2013

# Pass Parallel Privacy Standards or Privacy Perishes

Anne T. McKenna
*Penn State Law*

# PASS PARALLEL PRIVACY STANDARDS OR PRIVACY PERISHES

*Anne T. McKenna**



* Anne T. McKenna is a Partner at the law firm of Silverman, Thompson, Slutkin & White LLC, where she chairs the firm's Internet and Privacy Law Group, SilverMcKenna. Ms. McKenna is also Adjunct Faculty at The Catholic University of America, where she teaches media law, First and Fourth Amendment issues, and privacy law. Ms. McKenna is co-author of two treatises: CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (3rd ed. 2007), and CLIFFORD S. FISHMAN & ANNE T. MCKENNA, JONES ON EVIDENCE (7th ed. 2008). Ms. McKenna gratefully acknowledges the invaluable assistance of Michelle Lease in additional research and assistance with this Article. Ms. Lease is a 2014 J.D. Candidate and Law and Public Policy Certificate Candidate at The Catholic University of America, Columbus School of Law. Prior to law school, Ms. Lease was a Staff Aide to Chairman Sharon Bulova of the Fairfax County Board of Supervisors. Ms. Lease has interned with the D.C. Sentencing and Criminal Code Revision Commission, The Lawyers' Committee for Civil Rights Under Law, and most recently as a 2013 law clerk at SilverMcKenna.

## I. INTRODUCTION

This Article stems from my presentation at a Symposium hosted by Rutgers School of Law-Newark in March 2013, where I asserted that private industry's ability to surreptitiously gather, collect, store, and sell vast amounts of intimate, personal data constitutes a far more insidious threat to privacy than that posed by government electronic snooping, because government is bound by the constraints of the Fourth Amendment[1] and the federal wiretapping and electronic surveillance legislative scheme. I asserted that our constitutional concept of individual privacy and the protection we afford to the same will be eviscerated by the activities of private industry lest Congress act to protect individual privacy and an individual's power to control the data gathered, collected, stored, and sold by private industry in ways similar to the protections afforded individuals from such government activity by constitutional, legislative, and common law.

But headline events impacted my premise.

In June 2013, Edward Snowden's leaks about the National Security Agency's (NSA) wholesale Internet and cellular surveillance of all United States citizens' electronic activities—including, but not

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

limited to, Internet activity and constant geolocation data—and the Foreign Intelligence Surveillance Court's (FISC or FISA court) secret judicial support of such techniques changed the game.[2] While some privacy advocates and U.S. Senators had warned of such invasive government surveillance,[3] Snowden's leaks crystallized its scale. After weeks spent reading every internecine development in the story and updating research, the conclusion: Yes, the revelations required rewriting sections of this Article, but, in short, the new information strongly bolstered the grounds for this proposal.

Technological advances have turned our privacy jurisprudence on end. Applying the traditional reasonable expectation of privacy analysis and the third-party doctrine to advanced technologies and Internet-based activity requires courts to engage in absurd legal acrobatics[4] to preserve any sense of privacy.

The proposal: (1) We legislatively define what individual privacy is; (2) we do so independent of technology-specific language; (3) we restrict and legislatively regulate private industry *and* government surveillance, collection, storage, use, and distribution of data in the same or parallel ways; and (4) we legislatively provide individuals with the right to know and/or control (a) what data is collected about them, (b) who is collecting such data, (c) what data is retained, and (d) how such data is used.

As explained below, private industry tracks 24/7 our physical location, online travels, friends, activities, likes and dislikes, preferences (including religious and sexual), personal status (married, divorced, or single), and financial status.[5] Such tracking is accomplished in myriad ways and, more increasingly, it is done using individuals' biometric identifiers.[6] In the process of this tracking, private industry collects, stores, and sells an astonishing amount of personal data.[7] The Supreme Court is uncomfortable with twenty-

---

2. *See* Alexis C. Madrigal, *NSA Leak Catch-Up: The Latest on the Edward Snowden Fallout*, THE ATLANTIC (June 17, 2013, 3:51 PM), http://www.theatlantic.com/technology/archive/2013/06/nsa-leak-catch-up-the-latest-on-the-edward-snowden-fallout/276926/.

3. Brian Knowlton, *Lawmakers Mostly Defend Surveillance*, N.Y. TIMES, June 10, 2013, at A12.

4. As Justice Alito so famously stated in pointing out the problems of applying traditional privacy concepts to modern technologies: "The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both." United States v. Jones, 132 S. Ct. 945, 958 n.3 (2012) (Alito, J., concurring).

5. *See infra* Part IV.A-B.

6. *See infra* Part III.C.

7. *See* Daniel Zwerdling, *Your Digital Trail: Private Company Access*, NPR.ORG (Oct. 1, 2013, 2:00 PM), http://www.npr.org/blogs/alltechconsidered/2013/10/01/227776072/your-digital-trail-private-company-access.

eight days of 24/7 warrantless GPS tracking,[8] but nothing stops private industry from engaging in the same.[9] Snowden's NSA surveillance revelations and publication of secret FISA court orders irrefutably demonstrate that private industry's vast databases are open season for government investigators.[10]

This Article first summarizes our privacy law framework; it next discusses technological advances that permit invasive data gathering and how private industry uses these advances to track us; then it considers the problems posed by application of traditional privacy jurisprudence concepts to advanced technologies; and, lastly, this Article proposes a legislative solution.

## II. THE CURRENT STATE OF PRIVACY LAW: AN OVERVIEW

### *A. The Constitution*

#### 1. The Right to Privacy Concept

The word "privacy" does not appear in the United States Constitution.[11] In the seminal 1890 Harvard Law Review article, *The Right to Privacy*, Samuel Warren and Louis Brandeis framed our modern constitutional and common law concepts of privacy.[12] Thanks in part to Warren and Brandeis's article, our Constitution—despite missing the magic *privacy* word—is the cornerstone of modern privacy law.[13]

There are some marked similarities between today's societal and legal privacy struggles and those of the 1890s. At the time Warren and Brandeis's article was published, American society was facing aggressive, sensationalistic press;[14] there was incredible growth in newspaper circulation rates,[15] which fueled the financial rewards

8. *See Jones*, 132 S. Ct. at 949.

9. *See, e.g.*, *Fact Sheet 18: Online Privacy: Using the Internet Safely*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/content/online-privacy-using-internet-safely (last visited Nov. 3, 2013).

10. *See* Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, THE GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

11. *See* U.S. CONST.; *see also* Mark Silverstein, Note, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 218 (1989).

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

13. *See generally id.*

14. The term "Yellow Journalism" was coined to describe private press activities of the time. JOSEPH W. CAMPBELL, YELLOW JOURNALISM: PUNCTURING THE MYTHS, DEFINING THE LEGACIES 33 (2001).

