others in a myriad of ways.47 As Mark Zuckerberg stated in Time, “technology usually wins with these things,” to which Time followed, “And he’s right: the Internet was built to move information around, not keep it in one place, and it tends to do what it was built to do.”48 The Internet is moving personal data around swiftly, notwithstanding privacy settings or notions of privacy.49

In civil litigation, parties are being required to produce the contents of their “private” Facebook pages without regard to their privacy settings.50 On November 7, 2011, a Pennsylvania court posed the question: “But what if the people in your life want to use your Facebook posts against you in a civil lawsuit?”51 The court then held they can.52 It ordered the plaintiff to “turn over to Defense counsel her Facebook username email and password within 14 days

44. Id.
46. See generally Fowler, supra note 1 (discussing people’s willingness to share information on Facebook despite issues with user privacy).
47. See, e.g., Privacy Policy, supra note 6 (giving examples of how Google shares information with others).
48. See Grossman, supra note 3, at 68 (internal quotation marks omitted).
49. According to Grossman, 10,000 new web sites integrate with Facebook each day, allowing for greater access to information than ever before. See id. at 72.
50. See Equal Emp’t Opportunity Comm’n v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434, 436, 437 (S.D. Ind. 2010) (“[A] person’s expectation and intent that her communications be maintained as private is not a legitimate basis for shielding those communications from discovery.”); see also Bass v. Miss Porter’s Sch., No. 3:08cv1807 (JBA), 2009 WL 3724968, at *1-2 (D. Conn. Oct. 27, 2009) (ordering plaintiff to produce for defendants an over 750-page document chronicling Facebook activity); Ledbetter v. Wal Mart Stores, Inc., No. 06 cv 01958, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009) (finding that information from Facebook and MySpace were properly within a subpoena).
52. See id. at 2.
of the date of [the] Order," and to "not delete or otherwise erase any information on her Facebook account" for thirty-five days.\textsuperscript{53} The court entered this order because the defendant had "a good faith belief that information on [plaintiff's] Facebook profile is relevant to [defendant's] defense . . . ."\textsuperscript{54} In this opinion, the court blows a gigantic hole through the Stored Communications portion of the Electronic Communications Privacy Act (ECPA) by holding that the statute only applies to third-party subpoenas, not direct requests to a party during civil litigation.\textsuperscript{55}

Facebook and other social networking sites are also handing over data in criminal cases.\textsuperscript{56} Watchdog groups have released internal Facebook documents outlining how and when Facebook shares the "private" information on someone's Facebook page with law enforcement.\textsuperscript{57} Facebook's law enforcement guidelines seem to allow an ad hoc, case-by-case analysis.\textsuperscript{58} In its 2010 policy, Facebook informed law enforcement that it would respond to any informal request and potentially provide the following data about the Facebook user: User Identification Number; Email Address; Registered Mobile Number; Profile Contact Information; Status Update History; Shares; Notes; Wall Posting; Friend Listing, with Friend's Facebook ID; Group Listing, with Group's Facebook ID; Future and Past Events; and Video Listing, with filename.\textsuperscript{59} Facebook also stated that it would share "user photos" and "[p]rivate [m]essages if retained."\textsuperscript{60} In 2010, Facebook's law enforcement policy did not actually require any particular criminal subpoena or warrant and simply provided that "[w]e review each request for records individually and prioritize requests based upon case circumstances and other factors not always obvious from the formal process."\textsuperscript{61}

To date, no one has leaked Facebook's 2012 policy. However, Facebook currently states on its "Information for Law Enforcement Authorities" web page that it "will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve."\textsuperscript{62} Though vague, this statement suggests that law enforcement can

\textsuperscript{54.} Largent, No. 2009-1823, at 2.
\textsuperscript{55.} See id. at 12 (citing Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006)).
\textsuperscript{56.} See generally FACEBOOK, INC., FACEBOOK LAW ENFORCEMENT GUIDELINES (2010) (providing information in an internal Facebook report regarding when Facebook records will be provided to law enforcement officers).
\textsuperscript{58.} See FACEBOOK, INC., supra note 56, at 3.
\textsuperscript{59.} See id. at 4.
\textsuperscript{60.} See id.
\textsuperscript{61.} Id. at 3.
\textsuperscript{62.} Information for Law Enforcement Authorities, supra note 57.
access virtually anything on the Facebook servers as long as a request has been made with some particularity and authority.

The increasing number of litigants coveting Facebook discovery has prompted Facebook to require formal discovery procedures.\(^{63}\) A litigant may discover information by submitting one of three documents:

A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 U.S.C. Section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es), and a recent login IP address, if available.

A court order issued under 18 U.S.C. Section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.

A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent State warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, wall posts, and location information.\(^{64}\)

In addition, Facebook “interpret[s] the national security letter provision as applied to Facebook to require the production of only 2 categories of information: name and length of service.”\(^{65}\)

It is quite possible that it was under the 2010 version of this same policy that Facebook supposedly handed over information relating to those of its users who supported WikiLeaks and Julian Assange after Wikileaks leaked a series of confidential U.S. State Department wire messages.\(^{66}\) Julian Assange and Wikileaks accused Facebook of cooperating with the federal government, calling Facebook “the most appalling spying machine that has ever been invented.”\(^{67}\)

Although easily dismissed as paranoia, these accusations and Facebook’s law enforcement policy are consistent with the form contract Facebook’s users enter into when they sign up for its services.\(^{68}\) Facebook states in its privacy policy:

---

\(^{63}\) See id.

\(^{64}\) Id.

\(^{65}\) Id.


\(^{68}\) Compare Information for Law Enforcement Authorities, supra note 57, with Data Use Policy, supra note 5 (showing the similarity between the two).
We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves, you and others, including as part of investigations; and to prevent death or imminent bodily harm. . . . We also may retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations of our terms. 69

The bottom line is that once individuals post information on Facebook, neither the courts nor Facebook itself can promise that the information will remain private and confidential. 70 So much for those improved privacy settings.

Google, a company that stores information through Gmail, Android, Picasa, Google+ (the Facebook competitor), and a myriad of other online applications, 71 is no better than Facebook at protecting or ensuring user privacy. When signing up for Google, you agree through a series of complicated hyperlinks that:

When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works, communicate, publish, publicly perform, publicly display and distribute such content. . . . This license continues even if you stop using our Services . . . . 72

Google’s privacy policy warns that, “Google processes personal information on our servers in many countries around the world. We may process your personal information on a server located outside the country where you live.” 73 If there is, or should be, any legal framework for keeping our online data private, then that framework must take into consideration how companies like Google and Facebook store and use our information.

69. Data Use Policy, supra note 5 (emphasis added).
70. See id.
73. Privacy Policy, supra note 6 (emphasis added).


B. Businesses and Consumers Also Share the Contents of Their Computers and Digital Devices by Agreeing to Use Cloud Storage

Not only are individuals and businesses placing information at risk and potentially waiving their rights to privacy by sharing bits and pieces of data with third-party sites like Facebook, some are going a step further. They are agreeing to store all of their documents—everything that would traditionally be saved on a personal hard drive, computer workstation, or company server—on third-party storage devices, or series of devices or servers, around the country and the world.74

Microsoft, for instance, encourages individual consumers to go to the cloud by boasting that it "helps customers take a key step toward better business agility, economics, and user experiences."75 Microsoft, however, tells its customers only vaguely what the cloud is.76 To Microsoft, the cloud is one's agreement to store personal documents on the "Windows SkyDrive,"77 which is not in the sky, but on Microsoft's own servers, or a series of servers around the world on which Microsoft stores information with yet another third party.78 Similarly, the new tablet and smart-phone manufacturers are not stopping to explain how a tiny affordable device can possibly access and store a myriad of files and documents while having little or no storage space of its own. Chris Anderson, Editor in Chief of Wired Magazine, explains:

Finally, the cloud shows that as more and more of our data and software lives in servers somewhere, the computers we carry with us can be less and less powerful—thinner, lighter, longer battery life. Let Google buy the big iron; you can buy the sexy aluminum and glass that's a delight to hold.79

---

74. According to the National Institute of Standards and Technology, cloud computing is a "model for enabling 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." Gilbert, supra note 11, at 18 (quoting NIST Cloud Computing Program, NIST, http://www.nist.gov/itl/cloud/ (last updated Dec. 18, 2012)) (internal quotation marks omitted).


