PRIVACY IN THE CLOUD FRONTIER: ABANDONING THE "TAKE IT OR LEAVE IT" APPROACH

Scott Bender[*]

INTRODUCTION 487
I. BACKGROUND 491
A. *The Development of Privacy as a Fundamental Right* ... 491
B. *Privacy in Communications: The* Katz *Test* 492
C. *The Electronic Communications Privacy Act of 1986* ... 494
D. *Privacy in the Cloud* 497
E. *The "Take it or Leave it" Approach* 500
F. *The Google Buzz Settlement* 505
II. ANALYSIS 508
A. ProCD *and Its Impact on Terms of Service and Privacy Policies* 509
1. *Modern day privacy policies as clickwrap contracts* 510
2. *Retiring Easterbrook's approach* 513
B. *Pitfalls of the ECPA in Protecting Personal Data Privacy* 514
III. PROPOSED SOLUTION 517
CONCLUSION 521

INTRODUCTION

Imagine that you have just finished composing an e-mail, checking your favorite social networking website, and watching a streaming video online. This scenario should not stretch the imagination considering that, on average, 294 billion e-mails are sent each day,[1] Facebook maintains an active user base of over 800 million members,[2] and over 3 billion videos are watched each day on YouTube.[3]

* J.D. 2011, *magna cum laude*, Earle Mack School of Law; B.A. 2006, *cum laude*, The George Washington University. Mr. Bender is serving as an Attorney Advisor for the United States Social Security Administration. Special thanks to Shelby, my parents and family for their support and encouragement, Professor Deborah Gordon for her insightful comments on an early draft of this article, and the editors of the *Drexel Law Review* for their hard work preparing this piece for publication.

1. Heinz Tschabitscher, *How Many Emails Are Sent Every Day?*, ABOUT.COM, http://email.about.com/od/emailtrivia/f/emails_per_day.htm (last visited Feb. 19, 2012).

2. *Fact Sheet*, FACEBOOK, http://newsroom.fb.com/content/default.aspx?NewsAreId=22 (last visited Apr. 8, 2012).

Next, consider how you reached this stage in your technological life. You may recall the following series of events: first, you amassed gigabytes of personal documents, family photos and videos, and business contacts, which you desired to store and share with your friends on the Internet; next, you typed "www.gmail.com," "picasa.google.com," or "docs.google.com" into the Internet browser of your choice and were met with a login screen demanding a username and password.[4] Naturally, your desire to obtain Google's free-of-charge, incredibly popular services led you to click the "Sign up for a new Google Account" link and fill out the simple form[5]—a final obstacle standing between you and worldwide connectivity. After scrolling to the bottom of the form, you noticed a section labeled "Terms of Service."[6] Wanting to set up your account and begin sharing with your friends as soon as possible, you cursorily read the cautionary phrase, "By clicking on 'I accept' below you are agreeing to the Terms of Service above and both the Program Policy and the Privacy Policy,"[7] but ignored it, skipping right to acceptance. You did not take time to scrutinize the small, rectangular box labeled "Google Terms of Service" because of the sheer magnitude of the text within the box and because, at that moment, you did not believe that there were any ramifications for ignoring it. Moreover, you remember having ignored the Terms of Service and Privacy Policy when you signed up for your Facebook[8] and YouTube[9] accounts without any consequences.

With the familiar and casual treatment of electronic communications, it is difficult to imagine that users give much consideration to the prospective legal consequences of patronizing online service-providers. The relaxed attitude of Internet users is particularly significant in the current age of cloud computing, in which third-party servers store users' personal information and content—including e-mails, photos, personal documents, and videos—for service provid-

3. *Statistics*, YOUTUBE, http://www.youtube.com/t/press_statistics (last visited Apr. 8, 2012).

4. *See Gmail: Email from Google*, GOOGLE, http://www.gmail.com (last visited Apr. 8, 2012); *Picasa 3: Free Download from Google*, GOOGLE, http://picasa.google.com (last visited Apr. 8, 2011); *Google Docs: Online Documents, Spreadsheets, Presentations, Surveys, File Storage and More*, GOOGLE, http://docs.google.com (last visited Apr. 8, 2011).

5. *See Accounts*, GOOGLE, http://accounts.google.com (last visited Apr. 8, 2012).

6. *Id.*

7. *Id.*

8. *See Sign Up*, FACEBOOK, http://www.facebook.com/ (last visited Apr. 8, 2012).

9. *See Get Started with Your Account*, YOUTUBE, http://www.youtube.com/create_account (last visited Apr. 8, 2012).

ers like Google, Facebook, and Yahoo! so that the data can be accessed from anywhere.[10] Through the use of a cloud computing service, a user may create documents containing private information such as social security numbers, credit card numbers, or other financial information. That information is then stored on a massive server along with the information of millions of other users, which may be accessible from any source that is connected to the Internet.[11] Small startup companies leasing space on a large server, such as from Google, Amazon, Microsoft, or IBM, often administer such cloud-based services.[12] Thus, personal documents entrusted to a cloud-computing service provider may indeed be in the hands of a third-party company with an unknown security level.

This form of technological convenience, known as "the cloud," has led to the proliferation of handheld devices such as smartphones—inexpensive devices the components of which run the gamut of traditional surveillance equipment, including a high-definition camera, microphone, high-capacity memory, global positioning system, and full Internet access.[13] Such devices are only becoming more advanced; for example, with the advent of Near Field Communication (NFC),[14] users everywhere will soon be able to store credit card information on their phones to pay for bus fare by simply waving the device past a sensor.[15] Additionally, NFC-enabled devices could be used as "library cards, hotel room keycards, and office building passcards. . . . Even keys could someday become a relic of the past, replaced by the tap of a phone to a lock."[16] The security of one's sensitive financial information, and potentially one's private

10. *See* Andrew C. DeVore, *Cloud Computing: Privacy Storm on the Horizon?*, 20 ALB. L.J. SCI. & TECH. 365, 366 (2010).

11. *See, e.g.*, *Tour: Simplify Your Life*, DROPBOX, http://www.dropbox.com/tour (last visited Apr. 8, 2012).

12. *See* Susan A. Berson, *Safe in the Cloud? Online Service Risks Need Care and Coverage*, A.B.A. J. (Nov. 1, 2011), http://www.abajournal.com/magazine/article/safe_in_the_cloud_online_service_risks_need_care_and_coverage/ ("Cloud service providers like Dropbox, for example, store your data on storage they lease from a major cloud provider.").

13. *See* Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 73 (2008).

14. *See* Dan Nosowitz, *Everything You Need to Know About Near Field Communication*, POPULAR SCIENCE (Mar. 1, 2011), http://www.popsci.com/gadgets/article/2011-02/near-field-communication-helping-your-smartphone-replace-your-wallet-2010/ (explaining that Near Field Communication allows a smartphone to wirelessly complete a credit card transaction through the simple act of tapping the phone against a payment terminal).

15. *See* Paula Berger, *Building the Foundation for NFC*, NFC FORUM (Dec. 13, 2010), *available at* http://www.nfc-forum.org/resources/presentations/Foundation_for_NFC-MIT_Dec2010.pdf.

16. *See* Nosowitz, *supra* note 14.

residence, may be a mere inadvertent shift or click away from public exposure.

Users' lack of concern over how their communications are stored, or the potential that someone might intercept, use, or otherwise misappropriate the content of their e-mails or Facebook activity without their knowledge or consent poses a danger to personal privacy in the cloud. When something does go wrong, and a user's privacy is compromised, the current legal regime does not provide adequate recourse; rather, it leaves users in the precarious position of having to choose between protecting their private information by avoiding online services, or allowing it to be stored in the cloud, subject to a service provider's terms of service and privacy policy.

This Note will provide a critical look at personal privacy in the age of an ever-burgeoning Internet landscape. This Note urges that, when offered a free service such as Gmail or Facebook, the average Internet user does not expect to be encumbered with burdensome terms of service. Moreover, one does not expect to forfeit a substantial amount of privacy interest in the intimate details of one's life through the simple act of surfing the Internet. The collision of the two matters—privacy and "take it or leave it" terms of service—creates vulnerability for Internet users of all types, and these users are ill-prepared to protect themselves from harm. This Note suggests that the sophisticated players—businesses and government—and not the unwitting consumer, should be forced to solve the problem through the legislative process and through better business practices.

Part I begins with a perspective on historical precedent and pertinent case law giving rise to the right to privacy, followed by a look at the federal statute enacted to enforce that right in electronic communications. Next, Part I provides an overview of recent developments in Internet commerce—in particular, cloud computing—and a look at the leading case concerning the governing documents—i.e., terms of service and privacy policies. Part I finishes with a look at a recent class-action lawsuit against Google filed by Internet users for violations of privacy in the cloud. In following, Part II assesses the negative effects that the current system of commercial, federal, and common law has on personal privacy in relation to efficient business practices. Finally, Part III proposes that the solution to the attendant cloud-related privacy risks mandates the eradication of terms of service and privacy policies behind which cloud-based service providers currently hide. The proposed solution requires legislative action in the form of a uniform federal statute

providing for detailed notice in the event of a security breach in the cloud, immediate restorative action on the part of the cloud provider, and a private cause of action for individuals whose privacy was irreparably violated due to a breakdown in cloud security.