15. James H. Barron, *Warren and Brandeis,* The Right to Privacy*, 4 HARV. L. REV. 193 (1890): Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875, 889-90 (1979).

reaped from more invasive, intrusive newsgathering activities;[16] and technological developments flourished, including readily available and affordable photography devices[17] and recording devices,[18] both of which permitted individuals to be recorded and photographed at an unprecedented rate.[19] These factors—(1) legally unfettered gathering of personal data (2) by private industry for commercial gain (3) enabled through advanced technologies—combined to foster invasions of individual privacy on a scale heretofore unimaginable.[20] When boiled down to the aforementioned factors, which spurred Warren and Brandeis to write their article and advocate for a new legal right, connecting the dots further is unnecessary: The similarity of the privacy problems today and those in 1890 is strikingly similar.

In their introduction to *The Right to Privacy*, Warren and Brandeis overview the Anglo-American jurisprudence system that enables our law's developmental flexibility to keep abreast of social, political, and technological changes.[21] The authors then highlight how—enabled by developments in technology—the sacred precincts of private and domestic life were being invaded in ways not previously possible.[22] Warren and Brandeis ask whether existing laws in 1890 were capable of protecting the privacy of the individual.[23] After an analysis of available legal remedies,[24] the two conclude that, while some laws may hinder certain types of privacy invasion (e.g., libel and slander), existing laws were too limited in stopping unwanted personal data gathering by private industry.[25] Warren and Brandeis contend that there is a general right to privacy that, if properly understood, affords a remedy for the insidious, intrusive invasions of the right.[26]

By providing the factual stage and describing in detail the nature of injury caused by privacy invasions, Warren and Brandeis unequivocally demonstrate the societal need for a new right.[27] The two then persuasively explain how the right to privacy is both

16. *See id*. at 891.

17. This era saw the mass market introduction of Kodak's small snap camera. History of Kodak Milestones 1879-1929, KODAK, http://www.kodak.com/country/US/en/corp/kodakHistory/1878_1929.shtml (last visited Nov. 3, 2013).

18. *See* DAVID R. SPENCER, THE YELLOW JOURNALISM: THE PRESS AND AMERICA'S EMERGENCE AS A WORLD POWER 54 (David Abrahamson, ed., 2007).

19. *See, e.g.*, *id.* at 2-3.

20. *See, e.g.*, Barron, *supra* note 15, at 889-91.

21. Warren & Brandeis, *supra* note 12, at 193-95.

22. *See id.* at 195.

23. *See id.* at 197.

24. *See id.* at 197-207.

25. *See id.* at 207.

26. *See id.* at 198.

27. *See id*. at 197-98.

derived from and present throughout our common law and historical concepts of "an inviolate personality" and "the right to be let alone."[28] Pointing to privacy protections afforded by tort law, evidence, property rights, contract law, and criminal law, the two establish that the right to privacy is not a new concept, but something carried throughout all of these sources of common law, constitutional law, and statutory law.[29] Warren and Brandeis frame what the scope of the right to privacy is, outline the remedies it should afford, and reject criticisms of the recognition of the right to privacy they foresee.[30] As we know, Warren and Brandeis's proposed common-law right to privacy was ultimately recognized and adopted by the United States Supreme Court and by state courts and state legislatures across the nation.[31]

2. The Fourth Amendment

The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[32]

The Fourth Amendment applies only to government search and seizure.[33] It does not apply to private industry or third-party search and seizure.[34] While the Fourth Amendment provides no enforcement or privacy protections against private industry's collection and use of personal data, it may provide a guiding framework for restricting and regulating private industry's personal data collection and use. Due to space constraints, this Article must assume readers are generally aware of the Supreme Court's Fourth Amendment jurisprudence, and the Court's development of the reasonable expectation of privacy test and the third-party doctrine.[35] This Article considers the Court's

28. *Id*. at 193, 197-205.

29. *See id*. at 197-214.

30. *See id*. at 214-20.

31. *See generally* Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623 (2002) (examining the legal impact and legacy of *The Right to Privacy*); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479 (1990) (tracing the development of privacy rights from *The Right to Privacy*).

32. U.S. CONST. amend. IV.

33. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

34. *See id.*

35. *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) (discussing reasonable expectation of privacy test); Stephen

more recent, technology-specific Fourth Amendment cases to illustrate the vexing application of the Fourth Amendment, the reasonable expectation of privacy test, and the third-party doctrine to emerging surveillance technology and existing digital data collection practices and geolocation tracking.

### *B. The Federal Legislative Scheme*[36]

In 1968, in response to considerable social and political activity on a variety of fronts, Congress enacted the Omnibus Crime Control and Safe Streets Act.[37] Title III of that Act regulates interception of communications by public officials and private persons.[38] In general terms, the electronic surveillance statutory scheme developed by Congress is collectively referred to as Title III.

Congress enacted Title III with two primary goals in mind. First, it sought to safeguard the privacy of wire and oral communications[39]—electronic communications were added to the statute's coverage in 1986[40]—and, in particular, the privacy of innocent persons.[41] Thus, Title III forbids the interception of wire, oral, or electronic communications by private persons unless the communication is intercepted by, or with the consent of, a participant, and significantly restricts the authority of law enforcement officials to intercept such communications.[42] Second, Title III sought to provide law enforcement officials with a much-needed weapon in their fight against crime, particularly organized crime,[43] by empowering them to intercept such communications

---

E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011) (discussing third-party doctrine).

36. Portions of this discussion have been excerpted from 1 CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (3d ed. 2012), which provides a much more extensive discussion of the federal electronic surveillance legislative scheme.

37. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801(b), 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2012)).

38. *Id.*

39. § 801(b), 82 Stat. at 211; S. REP. NO. 90-1097, at 37, 60 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153, 2177; *see also* State v. Gilmore, 549 N.W.2d 401, 405 (1996) ("[T]he Senate Report accompanying Title III underscored that 'protecting the privacy of wire and oral communications' was a chief congressional concern in enacting the law."); FISHMAN & MCKENNA, WIRETAPPING & EAVESDROPPING, *supra* note 36, § 1.6, at 1-14.

40. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522 (2012)).

41. § 801(d), 82 Stat. at 211; S. REP. NO. 90-1097, at 60.

42. Omnibus Crime Control of Sale Streets Act of 1968, Pub. L. No. 90-351, § 2511(2)(c), 82 Stat. 197, 214 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (2012)).