76. See id.


Apple recently introduced iCloud, which offers to store every file on a user’s laptop, phone, and tablet at a third-party location Apple controls and owns.\textsuperscript{80} Google and Verizon are also offering their own cloud-books and thin-clients, which allow users to access all of their data and files through a high-speed device, like a tablet or phone, while storing nothing of consequence on the device itself.\textsuperscript{81}

The plain truth, however, is that the cloud is someone else’s computer. And that someone else wants to hold, and probably, own its customers’ files and data. Citizens who value privacy should be nervous, for the companies that want to store personal data on their “big iron” and simply allow users to visit the documents they create, spreadsheets they build, and books they buy are the same companies that force customers to agree to terms of service that will give these giant corporations a right to read, use, and pilfer customer data for value.\textsuperscript{82} What is worse, these are the same companies who will share personal data already in their control with law enforcement if it is in their best interest to do so, notwithstanding the law.\textsuperscript{83} Furthermore, there is little or no legal obligation for these companies to keep the information stored on the cloud private.\textsuperscript{84}

Apple’s iCloud Terms of Service provide:

You understand that by using the Service, you consent and agree to the collection and use of certain information about you . . . . You further consent and agree that Apple may collect, use, transmit, process and maintain information related to your Account, and any devices or computers registered thereunder . . . . [T]his information may be transferred to the United States and/or other countries for storage, processing and use by Apple, its affiliates, and/or their service providers.\textsuperscript{85}

Another hyperlink away, in the Privacy Policy, Apple tells its customers that it will indeed share personal and nonpersonal information with third parties: “At times Apple may make certain personal information available to strategic partners that work with Apple to provide products and services, or that help


\textsuperscript{81} See Wireless Watch, Google Revives ‘Network Computer’ with Dual-OS Assault on MS, THE REGISTER (Dec. 13, 2010), http://www.theregister.co.uk/2010/12/13/google_revives_network_computer_again/.

\textsuperscript{82} See, e.g., iCloud Terms and Conditions, supra note 5 (“You acknowledge and agree that Apple may, without liability to you, access, use, preserve, and/or disclose your Account information and Content . . . “).

\textsuperscript{83} See id.


\textsuperscript{85} iCloud Terms and Conditions, supra note 5 (emphasis added).
Apple market to customers.¹⁸⁶ Later, the Privacy Policy provides, similar to Facebook’s Data Use Policy,¹⁸⁷ that Apple will hand over information to law enforcement whenever Apple decides it is in its best interest to do so:

It may be necessary—by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence—for Apple to disclose your personal information. We may also disclose information about you if we determine that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate.¹⁸⁸

In other words, once a person saves data on Apple’s computers, the data belongs to Apple, and Apple will use and share it as it deems fit and profitable.

Businesses are moving towards cloud storage as well.¹⁸⁹ Skeptics are rightly concerned about confidentiality and privacy.¹⁹⁰ Many scholars and critics have advised companies to approach cloud storage with caution.¹⁹¹ For instance, a New York state ethics opinion counsels attorneys to store client data with a third-party cloud vendor only after taking “reasonable care to ensure that the system is secure and that client confidentiality [is] maintained,” which includes ensuring that the online data storage provider has an “enforceable obligation to preserve confidentiality and security.”¹⁹²

Unfortunately, there is no general or all-encompassing legal duty requiring a third-party cloud vendor to keep all of your data private.¹⁹³ Certainly, a law firm could, and should, enter into a well-drafted contract with the cloud service provider; however, there is no uniform federal law, and only a few state laws, allowing a contract to supersede a validly issued criminal subpoena, or perhaps even a civil subpoena, sent directly to the third-party storage provider.¹⁹⁴

By way of further example, some have suggested that medical providers that store patient data with a third-party cloud vendor could be in violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy rules

---

86. Privacy Policy, supra note 26.
87. See Data Use Policy, supra note 5.
88. Privacy Policy, supra note 26 (emphasis added).
89. See Gilbert, supra note 11, at 1.
90. See, e.g., Cloud with a Chance of Rain, ECONOMIST (Mar. 5, 2010), http://www.economist.com/node/15640793 (describing how information technology departments at corporations are hesitant to embrace cloud storage).
91. See, e.g., Herbert B. Dixon Jr., Cloud Computing, JUDGES’ J., Spring 2012, at 36, 38 (“Murphy’s Law applies even in the cloud.”).
94. See Gilbert, supra note 11, at 29 (implying that a cloud provider does not have a uniform duty to keep information private because “different rules apply” to different types and categories of information).
because most cloud-storage terms of service would conflict with HIPAA’s requirements for medical providers to obtain a “business associates” waiver in order to disseminate information to any third party. Thus, a medical provider could be liable for disclosing patient data simply by handing it over to the cloud storage vendor. To solve this problem, a market has developed where cloud services charge a premium to use “HIPAA-secure clouds.”

C. Our Information Is Being Tracked and Stored, Without Our Knowledge and Consent, by the Websites We Visit, Search Engines We Use, and the Data-mining Companies Who Profit from Scraping Our Data from the Publicly Available Sources

In addition to the data that customers share with social networking sites, Google, and cloud service providers, individuals also share data about their Internet usage in other unlikely ways, sometimes simply by surfing the Internet. Even when we believe we are anonymously visiting web sites, data-mining companies, curious corporations, and the web sites themselves use tracking methods, cookies, and legal spyware to watch and store information about what we do on the Internet.

Web sites, or third-party companies cooperating with a web site, send a small piece of code to your computer when you visit the web site. Once a company places a cookie on your computer it can track information about you, including whether you are a returning user, the sites you visited before, and after visiting their web site, the items you view on a web site, and sometimes even the information you enter into the computer while on the web site:

96. See Sotto et al., supra note 95, at 186.
99. See generally Anne Klinefelter, When to Research Is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking, 16 VA. J.L. & TECH. 1, 4, 5–18 (2011) (citations omitted) (describing how despite people’s beliefs that their actions on the internet are confidential, a variety of tracking mechanisms exist); Christopher Maag, Don’t Track Me: The War over Online Ads Starts Now, CREDIT.COM (Feb. 2, 2011), http://blog.credit.com/2011/02/don’t-track-me-the-war-over-online-ads-starts-now (same).
101. See id.
The amount and type of information gathered by these tools is almost as varied as the number of cookies. Some might track just your IP address, which allows them to see your actual physical address, often down to the block. Others, especially super-cookies and sophisticated tools called beacons, can record everything you type when you’re online, how far down the page you scroll, and what you’re looking at when you click away.\footnote{Maag, supra note 99.}

For instance, when eBay tracks you with a cookie, it can track and store all of the items you view online, the searches you make, your address and credit card information, and more.\footnote{See Managing Cookies, eBay, http://pages.ebay.com/help/account/cookies.html (last visited Feb. 15, 2013) ("[W]e use cookies to recognize you when you sign in, to remember your preferences, and to allow you to navigate the site without having to keep reentering your password.").} These web sites claim to store the information to better serve customers when they return.\footnote{See, e.g., Cookies, Web Beacons, and Your Privacy, eBay, http://pages.ebay.com/help/account/cookies-web-beacons.html (last visited Feb. 15, 2013) (listing the ways in which the web site uses cookies to provide features and services).} However, the web sites make no promises to delete all the information they collect.