I. BACKGROUND

A. The Development of Privacy as a Fundamental Right

In December 1890, Samuel D. Warren and Louis D. Brandeis's *Harvard Law Review* article, *The Right to Privacy*, broke new ground in the field of personal privacy.[17] According to the authors, "in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*."[18] Individual liberty was limited to freedom from physical seizure.[19] As Warren and Brandeis described, over time the common law broadened its conception of "the right to life" to include "the right to be let alone" and the right to freedom from intrusion upon intangible—as well as tangible—property.[20] Thus, the authors explained, from the ashes of the rudimentary idea that only a person's body and property were to be protected from actual physical injury, arose the principle that a person's reputation, dignity, and, moreover, the intimate details of her life, had inherent protectable value.[21]

With certain eloquence, the authors presented the evolution of the human ethos that has driven the flourishing of societies as "[t]he intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, [which] made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things."[22] As a contemporary manifestation of this idea, the authors explained that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[23] Due to the proliferation of

17. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

18. *Id.* at 193.

19. *See id.*

20. *Id.*

21. *See id.* at 193–95.

22. *Id.* at 195.

23. *Id.* (footnote omitted).

such widespread media outlets, the authors argued, "the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer."[24]

Accordingly, Warren and Brandeis contended that the protection of the intimate details of one's private life must increase as technology lifts the veil of personal secrecy:

> The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. Under our system of government, he can never be compelled to express them (except when upon the witness-stand); and even if he has chosen to give them expression, he generally retains the power to fix the limits of the publicity which shall be given them.[25]

In addition, the authors advocated that "[t]he existence of this right [to privacy] does not depend upon the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music."[26] Moreover, "the existence of the right [does not] depend upon the nature or value of the thought or emotion, nor upon the excellence of the means of expression. *In every such case the individual is entitled to decide whether that which is his shall be given to the public*."[27]

Moving forward, the stage was set for the common law to adapt to Warren and Brandeis's view of an ever-shrinking world, although not developed for several decades. The increased pervasiveness of the telephone provided the proper impetus for change as it became a primary source of personal communication in the first half of the twentieth century.[28]

B. Privacy in Communications: The Katz *Test*

In the winter of 1967, the everyday use of the telephone occasioned the Supreme Court to issue a seminal opinion involving tele-

24. *Id.*

25. *Id.* at 198 (footnote omitted).

26. *Id.* at 198–99 (footnotes omitted).

27. *Id.* at 199 (emphasis added).

28. *See Telephone History: The New Century 1901–1940*, TELEPHONY MUSEUM, http://www.telephonymuseum.com/History%201901-1940.htm (last visited Apr. 8, 2012).

phonic communication in *Katz v. United States*.[29] The factual background—presented by Justice Potter Stewart in summary fashion—involved Charles Katz's arrest for "transmitting wagering information by telephone from Los Angeles to Miami and Boston in violation of [18 U.S.C. § 1084]."[30] The twist presented by the arrest included the facts that (1) the phone calls made by Katz were conducted inside a telephone booth with the door shut and (2) the FBI agents who made the warrantless arrest listened in on Katz's phone calls by use of a wiretap device located outside of the public telephone booth.[31] In prior Supreme Court decisions, no Fourth Amendment violation of one's right to be free of unreasonable searches and seizures could be found unless there was evidence of an infringement on a property interest[32] (consisting of people's "persons, houses, papers and effects").[33]

The broad interpretation applied to the right to privacy in the *Katz* decision constituted a progressive step in the direction toward Warren and Brandeis's conception of the right.[34] Justice Stewart's analysis of the right to privacy set forth within the Bill of Rights,[35] coupled with his acknowledgement of a person's "right to be let alone by other people,"[36] led him to the novel conclusion that "the Fourth Amendment protects people, not places."[37] From there, the Court was able to reject the notion that there existed certain "constitutionally protected areas"[38] outside of which no privacy interest could be expected.

In a concurring opinion, Justice John M. Harlan expounded on the majority's reasoning by crafting a two-pronged test for determining what privacy protections the Fourth Amendment affords people.[39] Accordingly, Justice Harlan propounded what became the *Katz* test, requiring "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that

29. 389 U.S. 347, 348 (1967).

30. *Id.* at 348.

31. *Id.* at 348–52.

32. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464–66 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

33. *See* U.S. CONST. amend. IV.

34. *See* Warren & Brandeis, *supra* note 17.

35. *See Katz*, 389 U.S. at 350 n.5 (summarizing the privacy rights afforded by the First Amendment, Third Amendment, and Fifth Amendment to the Constitution).

36. *Id.* at 350 (citing Warren & Brandeis, *supra* note 17).

37. *Id.* at 351.

38. *Id.* at 351 n.9.

39. *See id.* at 361 (Harlan, J., concurring).

society is prepared to recognize as 'reasonable.'"[40] The test implied that, although "conversations in the open would not be protected against being overheard,"[41] under the proper circumstances, one could reasonably expect privacy in the content of her communications.[42] Notably, in addition to stating the test—still followed today in both federal and state court decisions[43]—Justice Harlan recognized the potential that "electronic as well as physical invasion" would further attenuate a person's reasonable expectation of privacy in the content of her communications.[44] Less than twenty years later, Justice Harlan's acknowledgment of the impact of electronic communication methods on privacy led to the drafting of the Electronic Communications Privacy Act (ECPA).[45]

C. The Electronic Communications Privacy Act of 1986

In 1985, Senator Patrick Leahy introduced the ECPA[46] due to concerns he foresaw with "the advent of electronic communications, principally e-mail."[47] Following the introduction of the Bill, the Congressional Office of Technology Assessment (OTA) released a study, finding that

> [t]here are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy,

40. *Id.*

41. *Id.*

42. *Id.* The notion of protecting the privacy of communications was particularly novel due to the fact that a conversation has never been recognized as a house, person, paper, or effect. *See* U.S. CONST. amend. IV.

43. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010); Rehberg v. Paulk, 611 F.3d 828, 842 (11th Cir. 2010); State v. Payne, 996 A.2d 302, 313 n.6 (Conn. App. Ct. 2010) (Robinson, J., concurring).

44. *See Katz*, 389 U.S. at 362 (Harlan, J., concurring).

45. Congress added The Electronic Communications Privacy Act in 1986 as an amendment to the Wiretap Act of 1968—passed as a direct result of *Katz*—in an effort to include protections for increasingly popular technologies such as cellular telephone usage and e-mail. *See Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 7 (2010) (statement of James X. Dempsey, Vice President, Center for Democracy and Technology), *available at* http://judiciary.house.gov/hearings/pdf/Dempsey100505.pdf.

46. *See* S. 1667, 99th Cong. (1985), *reprinted in* 131 CONG. REC. S11, 790–93 (daily ed. Sept. 19, 1985) (statement of Sen. Patrick Leahy).

47. United States v. Councilman, 418 F.3d 67, 76 (1st Cir. 2005).

> and when retained in the files of the electronic mail company for administrative purposes. *Existing law offers little protection*.[48]

The Department of Justice (DOJ) pushed back, refusing to accept the proposed extension of legal protection to e-mail at "the time after a specific communication has been sent and while it is in the electronic mail firm's computers but has not been delivered, or has been delivered to the electronic mailbox but has not been received by the recipient."[49] Eventually, however, Congress passed the ECPA into law, incorporating a broad definition for the term "electronic communication"[50] and intending to afford to e-mail similar protections as those enjoyed by first-class mail.[51]

Title I of the ECPA (the Wiretap Act),[52] together with Title II (the Stored Communications Act),[53] authorizes the federal government "to require internet service providers [(ISPs)] to disclose the contents of 'electronic communication[s]' of their customers in certain circumstances, including by way of an *ex parte* court order."[54] The Acts derive their principal authority from the Fourth Amendment and owe their existence in large part to Justice Stewart's opinion in *Katz*. The Wiretap Act provides the following three relevant definitions that bear on the meaning of the compelled-disclosure provisions of the Act:

> "*[E]lectronic communication service[s]*" permit "users . . . to send or receive wire or electronic communications,"[55] a definition that covers basic e-mail services.[56] "*[E]lectronic storage*" is "any temporary, intermediate storage of a wire or

48. OFFICE OF TECHNOLOGY ASSESSMENT, OTA-CIT 293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 48 (1985) (emphasis added), *available at* http://www.fas.org/ota/reports/8509.pdf.

49. *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong. 234 (1986) (statement of James Knapp, Deputy Assistant Att'y Gen., Criminal Division, United States Department of Justice).

50. *See id.* (quoting H.R. REP. NO. 99-647, at 35 (1986) ("The term 'electronic communication' is intended to cover a broad range of communication activities . . . .")).

51. *See id.*

52. 18 U.S.C. §§ 2510–2522 (2006).

53. *Id.* §§ 2701–2712 (2006).

54. *See* Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (citing 18 U.S.C. § 2703(d) (2006) (amended 2009)).

55. *Id.* (emphasis added) (quoting 18 U.S.C § 2510(15)).

56. *Id.* (emphasis added) (citing PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 584 (2d ed. 2004)).

> electronic communication . . . and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[57] "*[R]emote computing service[s]*" provide "computer storage or processing services" to customers,[58] and are designed for longer-term storage.[59]

As evidenced by the above terms, in particular "remote computing service," the ECPA is intimately connected to protecting privacy interests of computer users as they communicate with others across the Internet.[60] One might envision that an Act with such an important role in public policy would be drafted in a clear and unambiguous fashion so as to adequately protect its constituents; however, commentators and courts alike have long since complained of the murkiness of the Act's provisions.[61] In particular, those grappling with just application of the Act take issue with faulty notice requirements,[62] as well as the relative lack of civil remedies afforded for violations of the Act.[63]

Since the passage of the ECPA almost thirty years ago, many technological advances have come about in the field of computing, including cloud data storage, social networking, and the commercialization of the Internet itself.[64] Privacy advocacy groups, such as

57. *Id.* (emphasis added) (quoting 18 U.S.C. § 2510(17)).