43. § 801(c), 82 Stat. at 211; S. REP. NO. 90-1097, at 40, 60.

under carefully regulated circumstances.[44] With regard to the latter goal, Congress endeavored to satisfy the procedural and substantive requirements previously enunciated by the Supreme Court in *Berger v. New York*[45] and *Katz v. United States*[46] as constitutional prerequisites to a valid communication interception statute[47] while defining "on a uniform basis"—applicable to state as well as federal government—"the circumstances . . . under which the interception of wire and oral communications [and, subsequently, electronic communications] may be authorized" by a judicially issued interception order.[48]

Title III provides a detailed legislative scheme. It specifies who may authorize an investigator to apply for a court order, the information an application must contain, the findings a judge must make before issuing the order, how the order is to be executed, how recordings of intercepted conversations are to be secured, who must eventually receive notice that a phone or other communications facility was tapped or a location was bugged, among other details.[49] The statute describes when information obtained from intercepted communications may be disclosed, identifies who may seek to suppress evidence and on what grounds, and sets forth an exclusionary rule.[50] It also creates a civil cause of action for those whose communications are unlawfully intercepted.[51] An in-depth analysis of the federal electronic surveillance legislative scheme is well beyond the scope of this Article. For our purposes, however, there are components of this scheme that we must briefly consider.

The Electronic Communications Privacy Act of 1986 (ECPA) amended Title III's definition of "wire communication" to include "electronic" communications.[52] The broad definition of "electronic" communications brings a host of modern, Internet-based communications within the ECPA's purview.[53] In terms of tracking devices, a method by which private industry surreptitiously and

44. S. REP. NO. 90-1097, at 40-46.

45. 388 U.S. 41, 51 (1967) (holding that conversations are protected by the Fourth Amendment and that the capture of conversations using electronic devices constitutes a search).

46. 389 U.S. 347, 353, 359 (1967) (enunciating that the Fourth Amendment protects persons in addition to property and that Fourth Amendment protection guarantees a reasonable expectation of privacy).

47. S. REP. NO. 90-1097, at 44-46.

48. *Id.* at 37.

49. *See* Pub. L. No. 90-351, 82 Stat. 211, 216-23 (1968).

50. *Id.* at 222-25.

51. *Id.* at 223.

52. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(a)(6), 100 Stat. 1848, 1848-1849 (1986) (codified as amended at 18 U.S.C. § 2510 (2012)).

53. *See id.*

consistently gathers our geolocation data unfettered by statutory restraints, there are only two federal statutes that directly address the use of tracking devices, and they only apply to law enforcement.[54] The Pen/Trap Statute regulates the use of pen/trap devices,[55] and the Stored Communications Act (SCA) also regulates storage of and access to stored electronic communications.[56]

The Communications Assistance for Law Enforcement Act (CALEA) forbids communications service providers, such as Verizon or Sprint, from producing "any information that may disclose the physical location of the subscriber" when the provider is producing call-identifying information pursuant to the Pen/Trap Statute.[57] Thus, CALEA specifically limits information that providers may produce to law enforcement pursuant to the Pen/Trap Statute.[58]

The SCA authorizes government access to stored communications in the hands of third-party providers.[59] The SCA categorizes different types of stored communications (i.e., information) and outlines what the government must do to obtain access to those different types of communications.[60] The protection afforded by the SCA to these different types of information is based upon the type of stored information sought. Addressing or dialing information—which by system design is in the hands of the third-party provider for routing purposes—is afforded the least protection, whereas "content" information—which refers to the actual substance of the communication, whether email or voice call—is afforded the greatest protection from surveillance.[61]

While this complex federal legislative scheme regulates both private and government actors, it regulates these actors in different ways.[62] The scheme does not limit what personal information and geolocation data the private actor or provider may collect, but it limits what information the private actor may give the government in the absence of court order.[63] The scheme directly limits how and what information the government may gather without court order.[64] The 2013 NSA surveillance revelations do, however, raise a serious question as to whether the post-9/11 federal government and FISC

54. *See* 18 U.S.C. § 3117 (2006); Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002 (2006).

55. 18 U.S.C. §§ 3121-3127 (2006).

56. 18 U.S.C. § 2703 (2006).

57. 47 U.S.C. § 1002(a)(2)(B) (2006).

58. *Id.*

59. 18 U.S.C. §§ 2701-2712 (2012).

60. *Id.*

61. *See id*.

62. *See id.*

63. *Id.* § 2701-2703.

64. *Id.*

consider themselves to be constrained by Title III.

### *C. Recent Supreme Court Privacy Decisions*

Recent Supreme Court privacy decisions demonstrate the judiciary's understandable difficulty in navigating decisions involving modern technologies.[65] Some judges and several Supreme Court Justices appear unaware of how modern Internet and cellular communications function.[66] The result has been disjointed and narrow opinions providing little guidance for the government and private industry in how to lawfully implement certain technologies.[67] We are left with outdated jurisprudence that is counterintuitive and ill-suited for the world we live in. But this is not the fault of the judiciary nor does it reflect a lack of insight and intelligence on the part of those grappling with these issues. Rather, via strongly worded opinions, many in the judiciary have repeatedly called for Congress to pass legislation that will protect individual privacy in the face of evolving, increasingly intrusive electronic surveillance technologies.[68] Consider recent cases highlighting this disconnect between the law and technology.

#### 1. *City of Ontario v. Quon*

The Court's struggle with understanding the capabilities of advancing technologies was uncomfortably on display during oral arguments in *City of Ontario v. Quon*.[69] In *Quon*, the Court considered whether Special Weapons and Tactics Team (SWAT) members have an expectation of privacy in personal text messages sent on pagers issued by the city that employs them.[70] The Justices' struggle with the pager technology involved in the case was awkward. Chief Justice Roberts asked what would happen if a text message was sent to an officer at the same time he was sending a

65. *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (stressing the importance of exercising caution before establishing precedent which would "define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices").

66. *See, e.g.*, Transcript of Oral Argument at 44, *Quon*, 130 S. Ct. 2619 (2010) (No. 08-1332), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1332.pdf.

67. *See Quon*, 130 S. Ct. at 2630, 2632 (adopting a narrow holding that a police department's search of an employee's text messages sent from a cell phone owned and issued by the employer was not unreasonable because it was conducted for a "legitimate work-related purpose"); *see also* United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that the government violated a criminal suspect's Fourth Amendment rights when it "physically" intruded the suspect's private property).

68. *See, e.g.*, *Jones*, 132 S. Ct. at 964 ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

69. *See* Transcript of Oral Argument, *supra* note 66.

70. *See Quon*, 130 S. Ct. at 2624.

text to someone else,[71] at which point Justice Kennedy asked whether the officer in that situation would receive "a voice mail saying that your call is very important to us; we'll get back to you."[72] Later, Justices Roberts and Scalia grappled with the concept of a service provider when they revealed they did not know that text messages are sent to a service provider before reaching the intended receiver.[73] Such questions are particularly concerning because they demonstrate that the Justices lack an understanding that, by design, today's technology discloses all of one's personal information to third parties.[74] Accordingly, under the third-party doctrine established in *Smith v. Maryland* in 1979,[75] the vast majority of our electronic information is unprotected.