The intrusion is even greater when a third-party data-mining company installs cookies on someone’s computer and gathers information about them through a seemingly innocuous web site which has no obvious affiliation with the data-mining company. In May 2011, the European Union adopted a law that requires a user’s consent for a third party to use cookies.\footnote{See New EU Cookie Law (e-Privacy Directive), INFO. COMMISSIONER’S OFF., http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/the_guide/cookies.aspx (last visited Jan. 25, 2013). Consent, however, may be implied. See id.} Unfortunately, we have no such law in the United States. In other words, your favorite news web site, in exchange for a fee, could allow third parties to install cookies on your computer when you visit. These third parties could then study how you use the news site and generate a database of your likes and dislikes to use as they please. If this seems far-fetched, it is not. For instance, Yahoo! plainly admits that it allows third parties to install cookies on your computer in order to track your behavior online:

Yahoo! may allow certain partners to include web beacons [sophisticated cookies] within pages on the Yahoo! network of websites. Yahoo! may also share portions of our log file data, including IP address, with these partners for analytics purposes. . . . These partners aggregate information about our advertising and what you see on Yahoo! and then provide auditing, research and reporting for us and our advertisers. Yahoo! allows web beacons from and shares log file data with the following partners . . . : AdXpose, AdSafe Media,
Cookies were used for so long before anyone understood how they worked that they are now an integral part of contemporary e-commerce.107 What is frightening is “[n]obody, even the U.S. Government, knows exactly who is tracking online customers and how they’re doing it.”108 When the FTC proposed a “do not track” option for all web browsing, the Internet industry voiced its strong opposition.109 In response to the FTC’s proposal that consumers be given a right to opt out of Internet tracking, similar to their “Do Not Call” right to opt out of telemarketing, an Internet advertising spokesperson stated: “If your goal is to have a red flashing icon that says, ‘Click here to opt out of targeting,’ and to incentivize people to opt out, then we don’t share that goal.”110 The FTC tabled the bill in response to the strong opposition, under the guise that it was “still considering public comments on the report.”111 When Senator John McCain and then-Senator John Kerry proposed an online privacy bill in spring 2011, which also contained a do-not-track provision,112 the leading Internet-based companies, not surprisingly, opposed it.113 Instead, they assured Congress and the public that the industry could regulate itself.114 This bill died in committee, and no subsequent legislation has been introduced in the Senate.115

Even if lawmakers could somehow limit or prohibit the use of cookies to track an individual’s online data, data miners and web sites might still be able to track the same information by simply looking for an individual’s online digital fingerprint.116 Based on a recent study, experts have learned that a handful of very simple settings on the computers we use to access the Internet actually

107. See Maag, supra note 99, at 2 (“The thing that didn’t happen that should’ve happened is that . . . we didn’t work with the consumer to help them understand what was getting tracked,” says Steve Sullivan of the Interactive Advertising Bureau . . .”).
108. Maag, supra note 99, at 2 (quoting Eduard Goodman, Chief Privacy Officer, Identity Theft 911 (Credit.com’s sister company)) (internal quotation marks omitted).
110. Id. (quoting Mike Zaneis, Senior Vice President & Gen. Counsel, Interactive Adver. Bureau) (internal quotation marks omitted).
114. See id.
116. Peter Eckersley, How Unique Is Your Web Browser?, in PRIVACY ENHANCING TECHNOLOGIES 1, 3 (Mikhail J. Atallah & Nicholas J. Hopper eds., 2010).
create a fingerprint that can identify us as unique users.\textsuperscript{117} Using several variables, such as screen resolution, type and version of web browser, system fonts, time zone, plugins, and other settings on a computer, the watchers can run an algorithm that identifies a computer’s fingerprint when it is used to visit a web site.\textsuperscript{118} This study is alarming because most users believe they are surfing anonymously.\textsuperscript{119}

Using this technology, every time someone visits a web site, the companies monitoring the traffic could recognize the unique fingerprint and know that the individual is returning to their site. Further, if the visitor at any time identified themselves while on the web site, that site could then match his unique fingerprint to his actual identity and begin saving information about the person’s viewing history—without the use of a cookie.\textsuperscript{120} Thus, these digital fingerprints create “implications both for privacy policy and technical design.”\textsuperscript{121}

Although the world of online tracking is complex and murky, it is clear that we are sharing data about our online behavior and preferences with the sites we visit and third parties who pay to get that information. It is equally clear that there is no comprehensive legal framework for protecting the privacy of that information after it has been gathered.

\textbf{D. We Are Constantly Sharing Data About Our Whereabouts Through Our Mobile Phones and Personal GPS Devices}

Although there are many other ways that individuals create and share data about themselves than can be reasonably covered in this Article, one more category of personal data merits attention: geolocation data, one’s location on Earth at any given moment.\textsuperscript{122} Through our phones, mobile devices, personal GPS devices, and cars, we are constantly sharing information about where we are and where we have been.\textsuperscript{123} When a company or the government tracks your location, they bring to mind “Big Brother” from George Orwell’s 1984, capable of watching your every move.\textsuperscript{124} Lawmakers must take this type of data into consideration when creating a legal framework for privacy in the contemporary digital world.

\begin{itemize}
\item \textsuperscript{117.} See id. at 2 ("83.6% of the browsers seen had an instantaneously unique fingerprint.").
\item \textsuperscript{118.} See id. at 4, 5.
\item \textsuperscript{119.} See Klimefelter, supra note 99, at 4.
\item \textsuperscript{120.} See Eckersley, supra note 116, at 3.
\item \textsuperscript{121.} Id. at 15.
\item \textsuperscript{122.} Geolocation data reveals an individual’s physical location and is “obtained using tracking technologies such as GPS devices, IP geolocation using databases that map Internet IP addresses to geographic locations, and financial transaction information.” Geolocation: Risk, Issues and Strategies, ISACA, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Geolocation-Risks-Issues-and-Strategies.aspx (last visited Feb. 15, 2013).
\item \textsuperscript{123.} See, e.g., Nick Bilton, Tracking File Found in iPhones, N.Y. TIMES, Apr. 21, 2011, at B1 (describing how certain Apple products were storing users’ location data).
\item \textsuperscript{124.} See Orwell, supra note 4.
\end{itemize}
Many of the devices we use and carry constantly track our location data.\textsuperscript{125} The software and service providers on our phones purportedly ask our permission to use our geolocation information for advertising purposes.\textsuperscript{126} However, our mobile service providers track our phone’s location and store that data even when we refuse permission.\textsuperscript{127} Both Google, who is responsible for the Android mobile operating system, and Apple have recently been accused of tracking phone users’ locations even when the customers do not provide permission for them to do so.\textsuperscript{128}

What is more, the Federal Communications Commission (FCC) now requires, or is in the process of requiring, commercial mobile-services companies to be compliant with the enhanced 911 rules, which will require them, within one year of January 18, 2011, to be able to locate individual customers within 100 meters of their location in 60% of the counties where that mobile service provider does business.\textsuperscript{129}

Given that the FCC’s enhanced 911 rules mandate geolocation tracking, no one can truly opt out of location tracking. We may be able to opt out of allowing Verizon, AT&T, and others, from sharing our location information with third-party vendors and data-mining companies, but it seems that they will be required to locate us at any given time and will likely track each of us constantly.\textsuperscript{130}

Even if we were to decipher a reliable way to disable the geolocation tracking capability on our phones, the GPS devices in our cars could still track us most of the time.\textsuperscript{131} “Now you’re in a situation where, if someone has the time and expertise, they can say you drove from here to there at this speed, you parked at Whole Foods . . . then you got back in your car and drove here . . .”\textsuperscript{132}

Indeed, OnStar recently revealed that it had been storing its customers’ vehicle location information, even after the customers had terminated their OnStar service.\textsuperscript{133} Although it has back tracked on its decision to track ex-customers,

\textsuperscript{125} See, e.g., Bilton, supra note 123 (describing how iPhone were “logging users’ locations”); Chris Foresman, Google Faces $50 Million Lawsuit over Android Location Tracking, WIRED (May 1, 2011, 10:27 AM), http://www.wired.com/business/2011/05/google-faces-lawsuit/all/ (describing how Android devices cache users’ data).