58. *Id.* (emphasis added) (quoting 18 U.S.C. § 2711(2)).

59. *Id.* (citing Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1216 (2004)).

60. *See* Monique Mattei-Ferraro, *The States and the Electronic Communications Privacy Act: The Need for Legal Processes that Keep Up with the Times*, 22 J. MARSHALL J. COMPUTER & INFO. L. 695, 700 (2004) ("If not for the ECPA, there would be no barrier to prevent police from asking for any records held by ISPs.").

61. *See id.* at 701 ("While Congress had good intentions when it enacted the ECPA, the states have been mired in confusion since its passage.").

62. *See Warshak*, 532 F.3d at 526 (discussing *ex parte* searches of Warshak's e-mails under 18 U.S.C. § 2703(d)).

63. *See* DeVore, *supra* note 10, at 371.

64. *See generally* PATRICIA L. BELLIA ET AL., CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE 14 (3d ed. 2006).

> The Internet had its origins in 1969 as an experimental networking project supported and managed by the Advanced Research Project Agency ("ARPA") of the U.S. Department of Defense . . . . On January 1, 1983 . . . the networks . . . switched over to the [Transmission Control Protocol/Internet Protocol (TCP/IP)] suite . . . and the network that was to become "the Internet" was born. By 2006, the TCP/IP had over 400 million individual "hosts"—computers, or computer networks, capable of exchanging messages with one another.

Id.

Digital Due Process,[65] have been lobbying for amendment of the ECPA in order to bring Internet surveillance laws up to the times. Moreover, the proliferation of handheld devices, instantaneous worldwide connectivity, and rampant social networking has increased the need for the protection of easily publicized, but highly sensitive, information.[66] Thus, the mounting tension between technology-based businesses and consumer privacy rights is developing into a veritable tug-of-war over whether business, government, or the consumer should shoulder the load.

D. Privacy in the Cloud

No single phrase better articulates the corporate mindset relating to Internet privacy than the oft-quoted flippancy uttered by Sun Microsystems Chief Executive Officer Scott McNealy in 1999: "You have zero privacy anyway. . . . [G]et over it."[67] Although McNealy subsequently attempted to downplay the connotation of his statement, privacy advocates met it with harsh criticism.[68] Notwithstanding, it appears that the Internet-using public has "gotten over" the lack of privacy assurances on the Internet, namely by "routinely part[ing] with personal information and at least passively consent[ing] to its use, whether by surfing the internet, entering sweepstakes, or using a supermarket discount card."[69] Whether such passivity may be construed as ignorance, arrogance, or lack of savvy, it is becoming a particularly essential element in the ensuing epoch of technology: the era of cloud computing.

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with

65. *See* DIGITAL DUE PROCESS, www.digitalprocess.org (last visited Apr. 8, 2012).

66. *See* Zittrain, *supra* note 13, at 95, 99, 111.

67. Polly Sprenger, *Sun on Privacy: 'Get Over It,'* WIRED, Jan. 26, 1999, http://www.wired.com/politics/law/news/1999/01/17538. In a similar exposition of the corporate mindset towards privacy, LinkedIn CEO Reid Hoffman was quoted as saying, "all these concerns about privacy tend to be old people issues." Marc Cenedella, *Privacy is for Old People Says LinkedIn Founder*, RECRUITING & JOB SEARCH (Oct. 10, 2011), http://www.cenedella.com/job-search/privacy-is-for-old-people-says-linked-in-founder/.

68. *See* Sprenger, *supra* note 67 (quoting Jason Catlett, Chief Executive Officer of a company that makes privacy software as saying, "[McNealy's statement is] tantamount to a declaration of war").

69. Zittrain, *supra* note 13, at 69.

minimal management effort or service provider interaction."[70] The broad definition that NIST has propounded above may be summed up as "services provided by a third party, hosted by a third party."[71] Such services will often involve a remote, multiple-terabyte mega-server,[72] coupled with the ability for both the user and the service provider to access the server "from pretty much anywhere."[73] Due to their massive storage capacity and ease of access, such servers provide the potential for the "longer-term storage" implicated by Title II of the ECPA.[74]

For privacy purposes, submitting to the cloud amounts to the surrender of control of information to a potentially unknown third party, and the subsequent storage of said information for an indefinite period of time.[75] This practice can be very beneficial to an ISP seeking to offer an efficient and convenient method of doing business that will attract scores of Internet users.[76] On the other hand, the consequences can be dire when the cloud malfunctions. Specifically, the risks of operating through the cloud include the fact that voluminous amounts of high-value data collections are stored in the same place and are at the mercy of a potentially negligent third party.[77]

For example, two major cloud providers—T-Mobile and Google—have experienced third-party server meltdowns that have led to the

70. PETER MELL & TIMOTHY GRANCE, U.S. DEP'T OF COM., NAT'L INST. OF STANDARDS & TECH. SPECIAL PUBL'N 800-145, THE NIST DEFINITION OF CLOUD COMPUTING (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf. (last visited Apr. 8, 2012).

71. DeVore, *supra* note 10, at 366.

72. *See* R. Kayne, *What is a Terabyte?*, WISEGEEK, http://www.wisegeek.com/what-is-a-terabyte.htm (last visited Apr. 8, 2012) (defining the capacity of a terabyte as 1024 gigabytes, or 1,048,576 megabytes); MG Siegler, *Google Offers a 16 Terabyte Cloud Drive for $4,096 a Year*, TECHCRUNCH (Nov. 11, 2009), http://techcrunch.com/2009/11/11/google-offers-a-16-terabyte-cloud-drive-for-4096-a-year/.

73. *See* DeVore, *supra* note 10, at 366.

74. *See* Kerr, *supra* note 59, at 1216.

75. *See* DeVore, *supra* note 10, at 370 ("The heart of the privacy issue with regard to cloud computing is the fact that you are handing over potentially highly sensitive and private information to a third party to store and process.").

76. *See id.* at 366–67.

> Companies can gain substantial advantages by not having to acquire your own services, your own infrastructure, your own professionals to maintain the applications to make sure you have what you need, make sure that there are appropriate security protocols in place, make sure that there are appropriate privacy rules, policies, and procedures governing the information that you as a company have and use.

Id.

77. *Id.* at 369.

loss of all of the user information stored on the cloud.[78] In the T-Mobile debacle, Danger, Inc., a Microsoft subsidiary, destroyed all of the data stored on the cloud for use by T-Mobile "Sidekick" handheld devices.[79] Danger, Inc. did not have backups for the massive amount of user information that was lost.[80] The Google fiasco involved the popular cloud application Google Docs, which affords users a great amount of control in creating and storing documents online.[81] With a glitch on permissions, however, Google Docs released private information to non-authorized users.[82] Due to the large pool of businesses relying on Google Docs to store valuable information, this type of cloud malfunction poses "huge potential implications on privacy and security."[83]

In addition, data encryption has infrequently been implemented in the cloud, which has made it particularly difficult to prevent hackers from gaining access to that information.[84] A security breach on Twitter allowed hackers to change user passwords and send out "tweets" posing as a number of high profile individuals, including one tweet that read, "I'm high on crack right now, can't come into work today."[85] More recently, an online document-sharing service known as Dropbox experienced a malfunction where a "programmer's error had enabled any password to access any Dropbox site."[86] Due to the nature of the law governing cloud computing,[87] users whose accounts were compromised by the security breach were left without recourse.

Thus, although the utilization of cloud computing technology may lead to greater efficiency and ease-of-use functionality for users and businesses alike,[88] it remains highly vulnerable to both misfea-

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.*

82. *Id.*

83. *Id.* at 369–70.

84. *Id.* at 369.

85. *Id.* at 370.

86. *See id.*

87. What the law says, and it's quite clear, is that if you have private confidential information, you have certain privacy interests and corresponding legal protections for that information so long as you maintain the privacy and secrecy of that information. If you give that same information to a third party, however, you effectively lose those protections. That's the way the law works.

Id.; *see also* Smith v. Maryland, 442 U.S. 735, 740–44 (1979) (finding no expectation of privacy in information readily handed over to a third party).

88. *See* DeVore, *supra* note 10, at 366–67; *see also supra* note 76 and accompanying text.

sance caused by human error[89] and malfeasance caused by human intervention.[90] Whether the user is aware of the exact mechanism used to store her private information, she may place a great deal of trust in the cloud provider to protect her personal data. Further, the user may value the information that she has entrusted to the cloud, and she may wish to guard such information jealously. On the other hand, she may choose to remain blissfully ignorant and, for example, "decide that the convenience of free, web-based e-mail is ultimately worth the tradeoff of allowing the service provider to screen [her] e-mail."[91] Due to the importance of the seemingly conflicting interests of privacy and convenience at stake here, the method of governance of the Internet—e.g., by statute, contract, or otherwise—will dictate the way that both society and the Internet develop going forward.

E. The "Take It or Leave It" Approach

Commentators have analogized the present landscape of Internet regulation to a developing "frontier," seeking to establish itself as a legitimate territory in the conquest of modern society.[92] Not unlike the "Wild West" of nineteenth-century America, the Internet began as a largely self-regulated open frontier[93] in which "the freedom to experiment was considered important enough to justify discarding many old laws and morals."[94] Eventually, however, the Wild West transitioned into an integrated part of society, and the Internet is experiencing a similar shift.[95] In following, "[i]t has become routine to talk about government regulation of the Internet—ranging from 'net neutrality' to Facebook privacy."[96] As an evolving closed frontier,[97] the Internet requires proper regulation so as to preserve

89. *See supra* text accompanying notes 78–83.