### 2. *United States v. Jones*

In 2012, the Supreme Court took on law enforcement's warrantless use of GPS tracking devices.[76] In *United States v. Jones*, the nine Justices *unanimously* ruled that law enforcement's warrantless attachment of a GPS device to a car and subsequent warrantless use of that GPS device to track the location of a suspect for a period of twenty-eight days constituted an unlawful search in violation of the Fourth Amendment.[77] The majority opinion based its holding on the act of trespass that occurred when police physically attached the GPS device to the suspect's vehicle.[78]

---

71. Transcript of Oral Argument, *supra* note 66 ("What happens, just out of curiosity, if you're -- he is on the pager and sending a message and they're trying to reach him for, you know, a SWAT team crisis? Does he -- does the one kind of trump the other, or do they get a busy signal?").

72. *Id.*

73. *See id.* at 48-49.

> MR. DAMMEIER: Well, they -- they expect that some company, I'm sure, is going to have to be processing the delivery of this message. And --
>
> CHIEF JUSTICE ROBERTS: Well, I didn't -- I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing. (Laughter).
>
> MR. DAMMEIER: Well --
>
> JUSTICE SCALIA: You mean it doesn't go right to the other thing? (Laughter).

*Id.*

74. *See id.*

75. *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (stating that a person does not have a reasonable expectation of privacy when that person voluntarily conveys information by using the telephone and the phone company's service).

76. United States v. Jones, 132 S. Ct. 945, 948 (2012).

77. *See id.* at 948-49.

78. *See id.* at 952. There were three opinions issued with the ruling: Justice Scalia authored the majority opinion, which was joined by Justices Roberts, Kennedy, Thomas, and Sotomayor; Justice Sotomayor filed her own concurring opinion; and Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, filed a concurring

The *Jones* decision is remarkable in many respects, but for purposes of our discussion, there are three notable aspects of the decision. First, given earlier beeper and GPS-based location tracking decisions,[79] it is striking that all nine Justices unanimously agreed that the warrantless installation of a GPS tracking device on a suspect's car and subsequent tracking for twenty-eight days constituted an impermissible search.[80] Second, although the Justices were unanimous in their conclusion, the differences in the Justices' rationales were stunning.[81] And third, the Justices' candidly open struggle with certain issues reflects the growing quagmire at the intersection of advancing technologies, privacy, and reasonable expectations of privacy.[82]

In *Jones*, the majority held that the use of a GPS device to conduct prolonged surveillance was unconstitutional only because of the physical act of trespass on Jones's property when the police attached a GPS device to Jones's car.[83] As Justice Sotomayor notes in her concurring opinion, a search occurs "at a minimum" where the government "physically intrud[es] on a constitutionally protected area."[84] Her concurrence and Justice Alito's concurrence acknowledge very problematic limitations of the Court's decisions: Advanced capabilities of new technologies enable the collection of vast amounts of data without a physical trespass.[85]

---

opinion as well.

79. For example, in *United States v. Knotts,* the Court held that the use of a beeper to track Knotts's location was constitutional since a person does not have a reasonable expectation of privacy on public thoroughfares because one's movements are exposed to the public. 460 U.S. 276, 281-82 (1983). Additionally, police use of the beeper to supplement their visual surveillance did not result in a Fourth Amendment violation. *Id.* at 282. Rather, the Court stated: "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." *Id.*

80. *See Jones*, 132 S. Ct. at 948-49.

81. *Compare Jones*, 132 S. Ct. at 949 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."), *with id.* at 955 (Sotomayor, J., concurring) ("In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."), *and id.* at 958 (Alito, J., concurring) ("I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.").

82. *See Jones*, 132 S. Ct. at 962 (illustrating the Court's struggle regarding technology and privacy).

83. *See id.* at 949.

84. *Id.* at 954 (Sotomayor, J., concurring).

85. *Id*. at 959 (Alito, J., concurring) ("'[T]he search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which

3. *Florida v. Jardines*

In *Florida v. Jardines*, police took a drug-sniffing dog to the front porch of Jardines's home where police suspected Jardines was growing marijuana.[86] The dog tracked a scent he had been trained to detect and eventually sat, indicating that he had discovered the odor's strongest point.[87] The Court considered whether using a drug-sniffing dog on Jardines's porch to investigate the contents of his home constituted a search.[88]

In a five to four decision, Justice Scalia and the majority held that the use of the dog on the front porch constituted a search within the meaning of the Fourth Amendment because the police "learned what they learned only by physically intruding on Jardines' property."[89] The majority did not consider the *Katz* analysis or the use of a drug-sniffing dog as technology.[90]

Justice Kagan joined the majority, but adds in her concurrence that she would have found the same outcome using the *Katz* analysis and precedent in *Kyllo v. United States*,[91] which held that where the government uses technology "not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search.'"[92] Justice Kagan would have found that the police used technology not in general public use (i.e., the drug-sniffing dog) to explore details of the home.[93]

The dissenting Justices in *Jardines*, including the Chief Justice and Justice Kennedy, found there was no physical trespass.[94] Notably, the dissent did not consider the dog to be technology; rather, the dissenters said there was nothing that constituted trespass by bringing the dog to Jardines's front porch because "dogs have been domesticated for about 12,000 years."[95]

---

were detested by our forebears and which inspired the Fourth Amendment.'" (quoting Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting))).

86. 133 S. Ct. 1409, 1413 (2013).

87. *Id.* The Court noted that "[t]he dog was trained to detect the scent of marijuana, cocaine, heroin, and several other drugs, indicating the presence of any of these substances through particular behavioral changes recognizable by his handler." *Id.*

88. *Id.*

89. *Id.* at 1417.

90. *Id.*

91. 533 U.S. 27 (2001).

92. *Jardines*, 133 S. Ct. at 1419 (Kagan, J., concurring) (quoting *Kyllo*, 533 U.S. at 40). *Kyllo* involved the warrantless use of a thermal imaging device on one's home, which the Court found to be unconstitutional. 533 U.S. at 40.

93. *Jardines*, 133 S. Ct. at 1419.

94. *Id.* at 1426 (Alito, J., dissenting).

95. *Id.* at 1420.