\textsuperscript{126} See Foresman, supra note 125.

\textsuperscript{127} See Bilton, supra note 123 (“Law enforcement officials can already get this type of location information from cellphone companies . . .”).

\textsuperscript{128} See id.; Foresman, supra note 125.

\textsuperscript{129} See 47 C.F.R. § 20.18(b)-(1) (2011).

\textsuperscript{130} See Peter Maass & Megha Rajagopalan, That’s No Phone. That’s My Tracker, N.Y. TIMES, July 15, 2012 (Sunday Review), at 5.


\textsuperscript{132} Id. (quoting Dean Gonsowski, e-discovery counsel, Clearwell) (internal quotation marks omitted).

OnStar’s statements implicitly admit that the company certainly tracks and stores location information for current customers.134 Now, OnStar customers can pay extra money to access tracking information with which customers can track all of their family cars from a home computer.135

And, as seems to be the case with all data that can be stored, OnStar’s data likely will be stored and kept. In 2004, Dr. Robert P. Minch from Boise State University predicted: “Disclosure [of location data] will almost certainly occur in the marketplace unless prohibited or discouraged. Just as database marketing firms have offered for sale the phone numbers of virtually every resident in countries such as the U.S., it seems inevitable that location information will similarly be marketed.”136 Sure enough, by 2010, “[b]oth Google and Apple [were] gathering information ‘as part of their race to build massive databases capable of pinpointing people’s locations,’ . . . which could help them tap into a multi-billion [dollar] market for location-based services.”137 Google utilizes Google Maps for Mobile so customers may “find [themselves] on a map and then locate places nearby.”138 Google explains:

Estimating your location can be done in several different ways. Because GPS is not always available and locations derived from cell towers aren’t very accurate, Google (and other Internet companies) use publicly broadcast Wi-Fi data from wireless access points to improve our location-based services. By using signals from these access points, your mobile device is able to fix its general location quickly without using too much power.139

Unless and until information about our location is meaningfully protected from disclosure once stored, it seems likely that our mobile service providers will use the information for their benefit.

The issue of whether individuals have a right to privacy with regard to location is receiving considerable attention in criminal cases as well. The United

134. See OnStar Reverses Decision to Change Terms and Conditions, supra note 133.
139. Id.
States Supreme Court granted certiorari in a case, in which the Court of Appeals for the D.C. Circuit held that law enforcement did indeed need a warrant before placing a GPS tracking device on a suspect’s vehicle. The Seventh, Eighth and Ninth Circuit Courts of Appeals faced the same issue and concluded the opposite—that law enforcement does not require a warrant, in part because individuals in contemporary society do not have a reasonable expectation of privacy in their location. The circuit split hinged on whether individuals have a reasonable expectation of privacy in their location on earth, given the ubiquity of mobile phone and consumer GPS tracking. The issue was presented to the Supreme Court in United States v. Jones, in which the Court addressed whether the Fourth Amendment permitted warrantless tracking of individuals’ cars with GPS devices.

Unfortunately, in deciding Jones, the Court avoided the issue of whether an individual has a reasonable expectation of privacy in his location. It held that the defendant’s rights were violated, not because he had an expectation of privacy in his geolocation, but because law enforcement “physically occupied private property for the purpose of obtaining information” when it placed a tracking device on the defendant’s vehicle. The Court, therefore, never reached the issue of “expectation of privacy,” instead deciding the case solely on the, arguably arcane, right to be free from government trespass. In her concurrence, Justice Sotomayor correctly observed: “In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion’s trespassory test may provide little guidance.” In other words, the question of whether a citizen has a right to privacy from government tracking of “factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones” remains unanswered. To “remedy” the circuit split, the Supreme Court granted certiorari to the Seventh and Ninth Circuit cases, simply remanding them to determine whether they are “consistent” with Jones.

141. See United States v. Cuevas-Perez, 640 F.3d 272, 275–76 (7th Cir. 2011) vacated, 132 S. Ct. 1534 (2012); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010), vacated 132 S. Ct. 1533 (2012).
142. See Cuevas-Perez, 640 F.3d at 272, 275; Maynard, 615 F.3d at 555; Marquez, 605 F.3d at 609; Pineda-Moreno 591 F.3d at 1214.
143. 132 S. Ct. 945 (2012).
144. See id. at 948.
145. See id. at 950.
146. Id. at 949.
147. See id. at 949, 950 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).
148. Id. at 955 (Sotomayor, J., concurring).
149. Id.
Perhaps the Supreme Court surmised that a decision on whether there is a reasonable expectation of privacy in an individual’s location on Earth, would on one hand, substantially bolster, or on the other, gravely debilitate, individual privacy rights. Rather than make such a momentous decision, the Court opted to decide the case on the “constitutional minimum” required.\textsuperscript{151} A commentator present at the oral argument in the Jones case observed that some of the Justices were concerned about the Orwellian nature of geolocation tracking.\textsuperscript{152} It is encouraging that our Supreme Court does not wish to unwittingly create a Big Brother. However, it is disappointing that the Court was unwilling to face the issue head on. It seems that, for now, our privacy must be preserved through legislation or rulemaking.

III. PRIVACY MATTERS: IF WE Cede OUR RIGHT TO PRIVACY TO THE MARKETING COMPANIES AND DATA MINERS, WE MAY UNWITTINGLY LOSE OUR RIGHT TO PROTECT OURSELVES FROM UNWARRANTED GOVERNMENT INTRUSION

Our right to privacy is in danger. It may already be lost. As discussed above, we are knowingly and unknowingly bleeding data.\textsuperscript{153} The companies who claim to serve us and the government we empower to protect us use that data in unimaginable ways.\textsuperscript{154} Many individuals do not even realize how much of their information is being stored and sold for profit by, and to, third parties.\textsuperscript{155} Now that these third parties hold our data, we cannot control or predict how they might use it in the future or with whom they might share it.

Some respond by arguing that just because someone could read and compile our data, does not mean that they will—so-called security through obscurity.\textsuperscript{156} They claim that the only entities reading our emails and tracking our behavior are computers and software algorithms designed to help companies serve us more effectively.\textsuperscript{157} Thus, they argue, we should simply acquiesce to the contemporary norm of personal data gathering and storage.\textsuperscript{158} Journalist Joel Stein, in a \textit{Time} article, wrote: “[T]he more I learned about data-mining, the less...