90. *See supra* text accompanying notes 84–85.

91. Warshak v. United States, 532 F.3d 521, 527–28 (6th Cir. 2008) (examining the expectation of privacy Internet users exhibit in relation to terms of service-provider agreements).

92. *See* David Thompson, *The Closing of the Internet Frontier?*, THE VOLOKH CONSPIRACY (June 7, 2010, 12:26 PM), http://volokh.com/2010/06/07/the-closing-of-the-internet-frontier.

93. *Id.* ("Open frontiers are often characterized by self-reliance, self-defense, exploration of new norms, and informal law enforcement.").

94. *Id.*

95. *Id.*

96. *Id.*

97. *Id.* ("Closed frontiers are often characterized by increasing similarity to the 'old' society (often formed by combining elements of old and new), increasing formality, and active law enforcement.").

societal expectations of offline society while maintaining the ease of access and the free-expression characteristic of online communication.

Coming upon the Internet frontier in its early stages, businesses took tremendous advantage of the worldwide connectivity and efficient transactional capabilities of cyber-commerce. To date, the regulation of such commerce has been left largely to the businesses themselves in the form of terms of service, privacy policies, and the like.[98] Judge Frank H. Easterbrook's leading opinion on terms of service in *ProCD, Inc. v. Zeidenberg*, set forth the pragmatism of using these contract-based methods to dictate the terms of a commercial relationship; thereafter, Easterbrook's approach became the majority rule, rationalized as properly offering consumers the opportunity to "take it or leave it."[99]

In *ProCD*, the Seventh Circuit upheld the enforceability of shrinkwrap licenses[100] as long as their terms do not present individualized substantive defects (i.e., violation of positive law, or unconscionable terms).[101] ProCD, Incorporated (ProCD) was a company engaged in the compilation and distribution of telephone directories encoded on CD-ROM discs.[102] The database, known as SelectPhone, was the subject of copyright protection[103] and was sold under a price-discrimination scheme—commercial purchasers in the trade were able to resell the database but were required to pay a significantly higher price than that paid by the general consuming public

98. *See* Zittrain, *supra* note 13, at 69–70.

99. *See* 86 F.3d 1447 (7th Cir. 1996). This Note does not address the Seventh Circuit's subsequent decision in *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147 (7th Cir. 1997), because, although relevant, the opinion is not as potently characteristic of Judge Easterbrook's style. *See, e.g.*, Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1340 (D. Kan. 2000) (pointing out Judge Easterbrook's propensity to make conclusions without support).

100. 86 F.3d at 1449.

> The "shrinkwrap license" gets its name from the fact that retail software packages are covered in plastic or cellophane "shrinkwrap," and some vendors . . . have written licenses that become effective as soon as the customer tears the wrapping from the package. Vendors prefer [to use the term] "end user license."

Id. In modern Internet jargon, shrinkwrap licenses are known as clickwrap licenses because the agreements are purely web-based. *See Click-wrap Agreement Definition*, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/click-wrap-agreement.html (last visited Apr. 8, 2012).

101. *See ProCD*, 86 F.3d at 1449.

102. *See id.*

103. Although the data itself contained within the SmartPhone database was not sufficiently original to be protected by copyright, the software application program of the CD-ROM was. *See id.* at 1453.

(approximately $150 for five discs).[104] ProCD sought to enforce this scheme by encoding the terms of an end-user license on the SelectPhone discs, printing the terms in a user manual and placing the contents inside of the retail box that contained a notice to consumers that use of the software was subject to certain terms (i.e., limitation of consumer use to non-commercial purposes).[105] In derogation of the terms governing ProCD's price-discrimination scheme, Matthew Zeidenberg bought a consumer version of SelectPhone for $150, formed Silken Mountain Web Services, Incorporated—a Wisconsin corporation—and resold copies of the database through the corporation via the Internet.[106] ProCD sued Zeidenberg, seeking to enjoin him from further dissemination of the database contrary to the terms of the end-user license.[107]

Chief Judge Barbara B. Crabb of the Western District of Wisconsin found the licenses unenforceable because prospective purchasers were not able to review the terms on the outside of the package prior to purchasing the software.[108] In so holding, the district court reasoned, "a purchaser does not agree to—and cannot be bound by—terms that were secret at the time of purchase."[109] In reversing the lower court, and rejecting its pro-consumer view, Easterbrook determined that "[n]otice on the outside, terms on the inside, and a right to return the software for a refund if the terms are unacceptable . . . may be a means of doing business valuable to buyers and sellers alike."[110] According to Easterbrook, such ideology has been applied to commonplace unilateral business transactions such as purchasing insurance, airline tickets, concert tickets, and radios.[111] In

104. *See id.* at 1449. For an in-depth discussion of the intersection of Copyright Law and price discrimination, see Wendy J. Gordon, *Intellectual Property As Price Discrimination: Implications for Contract*, 73 CHI.-KENT. L. REV. 1367 (1998), *reprinted in* 5 INTELLECTUAL PROPERTY RIGHTS: CRITICAL CONCEPTS IN LAW 116–37 (David Vaver ed., 2006).

105. *See ProCD*, 86 F.3d at 1450.

106. *See id.*

107. *See id.* at 1447 (listing ProCD's claims "under [the] Copyright Act, Wisconsin Computer Crimes Act, and Wisconsin contract and tort law").

108. ProCD, Inc. v. Zeidenberg, 908 F. Supp. 640, 654 (W.D. Wis.), *rev'd*, 86 F.3d 1447 (7th Cir. 1996).

109. *ProCD*, 86 F.3d at 1450 (discussing district court's basis for finding end-user licenses ineffectual).

110. *Id.* at 1451 (citing E. ALLAN FARNSWORTH, 1 FARNSWORTH ON CONTRACTS § 4.26 (2d ed. 1990)); *see* RESTATEMENT (SECOND) OF CONTRACTS § 211 cmt. a (1981) ("Standardization of agreements serves many of the same functions as standardization of goods and services; both are essential to a system of mass production and distribution. Scarce and costly time and skill can be devoted to a class of transactions rather than to details of individual transactions.").

111. *ProCD*, 86 F.3d at 1451 (citing Carnival Cruise Lines, Inc. v. Shute, 499 U.S. 585 (1991)).

each instance, performance has not been rendered until after payment; yet, Easterbrook argued, "by accelerating effectiveness and reducing transaction costs,"[112] the use of shrinkwrap licenses serves buyers' interests.

Easterbrook further defended his position by putting forth the following anecdotal argument:

> One *could* arrange things so that every concertgoer signs [a] promise [not to record the concert] before forking over the money, but that cumbersome way of doing things not only would lengthen queues and raise prices but also would scotch the sale of tickets by phone or electronic data service.[113]

Thus, the fact that a purchaser has not read the terms of an agreement or has not had the opportunity to read said terms prior to purchase will not absolve the purchaser from those terms once she has consumed the product or service.

The final portion of Easterbrook's opinion examined the pertinent provisions of the Uniform Commercial Code (U.C.C.) in relation to the validity of standard-form user licenses.[114] Easterbrook initially noted (but summarily discounted) that the American Law Institute and National Commissioners on Uniform Law had proposed a new provision as a part of the draft Article 2B—U.C.C. § 2-2203—that would have effectively conceded the invalidity of shrinkwrap licenses under 1996 law.[115] These potentially significant changes in the uniform code that governed contract acceptance were of no particular import to Easterbrook.[116] In addition, Easterbrook eschewed any consideration of U.C.C. § 2-207 (2004) (the "battle-of-the-forms" provision)[117] because the transaction at issue in *ProCD* had "only one

112. *Id.*

113. *Id.*

114. *See id.* at 1452–53.

115. *See id.* at 1452. Specifically, draft section 2-2203 would have made standard-form licenses enforceable only if:

> (a) [P]rior to or within a reasonable time after beginning to use the intangibles pursuant to an agreement, the party
>
> (1) signs or otherwise by its behavior manifests assent to a standard form license; and
>
> (2) had an opportunity to review the terms of the license before manifesting assent, whether or not it actually reviewed the terms.

Mark A. Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239, 1293 (1995).

116. *See ProCD*, 86 F.3d at 1452.

117. *See id.* In 1996, U.C.C. § 2-207 (2004) stated, in pertinent part:

form."[118] To that effect, he reasoned that UCC § 2-204 (2004)[119] controlled, and that "[a] vendor, as master of the offer, may invite acceptance by conduct, and may propose limitations on the kind of conduct that constitutes acceptance."[120] The outcome of Easterbrook's designation of the purchaser as a *de jure* offeree, subject to the whims of the vendor-offeror, is that use of a product or service without express rejection of the accompanying terms amounts to an irrevocable acceptance by the purchaser. Zeidenberg ran the SelectPhone software and, in so doing, subjected himself to the full effect of the Terms of Service (including the inviolate price-discrimination terms).[121]

In the end, Easterbrook surmised that "[t]erms of [service] are no less a part of 'the product' than are the size of the database and the speed with which the software compiles listings."[122] As such, no reasonable consumer could expect to purchase an unencumbered good or service in a capitalist society where business is conducted on a macrocosmic scale. To hold otherwise would require a personalized, case-by-case negotiating scheme with each potential customer prior to purchase; Easterbrook would find such a situation untenable.[123] Thus, Easterbrook placed the burden of bearing the costs of efficient business transactions squarely on the shoulders of consumers, stating that "[c]ompetition among vendors, not judicial revision of a package's contents, is how consumers are protected in a market economy."[124] The following Section examines a concrete example of

> (1) A definite and seasonable expression of acceptance or a written confirmation which is sent within a reasonable time operates as an acceptance even though it states terms additional to or different from those offered or agreed upon, unless acceptance is expressly made conditional on assent to the additional or different terms.
> . . . .
> (3) Conduct by both parties which recognizes the existence of a contract is sufficient to establish a contract for sale although the writings of the parties do not otherwise establish a contract. In such case the terms of the particular contract consist of those terms on which the writings of the parties agree, together with any supplementary terms incorporated under any other provisions of this Act.