*Jardines*, like the *Jones* decision before it, provides little guidance to the electronic surveillance quagmire because it uses a property-based approach, and thus, arguably does not apply to technology capable of determining information without physical intrusion upon property.[96] Additionally, Justice Kagan's concurrence and reliance on *Kyllo*, in which the Court relied upon the consideration of whether the thermal imaging technology at issue was readily available to the public, demonstrates another weakness in the Court's privacy jurisprudence: Today, technology in general public use evolves so rapidly that previously expensive, highly invasive electronic surveillance technologies quickly become cheap, readily available, and mainstream.[97]

Determining a technology's availability to the public cannot form the basis of whether a form of surveillance technology is constitutionally permissible, because it does not take into account the astounding pace of technological developments and the corresponding affordability of highly sophisticated electronic surveillance devices. It creates an unsustainable and uncertain legal rule, if followed. Why? Because, in one year, use of a newer technology not in general public use would be constitutionally impermissible, yet advancements making the technology readily available to and affordable for the public one year later would render use of that same technology permissible simply because it had become widely available to the public.

Drones are a perfect example. Five years ago, drones were not generally available for private commercial purchase on the Internet. Today, run a Google search using "drones for sale" as your search term, and you will learn that any twelve-year-old with an Internet connection and some babysitting money can find a drone readily available for inexpensive purchase online.[98]

These discrepancies demonstrate that the property-based approach and other judicial precepts used to determine whether use of surveillance technology is constitutional (such as the third-party doctrine or the readily-available-to-the-public consideration) are not capable of creating clear precedent for courts. These approaches have been acknowledged to be inadequate by the very judges struggling to address and limit the capabilities of rapidly evolving modern surveillance technologies that permit highly invasive, intrusive, and surreptitious electronic surveillance.[99]

---

96. *See id.* at 1417; United States v. Jones, 132 S. Ct. 945, 953-54 (2012).

97. Colleen Kane, *Want to Spy on Somebody? It's Easier Than Ever*, CNBC.COM (Mar. 22, 2013, 4:17 PM), http://www.cnbc.com/id/100583418.

98. *See* Sara Qamar, *If You Want Your Own Drone, They're Available—and Legal*, MSNBC.COM (Aug. 21, 2013, 12:10 AM), http://www.msnbc.com/the-cycle/if-you-want-your-own-drone-theyre-available.

99. *See, e.g.*, *Jardines*, 133 S. Ct. at 1418 (Kagan, J., concurring); *Jones*, 132 S. Ct.

4. *Maryland v. King*

In June 2013, in another five to four decision, the Supreme Court ruled in *Maryland v. King* that taking and analyzing a cheek swab of an arrestee's DNA following an arrest based upon probable cause was reasonable under the Fourth Amendment.[100] The Court weighed the government interest in collecting the DNA against the privacy intrusion.[101] Justice Kennedy, writing for the majority, found there was a legitimate government interest in law enforcement's need "to process and identify the persons and possessions . . . take[n] into custody" and to be able to do so "in a safe and accurate way."[102] The majority categorized the taking of DNA as a routine booking procedure, similar to fingerprinting.[103]

The majority fails, however, to appreciate the distinction between an *intrusive procedure* and *intrusive information collected*. The majority described the collection of DNA by buccal swab as requiring no "'surgical intrusio[n] beneath the skin'" and one that "poses no threat to the arrestee's 'health or safety.'"[104] Such a distinction will apply to many existing and emerging technologies, including—importantly—almost all other biometric identification technology.[105] Merely because a method of collection has improved or become less intrusive does not necessarily negate or diminish the intrusively private nature of the data collected. Fingerprinting, for instance, provides a markedly sure and non-intrusive method of identifying an individual. But it does not also provide the government with intimate details about a detainee's familial blood relations, who the detainee's parents and siblings are, what a detainee's genetic makeup is, what a detainee's ancestry and country of origin is, and whether a detainee is more likely to have cancer than another individual due to their genetic makeup.[106] DNA collection can permit all of this to be accomplished using existing technologies.[107]

---

at 962; Kyllo v. United States, 533 U.S. 27, 34 (2001).

100. 133 S. Ct. 1958, 1980 (2013).

101. *Id.* at 1976-78.

102. *Id.* at 1970.

103. *Id.* at 1976.

104. *Id.* at 1963 (quoting Winston v. Lee, 470 U.S. 753, 760 (1985)).

105. *See infra* Part III.C.

106. *See generally* Stephanie Watson, *How Fingerprinting Works*, HOWSTUFFWORKS, http://science.howstuffworks.com/fingerprinting.htm (last visited Nov. 21, 2013) (explaining the process of fingerprinting and how it is used in the justice system).

107. *See* William Harris, *What Can Your Spit Tell You About Your DNA?*, HOWSTUFFWORKS, http://science.howstuffworks.com/life/genetic/spit-dna.htm (last visited Nov. 27, 2013); Shanna Freeman, *How DNA Profiling Works*, HOWSTUFFWORKS, http://science.howstuffworks.com/dna-profiling.htm (last visited

The dissent, written by Justice Scalia, firmly and correctly condemns the majority opinion.[108] He acknowledges that solving crime is a noble objective, but emphasizes the troubling scope of the majority's holding:

> Today's judgment will, to be sure, have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane (surely the Transportation Security Administration needs to know the "identity" of the flying public), applies for a driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.[109]

*King* is yet another recent case wherein the Court struggles with rapidly involving electronic surveillance and tracking technologies and with defining protections that should be afforded individual privacy in the face of a legislative void. The Justices could not be clamoring more openly for legislative guidance.

## III. SURVEILLANCE TECHNOLOGIES

Having set forth the existing constitutional, statutory, common law, and judicial framework in place to protect individual privacy, we will briefly overview the existing and emerging electronic surveillance technologies currently in use by government and private industry. These technologies permit the surreptitious collection, storage, and sale of personal, intimate data on a scale that is difficult to appreciate and comprehend because of the vastness and pervasiveness of data collection in almost every activity of daily living.

### *A. GPS Tracking*[110]

GPS stands for Global Positioning System. GPS devices are commercially available and readily affordable.[111] Typically, when one

---

Nov. 3, 2013).

108. *See King*, 133 S. Ct. at 1980-91 (Scalia, J., dissenting).

109. *Id.* at 1989. The Panopticon to which Justice Scalia refers was first conceived by Jeremy Bentham. *See* Ronald Collins, "*Panopticon*"? – *Keep your eyes on the word!*, SCOTUSBLOG (June 5, 2013, 11:26 AM), http://www.scotusblog.com/2013/06/panopticon-keep-your-eyes-on-the-word/. The idea is a prison designed with a central guard tower that may view all inmates housed there. *Id.* At the same time, the prisoners have no view of who is watching them. Eventually, the inmates modify their behavior to be in line with those who watch them. *Id.*

110. Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters ed., 4th ed. 2012).