\textsuperscript{151} See Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring).
\textsuperscript{153} See supra notes 29–73 and accompanying text.
\textsuperscript{154} See supra notes 100–21 and accompanying text.
\textsuperscript{155} See Klinefelter, supra note 99, at 4.
\textsuperscript{156} See, e.g., Joel Stein, Your Data, Yourself, \textit{Time}, March 21, 2011, at 40, 46 (believing that no human ever reads your files).
\textsuperscript{157} See id. at 42 (arguing that advertisers are “only interested in tiny chunks of information” about behavior, not an individual’s name or location).
\textsuperscript{158} See id. at 46.
concerned I was. Sure, I was surprised that all these companies are actually keeping permanent files on me. But I don’t think they will do anything with them that does me any harm."¹⁵⁹ He argues that the conveniences of modern technology outweigh the loss of privacy, "[e]specially because no human being ever reads your files."¹⁶⁰

But what Joel Stein and others forget is that plenty of flesh-and-blood beings could read your files if they chose to do so. And even those who do not read your data likely make decisions about you based upon your personal information that others have already tracked and stored.¹⁶¹ What Joel Stein also forgets is that when we lose control over our information and documents, when we lose the right to keep certain information about us truly private, we open the door to possible governmental abuse. There is a "general risk that the collection of information on individuals will upset the balance between government and individuals, resulting in a shift of power that is oppressive... ‘Accumulations of information about individuals tend to enhance authority by making it easier for authority to reach individuals directly.'"¹⁶²

Imagine a governmental official or law enforcement officer who is motivated to quiet a politically unpopular citizen.¹⁶³ Now, imagine that the government official, with a keystroke, could discover: each and every email written and received from the citizen, the citizen’s whereabouts for every minute of every day for the past year, the e-books and magazines the citizen has purchased, the web sites the citizen has visited, her friends’ identities, and more. Imagine the many ways that the government could reach the citizen and interfere with her rights to pursue life, liberty, and freedom.

Sure, some of this information may have been discoverable decades ago with the appropriate warrants and after a lot of work. But today, third parties are tracking and storing an unimaginable amount of data and compiling it in just a

¹⁵⁹. Id.
¹⁶⁰. Id.
¹⁶¹. See id. at 40 (discussing all the facts—correct and incorrect—that data-mining companies had “learned” about the author).
few locations from where it can be easily retrieved\textsuperscript{164} and used to influence us, quiet us, or threaten our constitutional rights. Our anonymity actually creates due process; without anonymity we are vulnerable to unwanted government intrusion.

As the Supreme Court held decades ago, without privacy, we lose the right to protect ourselves from government intrusion, to defend ourselves from criminal prosecution, and to demand due process.\textsuperscript{165} Although the Court in\textit{ Griswold} was only concerned with the right of citizens to protect themselves from unwarranted government intrusion,\textsuperscript{166} private “database companies are extremely solicitous to the government and actually design the databases for law enforcement use.”\textsuperscript{167} For instance, “eBay . . . revealed that it had crafted its privacy policy to maximize efficiency in responding to law enforcement requests for personal data.”\textsuperscript{168}

Thus, the distinction between governmental privacy intrusions and those committed by private third-party corporations, such as Google and Facebook, becomes meaningless. This is especially so when law enforcement has almost unlimited access to the information stored by these private third parties.\textsuperscript{169} And it seems they do. In 2001, the Federal Bureau of Investigation (FBI) analyzed whether it could use information gathered by ChoicePoint, one of the most infamous data-mining companies at the time, without obtaining a warrant or court order.\textsuperscript{170} The FBI concluded that doing so was “minimally intrusive”\textsuperscript{171} and that law enforcement “may use ChoicePoint to [its] heart’s content.”\textsuperscript{172}

The distinction between government-held and privately-held data becomes even more blurred, given the proposed association between the National Security Administration (NSA) and Google.\textsuperscript{173} The NSA is the information gathering


\textsuperscript{165} See Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (citing Boyd v. United States, 116 U.S. 616, 630 (1886)).

\textsuperscript{166} See id. at 484–85 (citing Boyd, 116 U.S. at 630; Mapp v. Ohio, 376 U.S. 643, 656 (1961)).

\textsuperscript{167} Hooofnagle, supra note 162, at 599.

\textsuperscript{168} Id. at 621 (citing Yuval Dror, Big Brother Is Watching You – and Documenting, HAARETZ (Feb. 20, 2003, 12:00 AM), http://www.haaretz.com/print-edition/features/big-brother-is-watching-you-and-documenting-1.18491).

\textsuperscript{169} See FACEBOOK LAW ENFORCEMENT GUIDELINES, supra note 56.


\textsuperscript{171} Id.


arm of the federal intelligence agencies. It is, however, a governmental entity bound to respect the privacy that citizens are afforded under the United States Constitution and the Privacy Act of 1974, which prohibits governmental agencies from amassing information about individuals without a proper purpose for doing so. Google is not so limited. Therefore, if Google and the NSA were to cooperate in any regard, our privacy from governmental intrusion would surely be in danger. In May 2012, the D.C. Circuit Court of Appeals seemed to immunize Google and the NSA from Freedom of Information Act (FOIA) requests regarding their association.

Beyond the threats posed to our constitutional rights, privacy is important for other fundamental reasons. Privacy is a component of freedom. When we lose our privacy, we lose our freedom to re-invent ourselves each day. We lose the freedom to choose, on our own, the companies with which we do business. We lose the freedom to control who in our life knows what about us. We lose the freedom to test new ideas, new philosophies and new selves, and then to forget them when they do not work for us. We lose our right to be complex humans defying categorization. Instead, we assume a unified online identity—an amalgamation of our spending habits, location data, Internet-surfing behavior, and wall postings—an identity ultimately beyond our control, but which has the power to determine how we are embraced by society.

Since there is a right to privacy, it is necessary to insist on a right to protect oneself from the discovery of private information. Essentially, all of the information stored in the cloud and on third-party servers and GPS location-service devices, as well as our Internet activity, could be discoverable because consumers have not insisted on a right to privacy. The consumer unknowingly signed away his right to privacy because the stipulation was hidden in the voluminous “terms and conditions.” Furthermore, the consumer lacks the bargaining leverage to insist on privacy with a multibillion-dollar corporation.

By ceding our rights to privacy, we also may be compelled to produce even more information in civil and criminal trials. The subtle encroachment on an individual’s right to privacy will be all the more noticeable when that individual is required to participate in discovery as part of a lawsuit or investigation. If

176. See id. § 522(a)(c).
there is no recognizable right of privacy, then there can be no reasonable basis for a confidentiality order or protective order. As the Federal Rules of Civil Procedure and the law of search and seizure currently stand, litigants or criminal defendants, as part of the discovery process, could be compelled to produce information into the public domain that they truly believed was private.\(^{181}\)

IV. LAWMAKERS MUST INTERVENE TO PROTECT U.S. CITIZENS FROM COMPLETELY LOSING THEIR FUNDAMENTAL RIGHT TO PRIVACY

A. The Current Laws Do Not Create a Comprehensive Right to Privacy for U.S. Citizens

The average U.S. citizen would likely be surprised to learn that they do not have an overarching right to privacy. The federal privacy statutes, although numerous, provide far less protection than one would expect. According to an article on ChoicePoint and other commercial data brokers, “American privacy law tends to be sectoral and context based. Unlike other nations, the United States lacks a comprehensive privacy law to protect data.”\(^{182}\) Therefore, lawmakers and judges must intervene on behalf of consumers to insist on a fundamental right to privacy.