U.C.C. § 2-207 (2004).

118. *ProCD*, 86 F.3d at 1452.

119. In 1996, U.C.C. § 2-204 (2004) stated, in pertinent part: "(1) A contract for sale of goods may be made in any manner sufficient to show agreement, including conduct by both parties which recognizes the existence of such a contract." U.C.C. § 2-204 (2004).

120. *ProCD*, 86 F.3d at 1452.

121. *See id*. at 1453 ("Zeidenberg inspected the package, tried out the software, learned of the license, and did not reject the goods.").

122. *Id.*

123. *See supra* text accompanying note 113.

124. *ProCD*, 86 F.3d at 1453.

the consequences of Easterbrook's view of terms of service—and how it can go awry—in an Internet privacy context.

F. The Google Buzz Settlement

In the real world, the "take it or leave it" approach has run up against personal privacy interests to the detriment of consumers (in the form of privacy violations) and businesses (in the form of costly litigation) alike.[125] A recent endeavor by Google to enter the social-networking arena exemplifies the havoc that cloud computing can wreak on Internet privacy under the *ProCD* approach. On Tuesday, February 9, 2010, Google rolled out a social-networking program called Google Buzz (Buzz) that raised serious concerns over the security of users' private information.[126] Buzz was intended to be Google's answer to the popularity of sites like Facebook and Twitter, but the implementation of the Buzz program charted a markedly different course than other social networking sites.[127]

When Google launched Buzz, Gmail users were initially given two options: "(1) set up Google Buzz; or (2) continue to [the user's] Gmail inbox."[128] To the user, then, it would have appeared that choosing the latter option would obviate the former.[129] As it turned out, the notice and choice offered by Google to its Gmail subscribers were merely illusory. Regardless of the option selected by a user, the following events automatically transpired: (1) Buzz was activated; (2) a list of "followers" was created for each Gmail user; (3) a list of persons whom the user was "following" was created;[130] and (4) any information that was previously posted to other websites—for example, YouTube, Picasa and Twitter—was "posted" to Buzz.[131] These actions gave rise to significant consequences for user privacy, including: (1) the "following" and "follower" lists of each user were made publicly available on the web and available to persons follow-

125. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting cases); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 182–83 (D. Conn. 2005); Freedman v. Am. Online, Inc., 329 F. Supp. 2d 745, 749–50 (E.D. Va. 2004).

126. Complaint at 4, *In re* Google User Privacy Lit., No. 10-CV-00672-JW (N.D. Cal. filed July 29, 2010).

127. *See id.*

128. *Id.* at 5.

129. *See id.*

130. "Google created the 'follower' and 'following' lists by using an algorithm that selected those email contacts with whom a Gmail user communicated most frequently. This meant that Google shared information about a Gmail user with the users' frequent mail contacts." *Id.*

131. *Id.*

ing that user; (2) followers could view any information posted on Buzz by someone they were following; (3) the contents of a user's "Google Profile" became visible to all followers;[132] and (4) for users who had created a "Google Profile," the "following" and "follower" lists of the user became visible to all followers and were made publicly available.[133]

These nonconsensual disclosures came as no surprise to Google; in the "Personal Information" section of its Privacy Policy, Google stated, "When you first enter Google Buzz, to make the startup experience easier, we may automatically suggest people for you to follow based on the people you email and chat with most."[134] And, further, "Your name, photo, and the list of people you follow and people following you will be displayed on your Google profile, which is publicly searchable on the Web."[135]

Despite having paid lip service to privacy concerns inherent in the functioning of Buzz and making several modifications to the program,[136] Google failed to prevent a "parade of horribles" from unfolding.[137] An example of these "horribles" involved Andrew McLaughlin, Deputy Chief Technology Officer in charge of Internet policy for the Obama administration.[138] McLaughlin had his "follower" and "following" lists publicly disclosed by Buzz; as a result, he was brought under scrutiny by a consumer advocacy group—which filed a Freedom of Information Act[139] request for personal documents—for potential ties with Google executives.[140] In another example, a woman's personal information was disclosed to an abusive ex-husband when Buzz automatically selected him as her "fol-

132. *Id.* at 6 ("A user's Google Profile may contain information such as the user's occupation, place of residence, and contact information.").

133. *Id.*

134. *Google Buzz Privacy Policy*, GOOGLE (Oct., 2010), http://www.google.com/buzz/help/privacy.html.

135. *Id.*

136. In response to pressure from the United States Congress and the Federal Trade Commission, Google gave users a "second chance" to confirm that "Buzz is set up just the way [they] like it"—requiring users to affirmatively opt-out of public sharing of "follower" and "following" lists. *See* Complaint, *supra* note 126, at 8–9.

137. *Id.* at 7.

138. *Id.*

139. 5 U.S.C. § 552 (2006) (requiring the White House to make "records promptly available" upon request).

140. *See* Jessica Guynn, *Watchdog Group Requests White House Official's E-mail After Google Buzz Mishap*, L.A. TIMES TECH. BLOG (Apr. 1, 2010, 2:13 PM), http://latimesblogs.latimes.com/technology/2010/04/google-buzz-privacy-lobbyist.html.

lower."[141] Perhaps most shocking, Buzz made it possible for lawyers' confidential client and contact lists to be disclosed to the general public without the lawyer's knowledge or consent.[142]

On July 29, 2010, several Gmail users filed a class action lawsuit against Google in the Northern District of California, alleging violations of the Wiretap Act,[143] the Stored Communications Act,[144] the Computer Fraud and Abuse Act,[145] and California common law.[146] The suit essentially amounted to a putative class of Gmail users accusing Google of publicly disclosing private information stored and transmitted through cloud computing technology without notice or consent from its users.[147] Shortly thereafter, on September 3, 2010, the Class agreed to settle its suit against Google, and the following privacy-specific relief was prescribed: (1) changes to the Google Buzz user interface that clarify Buzz's privacy settings; (2) dissemination of wider public education about the privacy aspects of Buzz; (3) establishment of an $8,500,000 fund for Class Administrator fees and expenses, cy pres relief, class-representative incentive payments, attorneys' fees, and costs; and (4) designation of the cy pres recipients as existing organizations focused on Internet privacy policy or privacy education.[148] Thus, for a relatively small fee, and without acknowledging the allegations of the Class, the important privacy issues raised by the lawsuit were disposed of without judicial decision on the merits (approved by the district court as of June 2, 2011).[149]

141. *See* Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. TIMES, Feb. 13, 2010, at B1.

142. *See* Don Cruse, *Lawyers (or Journalists) with Gmail Accounts: Careful with the Google Buzz*, SUP. CT. OF TEX. BLOG (Feb. 11, 2010), http://www.scotxblog.com/legal-tech/lawyer-privacy-on-google-buzz/. *See generally* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (1983) ("A lawyer shall not reveal information relating to the representation of a client.").

143. 18 U.S.C. §§ 2510–2522 (2010).

144. *Id.* §§ 2701–2712.

145. *Id.* § 1030.

146. The pendent state law claim was brought under a tort theory of Public Disclosure of Private Facts. Complaint, *supra* note 126, at 17.

147. *See id.* at 10–17 (laying out the elements of each cause of action).

148. Settlement Agreement at 5, *In re* Google User Buzz Privacy Litigation, No. 5:10-cv-00672-JW (N.D. Cal. Sept. 3, 2010). "'Class Action Administrator' means a mutually agreeable party, to be appointed by the Court, who will facilitate administrative matters and distribution of payments from the Common Fund under the direction of Lead Class Counsel, and who will be paid from the Common Fund." *Id.* at 2.

149. Amended Order Granting Final Approval of Class Action Settlement; Approval of Cy Pres Awards; and Awarding Attorney Fees at 2, No. C10-00672JW (N.D. Cal. June 2, 2011).

In an e-mail to its users dated November 2, 2010, Google tried its hand at transparency while attempting to address the Buzz settlement in a light sympathetic to Google.[150] From the outset, the e-mail phrased Google's recent legal troubles as, "hear[ing] from a number of people who were concerned about privacy" and being "sued by a group of Buzz users," thereby reaching a settlement.[151] Next, the e-mail explained the altruistic outcome that Google intended by entering into the settlement agreement, highlighting that Google "quickly changed the service to address users' concerns," established a multi-million-dollar cy pres fund, and that "[Google] will also do more to educate people about privacy controls specific to Buzz."[152] Importantly, however, Google emphasized that users were not entitled to compensation from the settlement; rather, they should seek comfort in the fact that their increased knowledge of "privacy online" would result in an enhanced "online experience."[153]

The closing points of Google's e-mail illuminate an important aspect of the development of the Internet: a base of Internet users that is educated in the protection of its privacy online is essential to the growth of the Internet as a functional closed frontier.[154] Privacy policies, although informative, merely provide the illusion of user education. Any explanation of an online business's privacy practices will likely be obscured by a lengthy terms-of-service agreement; moreover, the company does not expect the user to open the document and read its provisions. When an Internet user is faced with this situation and her only choice is to "take it or leave it"—with minimal recourse if something goes wrong—she is placed in an unfairly vulnerable position.