111. GPS devices are available for less than $100. Marshall Brain & Tom Harris,

refers to a "GPS" he or she is actually contemplating a GPS receiver.[112] The Global Positioning System is actually a constellation of twenty-seven Earth-orbiting satellites.[113]

In simplistic terms, the GPS receiver, which is the actual electronic tracking device attached or used, locates no less than four of these orbiting satellites and computes the distance between itself and each satellite by analyzing high-frequency, low-power radio signals from the GPS satellites.[114] Employing a mathematical principle known as trilateration, the GPS receiver uses these combined calculations to determine its own location.[115]

GPS reveals far more than a traditional electronic tracking device; a standard GPS receiver provides not only a particular location, but it also can, in real time, trace the person or thing's path, movement, and speed of movement.[116] GPS devices also maintain historical data recording the person or object's movements.[117] If a GPS receiver is left in "on" mode, it stays "in constant communication with GPS satellites."[118]

Thus, GPS can serve both passive tracking purposes (to locate a person or an object) as well as real-time tracking purposes (to track the movement of a person or object as it is actually occurring).[119] This distinction is referred to as passive monitoring, which describes location-only purposes monitoring, and active monitoring, which is described as realtime monitoring.[120]

The capabilities of a GPS device provide an almost endless list of potential uses. In the last decade, the use of GPS devices has proliferated to an extent difficult to sum up in words.[121] As discussed, personal hand-held GPS devices are commercially available in most electronic stores for far less than $100.[122] Most vehicles sold today

---

*How GPS Receivers Work*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gps.htm (last visited Nov. 21, 2013). For that amount of money, a consumer can purchase a pocket-sized or smaller gadget that discerns one's exact location on Earth at any moment.

112. *Id.*

113. Twenty-four of these satellites are in constant operation and three extra satellites are maintained in space in the event of failure with one of the other twenty-four satellites. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. See generally Fredericks v. Koehn, No. 06-cv-00957-MSK-KLM 2007 WL 2890466 (D. Colo. 2007), for a discussion of active and passive monitoring.

120. *Id.*

121. *See* M. Yanaklak & O. Baykal, *Transformation of Ellipsoid Heights to Local Leveling Heights*, 127 J. SURV. ENG. 90, 90 (2001).

122. Brain & Harris, *supra* note 111.

are GPS equipped. And, GPS devices are commonly used by government and private employers to keep track of the whereabouts of their employees and equipment.[123] GPS ankle devices are also used to track prisoners, both passively and actively.[124]

For government purposes, the use of GPS devices and GPS evidence is generally governed by the same statutes and case law progeny as that which governs traditional electronic tracking devices.[125] However, federal tracking laws typically do not apply to private industry's use of GPS tracking technology.[126]

### *B. Cell Phones as Tracking Devices*[127]

Cell phone technology permits cell service providers to easily use the signals emitted by a cell phone to track real time cell site location.

> A cellular phone is no longer just a means of mobile communication. More often than not, a cellular phone is capable of functioning as a mobile telephone, a camera, a video recorder, a text messaging device, a computer with Internet and e-mail capabilities, a television, and an MP-3 player.[128] These advances are occurring so rapidly that they blur distinctions made by legislatures and courts as to what is required to investigate, track, and/or search and seize a cellular telephone [as opposed to a computer].[129]

For tracking purposes, modern cell phones and smart phones come standard-equipped with GPS-based tracking or geolocation technology. Cell phones are still sometimes used to track an individual's location using triangulation, a process explained briefly below.[130] A cell phone operates like a two-way radio; it has a low-power transmitter that operates in a network of cell sites.[131] The

---

123. *See, e.g.*, Hinkley v. Roadway Exp., Inc., 249 Fed. Appx. 13 (10th Cir. 2007).

124. United States v. Freeman, 479 F.3d 743, 745 (10th Cir. 2007); *Koehn*, 2007 WL 2890466, at *2.

125. Ryan Gallagher, *The Spy Who GPS-Tagged Me*, SLATE.COM (Nov. 9, 2012, 8:33 AM), www.slate.com/articles/technology/technology/2012/11/gps_trackers_to_monitor_cheating_spouses_a_legal_gray_area_for_private_investigators.html.

126. *Id.*

127. Portions of this discussion have been excerpted from FISHMAN & MCKENNA, *supra* note 110.

128. "Blackberries and i-Phones are two examples of the newer, multipurpose model of a cellular phone." *Id.* at VI § 28:2 n.1.

129. *Id.* at VI § 28:2.

130. *Id.* at VI § 29:37.

131. *In re* Application for Pen Register, 396 F. Supp. 2d 747, 750–51 (S.D. Tex. 2005). For a general background on cell phones, see S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3563; Tom Farley, Cellular Telephone Basics, PRIVATELINE: TELECOMMUNICATIONSO EXPERTISE (Jan. 1, 2006, 8:55 PM)

word "cell" refers to geographic regions.[132] A "cell site" is where the radio transceiver and base station controller are located (at the point where three hexagons meet).[133] Thus, a cell site lies at the edge of several cells, not at the center of a cell.[134]

The cell site or tower constantly sends and receives traffic from the cell phones in its geographic area to what is called a Mobile Telecommunications Switching Office (MTSO), which handles all phone connections and controls all the base stations (or towers) in a given region.[135]

Cellular service providers' computers automatically keep track of the identity of all the cell towers serving a phone at any given time and the aspect of each tower facing the phone.[136] By triangulating the cell signals and towers, a cell phone's location can be precisely pinpointed.[137] Triangulation permits both real-time and historical tracking of cell phones.[138]

In conclusion, whether using GPS technology or triangulation, the cell phones we carry with us everywhere provide private industry with an always "on" form of tracking our location.[139] Moreover, the software with which our phones come preloaded and the mobile apps we download onto our phones more often than not surreptitiously record our GPS information and send that information back to the app supplier.[140]

### *C. Biometrics*[141]

"Biometrics" is a general term that is used interchangeably to describe a characteristic or a process.[142] As a *characteristic*,

---

http://www.privateline.com/mt_cellbasics/index.html.

132. Farley, *supra* note 131.

133. *Id.*

134. *Id.*

135. *Id.*

136. For an illustrative demonstration, see *Cellular 9-1-1 Triangulation Method*, ALABAMA NATIONAL EMERGENCY NUMBER ASSOCIATION, http://www.al911.org/wireless/triangulation (last visited Sept. 6, 2013).

137. *Id*.

138. *Cell Phone Tower Triangulation*, INTERNATIONAL INVESTIGATORS, INC., http://www.iiiweb.net/forensic-services/cell-phone-tower-triangulation/ (last visited Nov. 21, 2013).

139. *See supra* notes 116-18 and accompanying text.