The Table below summarizes the various federal privacy statutes and demonstrates that the federal statutory scheme provides limited protection for personal data shared online. Most of the statutes govern state actors or law enforcement alone\(^{183}\) and, even then, are riddled with exceptions.\(^{184}\) Those statutes that do seem to create a right to keep personal data private from third parties are also ineffective, because the protections can often be superseded when an individual consents to tracking, storage, and disclosure of personal data.\(^{185}\) The consumer consent exception creates a giant loophole that can be exploited by corporations who include such consent provisions in their one-sided, indecipherable online terms and conditions.\(^{186}\)

---

182. Hoofnagle, supra note 162, at 618.
186. See Gilbert, supra note 11, at 26–28.
### TABLE. SUMMARY OF FEDERAL PRIVACY STATUTES

<table>
<thead>
<tr>
<th>Statute</th>
<th>Which entities does it govern/regulate?</th>
<th>Whose information does it protect?</th>
<th>What type of information does it protect?</th>
<th>Does it govern Facebook &amp; Google?</th>
<th>Exceptions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Communications Policy Act 187</td>
<td>Cable television operators only</td>
<td>Cable television subscribers</td>
<td>Requires cable company to disclose types of personal data collected; prohibits data collection absent consent</td>
<td>No</td>
<td>Cable company can collect data and share it with third parties with “prior written or electronic consent” or other reasons listed by the statute</td>
</tr>
<tr>
<td>Census Confidentiality Statute 188</td>
<td>Federal Government and Census Bureau</td>
<td>Any personally identifiable information (“PII”) submitted to census bureau</td>
<td>Census data only</td>
<td>No</td>
<td>Information can be used for the statistical purposes for which census is conducted</td>
</tr>
<tr>
<td>Children’s Online Privacy Protection Act of 1998 189</td>
<td>Web sites directed at children 13 and younger</td>
<td>PII relating to children 13 and younger</td>
<td>Personally identifiable information relating to children 13 and younger</td>
<td>Yes (but Facebook has found a way around the statute 190)</td>
<td>Web sites can collect PII with “verifiable parental consent”</td>
</tr>
<tr>
<td>Communications Assistance for Law Enforcement Act 191</td>
<td>Law enforcement and telecommunications carriers</td>
<td>Citizens who are the subject of an investigation</td>
<td>Not really a protection—simply requires law enforcement to seek a warrant before monitoring electronic communications (mobile phone wiretaps)</td>
<td>No</td>
<td>Law enforcement may monitor communications and location in “emergency or exigent circumstances”</td>
</tr>
<tr>
<td>Criminal Justice Information Systems 192</td>
<td>Federal Government</td>
<td>Arrestees</td>
<td>Information relating to their arrest and the subsequent disposition</td>
<td>No</td>
<td>Can be used for statutorily authorized purposes, but must otherwise be kept confidential</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Statute</th>
<th>Which entities does it govern/ regulate?</th>
<th>Whose information does it protect?</th>
<th>What type of information does it protect?</th>
<th>Does it govern Facebook &amp; Google?</th>
<th>Exceptions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Proprietary Network Information</td>
<td>Telecommunications carriers (including mobile phone service providers)</td>
<td>Consumers</td>
<td>Fairly broad. Protects information that relates to the quantity, destination, location, and amount of use of a telecommunications service</td>
<td>No</td>
<td>Does not apply when customer provides approval, which all carriers require in their consumer contracts; additional exceptions for 911 compliance, to assist in an emergency situation, and to protect the rights of users</td>
</tr>
<tr>
<td>Driver’s Privacy Protection Act</td>
<td>State Departments of Motor Vehicles</td>
<td>Individuals whose information is held by DMV (license and title holders)</td>
<td>Prohibits disclosure of personal information and highly restricted personal information unless for “permissible use”</td>
<td>No</td>
<td>So many “permissible uses.” this statute is meaningless; can be used by any governmental agency, any law enforcement agency, to confirm ownership and with consent from the individual</td>
</tr>
<tr>
<td>Drug &amp; Alcoholism Abuse Confidentiality Statutes</td>
<td>Entities conducting federally-funded research or treatment of alcohol and drug abuse</td>
<td>Patients and Test Subjects</td>
<td>“Records of the identity, diagnosis, prognosis, or treatment of any patient”</td>
<td>No</td>
<td>May not be used to “initiate or substantiate” criminal charges absent a court order; otherwise, only exceptions are with consent or to assist with a bona fide medical emergency</td>
</tr>
<tr>
<td>Electronic Communications Privacy Act of 1986, Stored Communications Act</td>
<td>Entities providing “electronic communication service[s]” or “remote computing service” such as web mail providers and social networking sites</td>
<td>Consumers</td>
<td>Electronic communications in “storage” (not in transit or stored ephemerally); excludes data that is not a “communication”</td>
<td>Yes</td>
<td>There is a major exception that allows use and disclosure of “communications” with consent from the sender or receiver; the statute also allows disclosure to law enforcement</td>
</tr>
</tbody>
</table>

---

2013] BLEEDING DATA IN A POOL OF SHARKS 745

<table>
<thead>
<tr>
<th>Statute</th>
<th>Which entities does it govern/ regulate?</th>
<th>Whose information does it protect?</th>
<th>What type of information does it protect?</th>
<th>Does it govern Facebook &amp; Google?</th>
<th>Exceptions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Polygraph Protection Act of 1988 197</td>
<td>Employers</td>
<td>Employees and prospective employees</td>
<td>Employee polygraph test results</td>
<td>No (unless these companies required an employee to take a polygraph test)</td>
<td>Court must court order disclosure, and disclosure must be for the purposes of investigating or prosecuting a crime</td>
</tr>
<tr>
<td>Fair Credit Reporting Act; Consumer Credit Reporting Reform Act of 1996 199</td>
<td>Credit reporting companies, creditors, and individuals/entities who request credit reports</td>
<td>Individuals/Consumers</td>
<td>Detailed contents of credit reports</td>
<td>No (unless these companies unlawfully pull credit reports without a valid statutory purpose)</td>
<td>Limits the information that credit reporting agencies can disclose and requires disclosure only for permissible purposes; requires notification to consumers when their credit information has been requested; allows consumers to contest accuracy of data collected about them</td>
</tr>
<tr>
<td>Family Educational Rights &amp; Privacy Act 200</td>
<td>Educational institutions</td>
<td>Students and their parents</td>
<td>Educational records and personally identifiable information “other than directory information”201</td>
<td>No</td>
<td>Disclosure allowed: generally with consent from parents, to transferee school with notice to parents, to government or law enforcement, or to assist with requests for financial aid</td>
</tr>
<tr>
<td>Gramm–Leach–Bliley Act 202</td>
<td>Financial institutions, including retailers who extend credit</td>
<td>Consumers</td>
<td>Personally Identifiable Information and nonpublic financial information (account numbers, SS#, and more)</td>
<td>No</td>
<td>Disclosure allowed: with consent from customer, to assist law enforcement, to prevent fraud and to comply with a valid civil or criminal subpoena</td>
</tr>
</tbody>
</table>

201. See id. § 1232g(b)(1).
<table>
<thead>
<tr>
<th>Statute</th>
<th>Which entities does it govern/regulate?</th>
<th>Whose information does it protect?</th>
<th>What type of information does it protect?</th>
<th>Does it govern Facebook &amp; Google?</th>
<th>Exceptions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Insurance Portability &amp; Accountability Act (HIPAA) of 1996</td>
<td>Health plans, medical providers and their covered business associates</td>
<td>Patients</td>
<td>Information about medical care and “individually identifiable health information”</td>
<td>No (but discussion of patient information over Gmail or web-based email could be a violation of the privacy rule)</td>
<td>Disclosure allowed: with patient consent and to cooperate with law enforcement (in some occasions even without subpoena, warrant or court order)</td>
</tr>
<tr>
<td>Privacy Act of 1974, Paperwork Reduction Act</td>
<td>Federal government</td>
<td>Individuals</td>
<td>All records about individuals held by a government agency</td>
<td>No</td>
<td>Agencies and federal government cannot disclose records to any person without the individual’s consent unless for one of several permissible purposes, including pursuant to a valid court order or to assist law enforcement (even without court order)</td>
</tr>
<tr>
<td>Privacy Protection Act of 1980</td>
<td>Government Officers and Employees</td>
<td>Journalists</td>
<td>Information relating to news stories, books and pieces of journalism</td>
<td>No</td>
<td>Law enforcement may not seize journalistic records without a valid warrant or court order, unless the journalist is the subject of the investigation or it is necessary to protect someone from bodily harm or death</td>
</tr>
<tr>
<td>Right to Financial Privacy Act of 1978</td>
<td>Financial Institutions and Government</td>
<td>Banking customers</td>
<td>Financial records</td>
<td>No</td>
<td>Banks may not disclose financial information about customers to the government without a signed and approved revocable customer consent form or pursuant to a valid search warrant or subpoena</td>
</tr>
</tbody>
</table>

One of the most striking features of this summary of federal privacy statutes is that there are only two statutes that prohibit companies like Facebook and Google from invading an individual’s privacy by storing and tracking their data. With regard to the Children’s Online Privacy Protection Act of 1998, Facebook has found a way around that statute by not allowing individuals under the age of thirteen to join Facebook at all—a policy that the company must surely know is impossible to enforce. The second statute that prohibits companies like Facebook from invading individual privacy, the Stored Communications Act (SCA) that is part of the Electronic Communications Privacy Act (ECPA), is simply ineffective, as discussed further below.