II. ANALYSIS

Part I provided a historical view of the interplay between the development of the right of privacy in electronic communications and the form of governance—namely, self-regulation—that has predominated since the birth of the Internet. As examined, the emerging era of cloud computing has created new potential for consumer privacy violations far afield from those envisioned by Warren and Brandeis in the late nineteenth century, and as committed from afar by enti-

150. *See* E-mail from Google to users (Nov. 2, 2010, 3:30 PM EDT) (on file with author).

151. *Id.*

152. *Id.*

153. *Id.*

154. *See supra* note 97.

ties not in privity to any terms of service or privacy policy.[155] Judge Easterbrook's rationale in *ProCD*—concerning the efficacy of utilizing terms of service to conduct business—has been the leading force behind applying the "take it or leave it" approach to online privacy in the cloud, presently taking the form of "clickwrap agreements" (the online equivalent of "shrinkwrap licenses").[156] As demonstrated by the Google Buzz user privacy litigation, such application of Easterbrook's opinion can lead to serious consequences for user privacy in the cloud, with little or no notice to the user and, potentially, without monetary compensation.[157]

Part II assesses the weaknesses of allowing clickwrap agreements to govern the privacy interests of Internet users under the current regulatory scheme. First, Part II examines how *ProCD* has helped to create a liability shield for cloud-based service providers through the use of terms of service and privacy policies. Next, the Section surveys several recent cases that have declined to follow the reasoning of *ProCD* and came out on the side of the consumer. Finally, the Section lays out the pertinent provisions of the ECPA that are pertinent to privacy in the cloud but which have failed to provide the level of personal data privacy required in light of *ProCD*'s "take it or leave it" approach.

A. ProCD *and Its Impact on Terms of Service and Privacy Policies*

Since 1996, online businesses have followed the teachings of *ProCD*, engaging in the practice of conditioning the provision of services to customers on agreement to Terms of Service and, in likewise fashion, Privacy Policies. A modern example is provided by Apple, Inc.'s iTunes Store "Terms and Conditions"[158]—a verbose document approximately eighteen pages in length[159]—which contains within its four corners Apple's Privacy Policy. In observation

155. *See supra* Part I.A–D.

156. *See supra* Part I.E; *see also Click-wrap Agreement Definition*, *supra* note 100 (defining "click-wrap agreement" as the "[w]eb version of the shrinkwrap licensing agreement").

157. *See supra* Part I.F.

158. *iTunes Store – Terms and Conditions*, APPLE, INC., http://www.apple.com/legal/itunes/us/terms.html (last updated Oct. 12, 2011).

159. For users of Apple's iPhone, the iTunes Store "Terms and Conditions" document constitutes no fewer than fifty-five iPhone-screen-sized pages. 8Bit Jay, *iTunes Terms & Conditions: Try Reading 55 Pages on Your iPhone*, ISMASHPHONE.COM (Oct. 3, 2010), http://www.ismashphone.com/2010/10/terms-of-service-who-reads-them.html. Because the usefulness of the iPhone is so intimately tied to the iTunes Store, to respond to the acceptance screen by hitting "Cancel" instead of "Agree" would frustrate the purpose of the device. *See id.*

of this practice, critics have said that "[End User License Agreements] or terms-of-service agreements are long and legalistic, the deals are offered on a take-it-or-leave-it basis and the terms are often oppressive and one-sided."[160] Given that the veracity of that statement has substantial basis in the business realities of Internet commerce,[161] there is strong reason to believe that the security of personal information and content should not be governed in the same fashion as is, for example, a disclaimer of warranties. Privacy is not a commodity to be traded away during the exchange of a commercial transaction; on the contrary, it is a fundamental right that is to be closely guarded from unwanted intrusions. Notwithstanding, "[m]ost Terms of Service allow the provider of . . . cloud service[s] access to data, the ability to view data, and the ability to turn data over in the event that the Government or a third party asks for it. *Often* [*that is*] *true without any notice to the consumer*."[162] This uneven balance of power and privilege presents an untenable potential for abuse.

1. Modern day privacy policies as clickwrap contracts

During the Wild West days of the Internet,[163] there was little, if any, discussion about online privacy; third-party regulation was a distant dream at that time. Gradually, as the Internet's frontier began to close,[164] outside forces have persuaded businesses to implement privacy policies into their normal course of business. Undoubtedly, this is a step in the right direction—toward disclosure to consumers about what information is gathered and stored with every online transaction.[165] Acknowledging this evolution in better business practices, one might still object to its form—i.e., encumbering goods and services with "little-read boilerplate [language] answering questions about what information a website gathers about a user and what it does with the information."[166]

160. Jennifer Granick, *Courts Turn Against Abusive Clickwrap Contracts*, WIRED (Aug. 1, 2007), http://www.wired.com/politics/law/commentary/circuitcourt/2007/08/circuitcourt_0801.

161. *See supra* Part I.E–F.

162. DeVore, *supra* note 10, at 372 (emphasis added).

163. *See supra* text accompanying notes 93–95.

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

165. *See* Zittrain, *supra* note 13, at 69–70.

166. *Id.*

Further, even a cursory reading of the provisions of a privacy policy reveals the extensive permissions granted by the business to itself.[167] For instance, Facebook's Privacy Policy provides, "Even after you remove information from your profile or delete your account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied or stored by other users."[168] This seemingly important statement of post-membership data retention, buried well below the "fold,"[169] demonstrates the "useful fiction" that privacy policies actually put users on notice of a business's privacy practices.[170] This element of procedural unconscionability has provided the impetus for some courts to move away from the *ProCD* line of reasoning.[171]

Indeed, some Internet users may be savvy and sophisticated to the point where they are fully aware of how their information is stored and used by cloud providers. Some may have even read the terms of the privacy policy prior to clicking to verify their assent. Even so, mere knowledge of the privacy practices of a business does not suffice to alleviate concerns with the substance of that practice.[172] "While many individuals are willing to provide information directly in order to fulfill a transaction, they are skeptical about how their information may be used after the transaction has been completed."[173] Moreover, the information stored by cloud providers may be very valuable; if not standing alone, certainly it is valuable in the aggregate.[174] The more detailed and descriptive the information is, the

167. *Id.* at 70 (pointing out that, in relation to user information, privacy policies generally afford a company the ability to gather "as much as it can" and "whatever it wants").

168. *Facebook's Privacy Policy – Full Version*, FACEBOOK.COM, https://www.facebook.com/note.php?note_id=322194465300 (last updated Oct. 29, 2010); *see also More on Gmail and Privacy*, MAIL.GOOGLE.COM, http://mail.google.com/mail/help/intl/en_GB/more.html (last visited Apr. 8, 2012) [hereinafter *Gmail Privacy Policy*] (claiming that the retention of user data even after a message or account has been deleted is "standard practice in the email industry").

169. *See* Erico Nascimento, *Above or Below the Fold of a Web Page?*, APPNOVATION TECHS. (Feb. 2, 2010), http://www.appnovation.com/above-or-below-fold-web-page ("[The fold] is the area of the site that [Internet] users will see without having to scroll. . . . It is commonly said that users won't scroll bellow [sic] the fold [and] won't pay too much attention to the content bellow [sic] that line.").

170. Zittrain, *supra* note 13, at 70.

171. *See infra* Part II.A.2.

172. *See* KIRSTEN M. KOEPSEL & RONALD N. WEIKERS, DATA SECURITY AND PRIVACY LAW: COMBATING CYBERTHREATS § 1:56 (2011), *available at* Westlaw DATASPL.

173. *Id.*

174. *Id.* § 1:57 ("When combined with other information . . . a Social Security number becomes a very valuable piece of information.").

greater potential there is for a business to increase its advertising revenue by selling the information, and, therefore, the user will be less likely to want to part with it.[175] Of course, the user has the option of clicking "Cancel," thereby depriving herself of the service. Thus, assuming that a business makes its policies[176] entirely transparent to users prior to any binding transaction, the user remains in the precarious position of either taking the terms-encumbered service or leaving the service, only to seek out an equally undesirable alternative.

Not to be outdone, some cloud providers affirmatively recognize the damaging potential that long-term storage of personal information may have for their users' privacy interests. For example, Google's Privacy Policy contains the following caution in the "Conclusion" section—again, below the fold[177]—to Gmail users:

> Let's be clear: there are issues with email privacy, and most of these issues are common to all email providers. The main issue is that the contents of your messages are stored on mailservers for some period of time; there is always a danger that these messages can be obtained and used for purposes that may harm you, such as possible misuse of your information by governments, as well as by your email provider. *Careful consideration of the relevant issues, close scrutiny of email providers' practices and policies, and suitable vigilance and enforcement of appropriate legislation are the best defenses against misuse of your information*.[178]

This statement is characteristic of the attitude of cloud providers and, quite frankly, is a blatant deflection of responsibility from Google to its users and regulatory enforcement agencies. Treating non-committal statements like the one above as part of the "product" to benefit convenience and business efficiency, as Easterbrook would,[179] jeopardizes the privacy interests of the user.

175. *Id.* § 1:56.

176. Cloud provider privacy policies tend to cover the same basic practices: (1) Information Collection and Use; (2) Information Sharing and Disclosure; (3) Cookies; (4) Confidentiality and Security; (5) Data Retention; and (6) Change of Policy Terms. *See, e.g.*, *Privacy Policy*, YAHOO! (Nov. 22, 2006), http://info.yahoo.com/privacy/us/yahoo/details.html.

177. *See supra* note 169.

178. *Gmail Privacy Policy*, *supra note* 168.

179. *See supra* text accompanying note 112.

2. Retiring Easterbrook's approach

In the non-privacy world, courts are evolving and limiting the adhesive power of clickwrap contracts. At the state-court level, in *Gatton v. T-Mobile USA, Inc.*, the California Court of Appeals held that a cellular phone company's service agreement was unenforceable because of the one-sided results of the agreement, as well as the lack of a meaningful choice for the consumer.[180] In so holding, the court stated, "Although contracts of adhesion are well accepted in the law and routinely enforced, the inherent inequality of bargaining power supports an approach to unconscionability that preserves the role of the courts in reviewing the substantive fairness of challenged provisions."[181] Allowing such judicial review recognizes the tremendous obstacles that modern consumers have had to overcome in the face of corporate attempts to limit remedial avenues, and advances the possibility of a level playing field for arms-length negotiation.[182]

At the federal level, in *Douglas v. U.S. District Court*, the Ninth Circuit held that a service provider could not make changes to the terms of a service agreement by posting those changes on its website without notice to the customer.[183] Even though customers had the option of switching providers, the mere fact that they continued using the service from the original provider did not bind them to the new terms.[184] Unlike Easterbrook, the *Douglas* court held that the use of a good or service with opportunity to reject did not necessarily constitute assent to terms that arose after the original transaction.[185]

The line of reasoning employed in these two cases demonstrates the potential for transparency and equality in the field of commercial technology: "*Gatton* and *Douglas* show courts are moving away from applying a simplistic theory of contract formation toward developing legal rules that are more attuned with the modern marketplace and balance of power."[186] The public interest benefit of such a shift should outweigh the incremental detriment that businesses will experience when they are forced to develop new procedures to

180. 61 Cal. Rptr. 3d 344, 356–58 (Cal. Ct. App. 2007), *cert. denied*, 553 U.S. 1067 (2008).

181. *Id.* at 355.

182. *See* Granick, *supra* note 160.

183. 495 F.3d 1062, 1066–67 (9th Cir. 2007) (per curiam).

184. *See id.* at 1068.

185. *Compare id.*, *with* text accompanying note 110, *and* text accompanying notes 119–20.

186. Granick, *supra* note 160.

transact with consumers.[187] Notwithstanding any such detriment, placing the burden of protecting consumer privacy on businesses will likely breed new business methods and marketable inventions designed to enhance online privacy. Thus, although the unabashedly pro-consumer views put forth in the lower-court decisions in *ProCD, Inc. v. Zeidenberg*[188] and *Klocek v. Gateway, Inc.*[189] have yet to be found persuasive in the online arena, it appears that the time is ripe for the advancement of online privacy laws that better represent the interests of the consuming public.

B. Pitfalls of the ECPA in Protecting Personal Data Privacy

As demonstrated by the Google Buzz privacy litigation discussed above,[190] the ECPA may provide the basis for a cause of action at law for damages caused by a cloud provider's commission of the statutory prohibitions of the Act.[191] Unfortunately, however, the class of Gmail users in the Buzz suit decided to settle with Google and, therefore, no determination on the merits of the claims followed. Additionally, case law discussing the civil aspects of the ECPA is relatively sparse, and the Supreme Court has not had the occasion to interpret the civil provisions of the Act.[192] In an age where all aspects of life are significantly affected by the presence of the Internet, it is of great importance that the corresponding law is clear, direct, and comprehensible to the lay and expert user alike.

The statutory protection afforded by the ECPA is regularly regarded as insufficient, and commentators often attempt to convince

187. *See id.*

> This is a good development for consumers, who would otherwise be saddled by oppressive terms they have neither the legal sophistication to understand nor the bargaining power to avoid, and for the public interest, which suffers when customers are forced to waive rights that capitalist democracies rely on for innovation and accountability.

Id.

188. "Mere reference to the terms at the time of initial contract formation does not present buyers an adequate opportunity to decide whether they are acceptable. They must be able to read and consider the terms in their entirety." 908 F. Supp. 640, 654 (W.D. Wis.), *rev'd*, 86 F.3d 1447 (7th Cir. 1996).

189. "In typical consumer transactions, the *purchaser is the offeror*, and the vendor is the offeree." 104 F. Supp. 2d 1332, 1340 (D. Kan. 2000) (emphasis added).

190. *See supra* Part I.F.

191. *See* 18 U.S.C. §§ 2520, 2707 (2011).

192. *See* Mattei-Ferraro, *supra* note 60, at 711–12.

Congress to amend the outdated provisions of the Act.[193] For example, one commentator has opined that the ECPA is "a very complicated statute," attempting to apply 1986 law to what is going on twenty-five years later "in a world that is changing dramatically every couple of years if not every couple of months, with the law struggling to catch up at every step."[194] The Act's verbiage, including "electronic communication," "electronic storage," and "remote computing service" may have been workable in the pre-World Wide Web 1980s,[195] but modern Internet users in similar transactions speak in terms of "e-mail," "HTML," "packet," and "ISP."[196] It is conceivably much simpler to attempt to define what an e-mail is in an Internet-specific context than it is to interpret the exceedingly broad "electronic communication."[197] A federal statute's shelf life may be considerably longer than thirty years, and the law enacted may be readily applicable to future generations; however, in the case of statutory language governing rapidly changing fields such as the Internet and technology in general, the law must advance in tow.

Further, the ECPA's substantial focus on prohibiting criminal violations of privacy—specifically, communications intercepted in transit or in electronic storage[198]—detracts from the already scant civil remedy afforded to Internet users. Even so, it appears that Justice Black's characterization of the "'broad, abstract and ambiguous concept' of 'privacy'"[199] put forth by the majority in *Katz v. United States* has come to bear in the criminal context. Moreover, despite Congress's intent to protect against the unauthorized disclosure of personal information by public officials and private parties,[200] less energy has been spent on regulating the actions of the private sector: "[I]n the context of a civil proceeding, the [ECPA] affords virtually

193. *See, e.g.*, DeVore, *supra* note 10, at 371; Mattei-Ferraro, *supra* note 60, at 712–14; Kerr, *supra* note 59, at 1208; *see generally* DIGITAL DUE PROCESS, *supra* note 65 (advocating for the simplification, clarification, and unification of the ECPA's "patchwork of confusing standards that have been interpreted inconsistently by the courts").

194. DeVore, *supra* note 10, at 371.

195. *See supra* text accompanying notes 55–59.

196. *See Glossary of Internet & Web Jargon*, U.C. BERKELEY LIBR., http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/Glossary.html (last updated Feb. 6, 2011).

197. *See supra* note 50 and accompanying text.

198. *See* 18 U.S.C. §§ 2510, 2701(a)–(b) (2011).

199. 389 U.S. 347, 374 (1967) (Black, J., dissenting) (quoting Griswold v. Connecticut, 381 U.S. 479, 509 (1965) (Black, J., dissenting)).

200. *See* United States v. Councilman, 418 F.3d 67, 80–81 (1st Cir. 2005) (quoting S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557).

no statutory protection—and there is correspondingly little constitutional protection—for the great bulk of business communications or other work documents stored with a third party online."[201] Thus, as the law currently stands, businesses engaged in Internet commerce have very few incentives to protect the privacy of the very parties who are most vulnerable—the users.

Finally, even assuming that the prima facie privacy protections of the ECPA as originally drafted are sufficient, the statutory safe harbors for ISPs—including cloud providers—cast an unacceptably wide net. Because the right to a private civil action arises only upon violation of the criminal provisions of the Act,[202] a criminally immune ISP will likewise be exempt from civil liability. Under section 2703(e) of Title II of the Act, an ISP is expressly exempted from civil liability when it acted in compliance with the terms of a "court order, warrant, subpoena, statutory authorization, or certification under this chapter."[203] Although facially consistent with constitutional mores, the Act "allows a court to issue an order based on less than probable cause, allowing the government to search a [person's] email communications stored with an electronic service provider for more than 180 days."[204] Thus, a potential civil right of action for an aggrieved user may vanish solely upon a showing of "reasonable grounds"[205] and/or with little or no notice to the user.[206] Additionally, under section 2701(c)(1) of the Act, an ISP may indiscriminately search user-created content and personal information stored on its server without fear of liability.[207] As such, the criminal provisions of the ECPA do not apply to an ISP that "'obtains, alters, or prevents authorized access to a[n]' e-mail while it is in 'electronic storage' in such system."[208] By giving ISPs such free reign, the Act effectively

201. DeVore, *supra* note 10, at 371.

202. *See* 18 U.S.C. § 2707(a) (2012) (establishing a cause of action for "any . . . person aggrieved by any violation of this chapter").

203. *Id.* § 2703(e).

204. Warshak v. United States, 532 F.3d 521, 534 (6th Cir. 2008) (Martin, J., dissenting) (citing 18 U.S.C. § 2703(d)).

205. *See* 18 U.S.C. § 2703(d) (2006).

206. *See id.* § 2703(b)(1) (providing for compelled disclosure of "the contents of any wire or electronic communication" without notice under the Federal Rules of Criminal Procedure, with prior notice, or with delayed notice under section 2705 of Title II of the Act).

207. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2003) ("[W]e read [section] 2701(c) literally to except from Title II's protection all searches by communications service providers.").