State statutory and common law provide some privacy protection in the absence of adequate federal statutory safeguards. For instance, many jurisdictions offer protection through social security number protection statutes, detailed and powerful identity theft laws, and tort recovery from invasion of privacy, appropriation, intrusion, and public disclosure of private facts. California even “includes an express privacy right in its Constitution.”

<table>
<thead>
<tr>
<th>Statute</th>
<th>Which entities does it govern/ regulate?</th>
<th>Whose information does it protect?</th>
<th>What type of information does it protect?</th>
<th>Does it govern Facebook &amp; Google?</th>
<th>Exceptions?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiretap Act of 1934</td>
<td>All persons, including law enforcement</td>
<td>Individuals</td>
<td>Wire, oral, or electronic communication</td>
<td>No</td>
<td>It is unlawful for any individual to intercept a communication to which they are not a party; law enforcement may do so, but only with a valid warrant or court order</td>
</tr>
</tbody>
</table>

211. Facebook: Help Center, How Do I Report a Child Under the Age of 13?, https://www.facebook.com/help/441374602560317/ (last visited Jan. 28, 2013) (“Facebook requires individuals to be at least 13 years old before they can create an account.”).
213. See infra Part IV.B.
214. See, e.g., GA. CODE ANN. § 16-9-121 (2011) (setting forth the elements of identity fraud); MISS. CODE ANN. § 97-19-85 (Supp. 2012) (criminalizing fraudulent use of another’s identity or social security number); S.C. CODE ANN. § 16-13-510(A) (Supp. 2011) (“It is unlawful for a person to commit the offense of financial identity fraud or identity fraud.”).
215. See Elizabeth D. DeArmond, A Dearth of Remedies, 113 PENN ST. L. REV. 1, 39–42 (2008) (“Thus, the common law of torts offers a number of avenues to pursue those who breach privacy.”).
However, given the broad reach of the Internet and the current strong political will to regulate privacy from Washington, D.C., it seems that a majority of the state-level privacy protections will soon be preempted by a federal legislative response and may, despite their efforts, be too localized to provide adequate protection.

Indeed, “the common law of torts offers a number of avenues to pursue those who breach privacy. However, the torts, interpreted in a cramped and faded way, may insufficiently protect individuals from modern privacy invasions.” In one example, the Illinois Appellate Court recently distinguished “personal” from “private” information—holding that a plaintiff in Illinois cannot sue for damages under a theory of common law invasion of privacy when the alleged damages are caused only by a third party’s disclosure of “personal” information, rather than the disclosure of “private” information. The court defined “private” facts as those that are “facially embarrassing and highly offensive if disclosed.” Using that definition of “private facts,” the court held that there is no private cause of action for damages caused by disclosure of “names and social security numbers.” By analogy, outside of a particular statutory right of privacy, citizens, at least in Illinois, could not claim a common law right of privacy to most personal information they intentionally, and unintentionally, share online and through their phone with Google, Facebook, Apple, and others.

Because of the spotty coverage and overall inadequacy of American privacy law and combined with the frightening power of Google, Facebook, and other private corporations that are compiling massive databases of information about people for profit and sharing those databases with governmental agencies, Congress should act now to create a comprehensive, coherent privacy statute.

B. The Stored Communications Act Should Be Amended or Replaced Because It Is Ineffective

Of the federal privacy statutes in force, the ECPA, which includes the SCA, seems to provide the most likely basis for meaningful protection from third parties that store and process personal data. That statute was intended to

218. DeArmond, supra note 215, at 42.
220. Id.
221. Id.
222. See id.
protect the privacy of electronic “communications” stored with third parties.\textsuperscript{224} Although the SCA does not apply to criminal warrants and subpoenas, it does protect communications from civil subpoenas and other disclosure requests.\textsuperscript{225} The statute would thus seem to prevent companies like Google from disclosing individual emails and text messages pursuant to a civil subpoena or a request from anyone other than the originator or recipient of the message.\textsuperscript{226} It has even been held to protect postings on a Facebook “wall” from disclosure to third parties, although it does not apply to other portions of Facebook that are not “communications.”\textsuperscript{227}

There are, however, some real problems with the SCA. First, it protects too narrow a category of data. When it was written, the Internet was in its infancy, and no one could imagine the broad range of documents and information that people would voluntarily store on other people’s servers, much less the cloud.\textsuperscript{228} As a result, the SCA protects only “communications,” which includes emails,\textsuperscript{229} instant messages, and perhaps, as the Crispin court held, wall postings on Facebook.\textsuperscript{230} The SCA does not cover photos, profiles, or the entire contents of your personal hard drive, much less the laundry list of items that Facebook tracks and stores. The statute should, therefore, be amended or replaced with a statute that prevents a third party who is storing any of your data, not just your communications, from disclosing it to third parties.

There is another problem with the statute. The SCA expressly allows—and may arguably require—a third-party “remote computing service” (read “web site”) or “electronic communication service,” (read “web-mail provider”) to release your own data to you when you request it.\textsuperscript{231} Therefore, the statute cannot prevent a court in a civil case from ordering a party to demand the release of their own data, then ordering that party to hand it over to their litigation opponent. A Pennsylvania court did just that in Largent v. Reed when it ordered

\footnotesize{
226. See id.
229. See J.T. Shannon Lumber Co. v. Gilco Lumber, Inc., No. 2:07-CV-119, 2008 WL 3833216, at *1 (N.D. Miss. Aug. 14, 2008) (citing 18 U.S.C. §§ 2701–2703 (2006)); see also Wyatt v. City of Barre, No. 2:11 CV 297, 2012 WL 3192717, at *6 (D. Vt. Aug. 6, 2012) (citing Thompson v. Ross, No. 2:10 cv 479, 2010 WL 3896533, at *1–5 (W.D. Pa. Sept. 30, 2010)) (“The court found that once the plaintiff saved the emails to his laptop, they were no longer within a facility provided by an electronic communication service. In order for there to be a violation of the SCA, the defendants would have had to view the emails while still in the storage provided by plaintiff’s Internet service provider. Once the plaintiff removed them from his personal email and downloaded them to his laptop, the SCA no longer applied.”).
231. See 18 U.S.C. § 2702(a)–(b)(1) (2006). Although these two categories are treated differently in the statute, both must disclose data to the person who created it. \textit{Id}. 
}
the plaintiff to share the entire contents of her Facebook page with the defendant, despite holding that Facebook was both a remote computing service and an electronic computing service and was covered by the SCA.232 In so holding, the court observed: "The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications." Rather, it only applies to the enumerated entities. [Plaintiff] being neither an [Electronic Communication Service] nor a [Remote Computing Service], the SCA does not protect her Facebook profile from discovery.233

At first blush, this would not seem problematic; the court simply treated the information and data as if it were on the party's own computer.234 But there is a subtle and perplexing problem: users do not actually control the data that these third-party sites track and store about them, nor do they have any input into how long they are kept. In other words, there is an end-run around the statute that threatens users' privacy, yet they do not even have the option of preventing the end-run by managing or deleting the data (lawfully and before a preservation duty has arisen) or by controlling what data they create in the first place.