208. United States v. Councilman, 418 F.3d 67, 81 (1st Cir. 2005) (reading the immunity provision of section 2701(c) into the main criminal provision of 18 U.S.C. § 2701(a)).

eviscerates any expectation of privacy possessed by users in e-mail or other Internet communications.[209]

Of course, the antiquated posture of the ECPA is only one link in the chain of the inadequate legal regime surrounding Internet privacy law. If it is true, as a plurality of commentators have said, that the ECPA is in need of a makeover, amendment is a good idea; however, merely attempting to rework a broken criminal act will not sufficiently protect people's interest in obtaining civil remedies for violations of privacy online. As such, Congress should enact a separate, Internet-specific remedial statute to guard such privacy interests.

III. PROPOSED SOLUTION

The apparent dichotomy between consumer privacy and corporate efficiency strikes a delicate balance which, to date, has tipped in favor of the party with the most bargaining power—corporations. This imbalance has likely resulted from at least three beliefs about the current Internet frontier: (1) people are nonchalant in their online dealings and passively consent to use of their personal information; (2) corporations are in the best position to protect people's online privacy concerns; and (3) the legislative process itself is inefficient, and change is difficult to achieve.[210] These arguments, although reasonable, do not account for the realities of what Internet commerce has become and how important a well-protected Internet is to the preservation of sacrosanct civil freedoms.

To the first point, what at first glance appears to be a blasé attitude on the part of Internet users, may be explained by the growing disconnect between sender and receiver that has come about with the rise of the Internet: "Since the days of Warren and Brandeis, technology has developed to a degree that invasion of privacy no longer requires physical proximity. In fact, technology has advanced so rapidly that the average citizen is unaware of the capabilities of most organizations to capture and store private information."[211] This lack of face-to-face contact requires users to hand over information to a cloud rather than a human in exchange for services that average citizens see as essential to their daily lives.

209. *See generally* Mitchell Waldman, Annotation, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5th 15 (2001) (discussing, *inter alia*, the implications of the ECPA on Internet users' expectation of privacy in online correspondence).

210. *See* Zittrain, *supra* note 13, at 69.

211. KOEPSEL & WEIKERS, *supra* note 172, § 1:55.

Further, individual privacy interests are defined in large part by subjective proclivities. For instance, "social, cultural, religious, political, and economic influences" may inform what a particular user deems "private."[212] This variety of competing influences is particularly relevant in an age where it is no longer an absurd notion that a peeping Tom could accuse his prey of public indecency. The bright-line rule established in *ProCD*[213] does nothing to compensate for this warped public/private distinction or the diversity of the Internet's constituency. The attempted remedy—attaching corporate privacy policies to must-accept terms of service—has served only to exacerbate the problem by providing businesses a potential liability shield without engendering transparency as those businesses have advertised. Legislation in this area should take into account the reality that consumers are not savvy and, as a consequence, do not understand the technical exactitudes of information storage.

Balanced against this, the importance of free-flow information[214] must also inform the lawmakers. The self-regulation scheme that has proliferated since the dawn of the Internet has had certain upsides—mostly supporting the business world—but the consumer has also benefited from advances in convenience, increased competition among vendors, and the progress of innovative technology and the enhancement of the quality thereof. New legislation should not seek to eradicate all storage and usage of information; it should aim to reign in practices that overstep the bounds of personal privacy.

Congress should look to existing state law as a guide to help ease the legislative process. To date, forty-two states and the District of Columbia have enacted statutory provisions that require full and immediate notification to the user in the event that personal information stored on a third-party server has been compromised.[215] For instance, Washington state law requires that

> [a]ny person or business . . . that owns[, maintains] or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the

212. *Id.*

213. *See supra* text accompanying note 110.

214. *See* KOEPSEL & WEIKERS, *supra* note 172, § 1:55 ("Information enables companies to provide better services or products, to market more effectively and to better utilize resources. Information also results in lower costs for consumers.").

215. For a discussion of the notification statutes, see G. Martin Bingisser, *Data Privacy and Breach Reporting: Compliance with Various State Laws*, 4 SHIDLER J. L. COM. & TECH. 9 (2008).

> security of the data to any [person] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[216]

The terms of this provision are easily definable in context, and are given further precision within the Code. Importantly, the Washington provision states as follows:

> For purposes of this Section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, *when either the name or the data elements are not encrypted*:
>
> (a) Social security number.
> (b) Driver's license number or . . . Identification Card number.
> (c) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.[217]

Of those states that have enacted such a provision, however, only seven maintain a private cause of action for individuals who have fallen victim to a security breach of a cloud server on which their personal information is stored.[218] For example, California law provides that "[a]ny customer injured by a [security breach] may institute a civil action to recover damages."[219] Additionally, "[a]ny business that violates, proposes to violate, or has violated" the customer's privacy in her personal information may be enjoined,[220] and a "prevailing plaintiff . . . shall be entitled to recover his or her reasonable attorney's fees and costs."[221] The allowance for both legal and equitable remedies under a federal statute would provide incentive for cloud providers to enhance the security of their servers

216. WASH. REV. CODE ANN. § 19.255.010(1)–(2) (West 2012).

217. *Id.* § 19.255.010(5) (emphasis added).

218. *See, e.g.*, Louisiana Data Security Breach Notification Law, LA. REV. STAT ANN. § 51:3075 (West 2011); Tennessee Identity Theft Deterrence Act of 1999, TENN. CODE ANN. § 47-18-2104 (West 2012).

219. CAL. CIV. CODE § 1798.84(b) (West 2012). A customer may recover up to three thousand dollars ($3000) per violation if the service provider acted willfully, intentionally, or recklessly; otherwise, the customer may recover up to five hundred dollars ($500) per violation of the California statute. *Id.* § 1798.84(c).

220. *Id.* § 1798.84(e).

221. *Id.* § 1798.84(g).

rather than allowing the providers to continue hiding behind their privacy policies and terms of use.

As such, the proposed federal statute would require cloud providers to operate under greater transparency in its privacy practices. As discussed above, the advent of privacy policies over the years has evinced progress towards educating the consumer about online privacy, but the use of privacy policies and terms of use has not necessarily served to protect the consumer.[222] Rather, those documents merely stand as potential liability shields for cloud providers, especially when privacy policies are hidden within complex terms of use or in small, indistinguishable type.[223] The California statute makes this practice illegal by instructing businesses to add the words "Your Privacy Rights" in the "same style and size as the link to the business's privacy policy."[224] Further, if a business does not have a privacy policy, then the words "Your Privacy Rights" shall be written in distinguishable and obvious style and size, and the home page shall link to a page that describes a customer's rights pursuant to the California statute.[225] Thus, the California statute provides helpful guidance for potential congressional legislation.

Under the proposed law, the security of such information can be obtained lawfully and guarded through encryption—a cost-effective measure.[226] In the event of a security breach, detailed notice to the user and immediate restoration of the integrity of the system would be required;[227] the lack thereof would result in the availability of statutory damages per violation. Further, cloud providers could no longer turn a blind eye to the privacy problem by hiding behind dense privacy policies and terms of service. This type of rule recognizes the aggregate value of information and gives guidance as to the information that should be protected most zealously by cloud providers. Moreover, due to the strong interest of the federal government in regulating interstate commerce,[228] protecting personal information across the Internet in the same way as the several states

222. *See supra* text accompanying note 165.

223. *See supra* notes 158–59 and accompanying text.

224. CAL. CIV. CODE § 1798.83(b)(1)(B) (West 2005).

225. *Id.*

226. *See* Zittrain, *supra* note 13, at 71; *see also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 172–73 (2000) (describing how encryption could help "individual internet users . . . come close to realizing Louis Brandeis and Samuel Warren's [privacy] ideal").

227. *See* WASH. REV. CODE § 19.255.010(1).

228. *See* U.S. CONST. art. I, § 8, cl. 3 (establishing Congress's power "to regulate Commerce with foreign Nations, and among the several states").

above would alleviate privacy violations nationwide. The federal codification of such a rule would also promote uniformity across jurisdictions and bring a sense of certainty to American Internet users and online corporations.

Based on the foregoing, Congress should repeal the antiquated civil provisions of the ECPA[229] and enact legislation that provides more clarity to business and user alike and obviates the need for privacy policies contained within prolix terms-of-service agreements. As an additional incentive for better business practices, the ECPA should go through its own amendment process in order to better protect users' personal information in a criminal context. Technology is only going to grow more intrusive as time passes; America needs to ensure that it adequately prepares for the next wave of innovation in the field of communication technology.

CONCLUSION

Privacy and efficiency need not be mutually exclusive areas of concern; rather, society must learn to adapt newly emerging technologies to benefit both sides of the issue.[230] On the one side, the public has a strong interest in the fundamental right to exclude others from the intimate details of one's life—as propounded by Warren and Brandeis. On the other side, the mass-market design of Internet commerce necessarily requires a certain degree of efficiency and convenience in online transactions. Although this principle may have been correctly applied in *ProCD* on its facts, the resulting legal developments have placed all of the bargaining power in the hands of the corporation. This unfairness became particularly evident when businesses began to include the sole notice of their policy practices within verbose terms-of-service agreements, conditioning the provision of services upon acceptance of both. All the while, existing law has done little to clear up the confusion and, in fact, has created a greater schism between privacy interests and efficient business practices—as evidenced by the Google Buzz user privacy litigation. The answer to this problem is not mere amendment or reinterpretation of current law; rather, new law needs to be enacted that provides clarity, uniformity, and a viable cause of action for consumers who are harmed by violations of their privacy. Online

229. 18 U.S.C. §§ 2520, 2707 (2006).

230. *See* Berson, *supra* note 12 ("Cloud computing is here now, and is the future; we just have to learn how to manage risks.").

corporations will benefit from the development of new business methods and innovations in security technology, and Internet users will be able to protect their personal information as jealously as they deserve.