As a result, the SCA should be replaced with a statute that gives individuals greater control over the information that is saved about them. If the courts continue to treat personal data on Facebook and other third-party sites as if it is in a litigant's possession, custody, and control—as was the case in Largent v. Reed235—then individuals and customers must have the same level of control over the data held by a third-party as they would if it were on their own laptop or home computer. Without control, individuals may one day be forced to disclose information residing with a third party that they had no chance to vet, correct, or delete. Preserving privacy means preserving a party's right to control and delete personal data that can be used against them in court.

C. Congress Should Pass a Comprehensive Privacy Statute, Similar to the 2011 Bill Proposed by Senator McCain and then-Senator Kerry

In April 2011, Senator McCain and then-Senator Kerry proposed a comprehensive privacy bill.236 The bill, if passed into law, would have mandated a method through which individuals could opt out of being tracked, similar to the do-not-call list.237 It provided that the federal government, through the FTC, would enforce privacy238—allowing companies to track only the data

233. Id. (quoting Kerr, supra note 223, at 1214).
234. See id.
235. Id.
238. See id.
they actually needed.\textsuperscript{239} Although the bill may be proposed again during the next session of Congress, the “do-not-track” feature was met with strong resistance.\textsuperscript{240} Senators McCain and Kerry should be lauded for their proposed bill; however, a truly comprehensive and meaningful privacy statute should go even further. It should reconcile the sectoral privacy statutes in force and provide a private cause of action for privacy violations, which, given the limited resources of the government, will be the only way to ensure true corporate accountability for individual privacy violations. The statute should also provide detailed guidance—thus delegating minimal rulemaking power to the agencies responsible for enforcing it. For all of the reasons set forth above, Congress should pass an even stronger comprehensive privacy statute that provides the appropriate enforcement agencies with the power they need to protect the privacy of the American people. The statute should: (1) create a comprehensive statute that supersedes all statutes relating to nongovernmental collection, use, and disclosure of personal data, such as Gramm–Leach–Bliley, HIPAA, and the Right To Financial Privacy Act; this effort should include replacing the ECPA and SCA with a statutory scheme to protect all data—not just communications data—from disclosure absent a valid criminal warrant or an equally compelling reason; (2) prohibit Internet-activity tracking through the use of cookies, spyware, and beacons without clear and meaningful consent from the individual or corporate customer; (3) mandate clear and meaningful disclosures regarding how and why Internet companies with whom we do business—such as social networking sites, web-based email providers, and search engines—track and store our data before a customer signs up for the services and prohibit any changes to those policies after the customer has entered into a contractual relationship with the company; (4) strengthen the law of unconscionability and empower courts to void consumer contracts that force consumers to waive their privacy rights in exchange for the goods and services used by all, such as mobile phone services, Internet, and email; (5) provide access, control, and oversight with regard to the data tracked and stored about individuals by these giant for-profit corporations; (6) provide a private right of action and a right to proceed as a class action plaintiff for statutory privacy violations; and (7) allow for presumed statutory damages for each violation of the statute.

Without a comprehensive “Privacy Bill of Rights,” as Senators McCain and Kerry called it, we may extinguish the actual Bill of Rights and put the government as well as the largest corporations in the world in a position to easily reach and control us with a mere keystroke.

D. In Addition, the Judicial Conference of the United States and the Committee on Rules of Practice and Procedure Should Propose Amendments to the Federal Rules of Civil Procedure to Account for the Discoverability of Inadvertently Shared Online Information in Litigation

The Federal Rules of Civil Procedure should once again be amended to account for “private” electronically stored information (ESI). As the discovery rules currently stand, a litigant is entitled to discover ESI relating to any “nonprivileged matter that is relevant to any party’s claim or defense.”241 Furthermore, discovery provisions “are to be applied as broadly and liberally as possible.”242 This means that information stored on iPads, iPhones, OnStar, cloud servers, Google, and Facebook that consumers give voluntarily, as well as information such as IP addresses and shopping proclivities that consumers may give involuntarily, is discoverable if relevant.243

However, as discussed above, much of this information was created by third parties. Further, huge seas of data about us have been shared or created without our knowledge.244 This ESI is far different from the journal entry written in Microsoft Word and stored on a personal hard drive; instead, this is the ever-growing volume of highly personal information stored on third-party computers.245 Thus, in litigation, it should not be deemed discoverable in the same sense as a document created by the litigant itself—especially when the litigant was not even aware it existed.

Thus, the Judicial Conference of the United States, through the Committee on Rules of Practice and Procedure, should implement a contemporary discovery rule that addresses the tension between broad discoverability and the threat to individual privacy in this digital age. This rule, or amendments to Rules 26 and 45, should provide that ESI involuntarily collected by a third party or unknowingly shared with a third party shall only be discovered from the litigant itself, i.e., the party that holds the right to privacy, and not through a third-party request or subpoena intended to circumvent those rights. Additionally, the rule should create a presumption that ESI involuntarily collected by a third party or unknowingly shared with a third party is “not reasonably accessible”246 and thus be subject to the same procedures and safeguards set forth in Federal Rule of Civil Procedure 26(b)(2)(B). The rule should further enlarge the definition of “not reasonably accessible” in Rule 26(b)(2)(B)247 and require courts to consider

241. FED. R. CIV. P. 26(b)(1).
244. See Roos, supra note 98.
245. See id.
247. Id.
the responding parties claims of privacy—perhaps through a balancing test similar to that described in Federal Rule of Evidence 403\textsuperscript{248}—before allowing discovery of such materials. The rule should also take into account a litigant’s privacy settings on social networking web sites to determine whether the information was intentionally placed on the Internet with unlimited or restricted third-party access and provide methods for a litigant to protect private information. Specifically, the rule should provide a litigant with a per se presumption that information shared with a vendor or third party according to a “privacy policy” or terms and conditions purporting to afford them some right to privacy is entitled to protection from public disclosure through a protective order sealing or segregating private information.

Given that almost all relevant, nonprivileged ESI is discoverable in litigation\textsuperscript{249} and given that individual litigants no longer control their own ESI, only a discovery rule granting litigants some mechanism for protecting their unintentionally and unknowingly shared private and confidential information can prevent the further deterioration of the once fundamental right to privacy.

V. CONCLUSION

There is an ever-widening gap between each American citizen’s expectation of privacy and the ease with which each citizen’s personal information can be accessed using modern technology. Given that Google, Facebook, and the other Internet giants are determined to profit from sharing citizens’ data with the world and given the ineffective patchwork of existing federal privacy statutes and the slow and inconsistent progression of the judicial opinions on the subject, Congress should act now to pass a comprehensive privacy bill before it is too late. The Judicial Conference of the United States should act to limit the discoverability of that private information in litigation. By failing to act as a nation, we could create the very Orwellian nightmare that many fear.

\textsuperscript{248} FED. R. EVID. 403.

\textsuperscript{249} See Derek S. Witte, Your Opponent Does Not Need a Friend Request to See Your Page: Social Networking Sites and Electronic Discovery, 41 McGeorge L. Rev. 891, 892–93 (2010) (citing FED. R. CIV. P. 34(a)(1)) (explaining that the contents of social networking pages—such as a Facebook page—are ESI under the plain meaning as defined by the Federal Rules of Civil Procedure).
*