140. *See, e.g.*, Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 BERK. TECH. L.J. 55, 91 (2012).

141. Portions of this discussion have been excerpted from FISHMAN & MCKENNA, *supra* note 110.

142. For a definition of "biometrics," developed by the National Science & Technology Council's (NTSC) 2006 Subcommittee on Biometrics, see Biometrics Glossary, BIOMETRICS.GOV, http://www.biometrics.gov/documents/glossary.pdf (last visited Nov. 21, 2013).

biometrics is defined as "[a] measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition."[143] As a *process*, biometrics is defined as "[a]utomated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics."[144]

"In 1907, the Department of Justice (DOJ) established a Bureau of Criminal Identification," which was "based upon fingerprints."[145] In 1924, the DOJ tasked the precursor of the Federal Bureau of Investigation (FBI) with creating a national identification and criminal history system.[146] This led to today's Criminal Justice Information Services (CJIS) of the FBI.[147] By the 1960s, the United States had created automated technology for the storage and comparison of prints.[148] Digitization in the 1980s and early 1990s further increased the ease and efficiency of fingerprints as a biometric identifier, and by the end of the twentieth century, fingerprint identification had become the norm for governments around the world. [149]

In the 1990s, private industry and the United States government earnestly invested in developing new biometric identification technologies.[150] The early 1990s saw the beginnings of face recognition software development, and in 1993, "the [Department of Defense] initiated [its] Face Recognition Technology . . . program.[151] In 1994, "[t]he first patent granted for automated iris recognition . . . was issued."[152] In 1996, the United States Army implemented "real-time video face identification."[153]

In 2000, the Defense Advanced Research Projects Agency (DARPA) "initiated the Human Identification at a Distance

143. *Id.*

144. *Id.*

145. SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., NAT'L SCI. & TECH. COUNCIL, THE NATIONAL BIOMETRICS CHALLENGE 5 (2011), *available at* http://www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf.

146. Kenneth R. Moses et al., *Automated Fingerprint Identification System (AFIS)*, *in* NAT'L INST. OF JUSTICE, THE FINGERPRINT SOURCEBOOK 6-1, 6-4 (Alan McRoberts & Debbie McRoberts eds., 2011), *available at* https://ncjrs.gov/pdffiles1/nij/225320.pdf.

147. SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., NAT'L SCI. & TECH. COUNCIL, *supra* note 145.

148. Moses et al., *supra* note 146.

149. Nat'l Sci. and Tech. Council Subcomm. on Biometrics and Identity Mgmt, *Biometrics Glossary,* BIOMETRICS.GOV, http://www.biometrics.gov/Documents/BioHistory.pdf (last visited Nov. 26, 2013).

150. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 419 (2012).

151. *Id.* at 423.

152. *Id.* at 419 n.39.

153. *Id.* at 423.

Program."[154] "The goal [of this program] was to develop algorithms for locating and acquiring subjects up to 150 meters . . . away, [by combining] face and gait recognition [technologies] . . . ."[155] The stated "purpose of [this] program was to provide early warning . . . for force protection . . . against terrorism and crime."[156]

The events of 9/11 ushered in dramatic changes in the use of biometrics and in funding for advancements in biometric technology.[157] 9/11 also provided the impetus for homeland security-related legislation that, with little constitutional consideration, funded the development and implementation of biometric identification systems and authorized the collection (by both overt and covert means), retention, and sharing[158] of individual biometric data.[159] In describing the impact of 9/11 on government-conducted electronic surveillance, one commentator noted:

> In this process, there is a widening of surveillance, with a wide range of personal data being collected for the purposes of securitized immigration control and a wide range of government agencies (and not only immigration agencies) having access to such data, as well as a deepening of surveillance (via the collection of extremely sensitive categories of personal data, including biometrics) . . .Great emphasis [is] placed on the widening and deepening of information collection and sharing (including . . . biometrics) from a variety of sources.[160]

The astonishingly rapid developments in biometric identification systems have revolutionized government, military, and private industry's security systems and means of identification of persons.[161] The use of biometrics and emerging biometric technologies continues to alter and change the way persons are and can be identified and, in turn, the way persons can be tracked and subjected to surveillance.[162]

---

154. *Id.* at 423-24.

155. *Id.* at 424.

156. *Id.* This program is one of the first examples of transition to biometric identification via remote technology. *See* NAT'L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS 18 (Heather Rosenker & Megan Hirshey eds., 2008), *available at* http://www.biometrics.gov/Documents/Biometrics%20in%20Government%20Post%209-11.pdf.

157. Donohue, *supra* 150, at 425.

158. *See id.* at 427-28. As a result of post-9/11 legislative changes, this sharing of data amongst government agencies occurs both horizontally (between federal agencies) and vertically (between federal and state and local governments). *See id.* at 416, 410, 459-61.

159. *See* Valsamis Mitsilegas, *Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, 19 IND. J. GLOBAL LEGAL STUD. 3, 12 (2012).

160. *Id.* at 12-13.

161. *See* Donohue, *supra* note 150, at 410.

162. *See id.* For instance, in Israel, a security technology firm partnered with an

For instance, the technological advances in the biometric identification system known as face or facial recognition and the corresponding relatively recent ability of government and private industry to surreptitiously collect, retain, and access hundreds of millions of individuals' facial biometric data have coalesced to permit the almost immediate identification of individual "faces in a crowd and three-dimensional face recognition."[163] Government and private industry have developed a variety of handheld mobile devices that permit collection and wireless verification of identity via fingerprint biometrics, face biometrics, and iris scanning.[164]

Thus, low cost "biometric handheld devices now make it possible to obtain rapid identification virtually anywhere."[165] Most people seem unaware of how private industry uses biometrics to identify and track individuals' locations, preferences, and associates.[166]

## IV. USE OF SURVEILLANCE TECHNOLOGY BY PRIVATE INDUSTRY

### *A. Cellular Telephones and GPS Tracking*[167]

It is common knowledge that mobile software applications collect more personal data from our smart phones than they need or should. One such example is Apple's much-touted Siri: There was a media uproar when it became known that Siri was surreptitiously collecting our geolocation data, search requests, address books, recording the sound of our voices (and using voice recognition biometric technology to "remember" us), and sending the information back to Apple.[168]

---

Israeli company, i-Mature, to create Age-Group Recognition (AGR) software that requires a computer user to submit to a scan of a finger bone to determine age prior to accessing certain websites. *See* Press Release, EMC Corporation, RSA Security and i-Mature Partner on Next-Generation Biometric Technology to Further Protect Children on the Internet (Feb. 7, 2005), *available at* http://latinamerica.rsa.com/press_release.aspx?id=5497.

163. SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., NAT'L SCI. & TECH. COUNCIL, *supra* note 145, at 12.

164. *Id.* at 13.

165. *Id.* at 19.

166. *See* Lisa Vaas, *Apple's Siri Voiceprints Raise Privacy Concerns*, NAKED SECURITY, SOPHOS (June 28, 2012), http://nakedsecurity.sophos.com/2012/06/28/apples-siri-voiceprints-raise-privacy-concerns/ (asserting that IBM employees unaware of security risks from use of mobile device apps).

167. *See* Anne T. McKenna, *FTC's December 10, 2012 Report: Mobile Apps for Kids: Disclosures Still Not Making the Grade*, INTERNET, SOCIAL MEDIA AND PRIVACY LAW BLOG, SILVERMCKENNA, (Jan. 18, 2013), http://www.internetprivacylawblog.com/2013/01/ftcs_december_10_2012_report_m.html; *see also* PRWeb, *FTC Releases New, Troubling Report On What's Being Done With Children's Private Information says Anne McKenna From Baltimore Law Firm Silverman, Thompson, Slutkin & White*, (Dec. 13 2013), http://www.prweb.com/releases/2012/12/prweb10236296.htm.

168. Vaas, *supra* note 166.

Privacy policies provide no assurances: Most mobile apps' privacy policies shroud the app's data collection practices in a byzantine collection of legal terms, and most individuals do not read the policies.[169] Smart phones, from which we check our email, surf the web, access Facebook, make calls, and do work, are loaded with numerous software programs that use the phone's built-in GPS or geolocation technology ostensibly to better serve our needs ("Where is the closest Starbucks? What is my current location? Where are my friends? Where was that photo taken?"). However, our geolocation data is also extremely valuable to private industry.[170] Software that collects such data enables the software app developer or owner to sell our geolocation and other collected data to third parties for purposes of marketing and targeted advertising.[171]

In December 2012, the Federal Trade Commission (FTC) issued a report that illustrates the potentially insidious and highly invasive nature of such surreptitious data collection by private industry.[172] The FTC's detailed report revealed that the most popular children's mobile software apps are surreptitiously collecting and then selling to hundreds of marketers and third parties information regarding where our children physically are at all times, what their mobile phone numbers are, and where they go and what they do online, and are doing so without notice to parent or child.[173] Replete with research and data, the report demonstrates that the most popular mobile software apps designed for, marketed to, and used by our children are doing all of this, and in so doing, may be running afoul of numerous federal consumer protection, deceptive advertising, and privacy laws.[174]

The December 2012 report is a follow-up to a February 2012 report wherein the FTC surmised that there may be significant privacy issues with mobile apps designed for and targeted to children.[175] After releasing the February 2012 report, the FTC did its homework: It investigated 400 popular children's mobile software apps, reviewed the apps' stated privacy policies, and tested the apps' actual data collection and tracking practices.[176] What it found is

169. FED. TRADE COMM'N, *Mobile Apps for Kids: Disclosures Still Not Making the Grade* 8 (2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

170. *See* FED. TRADE COMM'N, *Mobile Apps for Kids: Current Privacy Disclosures Are Dis*appo*inting* 1 (2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

171. *See* FED. TRADE COMM'N, *supra* note 169, at 3.

172. FED. TRADE COMM'N, *supra* note 169.

173. *Id.* at 8.

174. *Id.* at 5.

175. *Id.* at 1.

176. *Id.* at 5.

troubling.[177]

First, the FTC noted that only twenty percent of the 400 children's mobile software apps it investigated—most of which are available, and supposedly vetted, through Apple and Google's respective mobile app stores—even provided disclosures about their data collection practices.[178] Those twenty percent that did so employed links to long, verbose, technically-detailed privacy policies beyond the average adult user's ken, much less that of a child.[179]

Overwhelmingly, the vast majority of the investigated children's apps, even those with stated privacy policies, failed to provide any information about the general data collected, the type of data collected, the purpose of the data collection, and who would and could obtain access to the data.[180] Worse still, most apps routinely and actively shared the phone number of the child's device, the precise location of the child's device (and thus, the child), and the unique identification code of the device with numerous third parties. [181] Notably, while one app's privacy policy claimed that it did not transmit any information to third parties, a quick look by the FTC revealed that it in fact transmitted the three pieces of information listed above.[182]

The immediate and invasive nature of private data collected and transmitted to third parties is both astonishing and frightening. For instance, the FTC noted that "[o]ne app . . . transmitted [the child's] geolocation information to two separate ad networks within the first second of the app's use."[183] Being a diligent parent or guardian does not stop data gathering.[184] Why? Because the FTC found that many of the apps it reviewed failed to advise parents when the app contained interactive features like advertising, social network sharing, and allowing children to purchase virtual goods within the app.[185] The FTC found the apps that linked, without disclosure, to social media sites to be particularly troubling, noting that children could "communicate with other users who they have never met or . . . post information about themselves or their whereabouts."[186]

Mobile apps that allow children to upload photos or that record children's voices without advising parents of social media linkage

177. *Id.*
178. *Id.* at 6.
179. *Id.* at 8 n.23.
180. *Id.* at 4.
181. *Id.*
182. *Id.* at 8.
183. *Id.* at 13 n.27.
184. *See id.* at 7.
185. *Id.* at 4.
186. *Id.* at 20.

enable another potentially insidious privacy violation.[187] Social media sites that use or have used face or voice recognition software to surreptitiously scan and record users' facial biometrics or voice biometrics for future identification and marketing purposes are potentially storing this information.[188] This means that marketers might be able to track children's whereabouts via their facial biometrics in public places, like malls, even when a child does not have a mobile device on his or her person.[189]

The FTC found that over fifty percent of the 400 popular children's mobile apps it investigated were transmitting children's data to various third parties, often marketers.[190] While a mere nine percent of the children's apps reviewed willingly admitted to parents that the apps contained advertising targeted to children prior to download, the FTC found that fifty-eight percent of the apps reviewed were actually advertising to the child users.[191]

According to news sources, prominent media companies want the FTC to reduce its restrictions for children and online privacy protection because of the vast marketing income the child market presents,[192] whereas child and privacy advocates argue that this detailed collection of data, including the child's photo, voice recordings and unique device identification codes, will enable marketers and advertisers to track children wherever they go, both online and off.[193] Right now, according to the FTC, the law may be on the side of the privacy advocates. The FTC is investigating whether a majority of these popular children's apps could be violating numerous laws, including the FTC's prohibition against unfair or deceptive marketing practices, federal consumer protection statutes, and the Children's Online Privacy Protection Act (COPPA).[194]

---

187. *See, e.g.*, Carmen Aguado, *Facebook or Face Bank?*, 32 LOY. L.A. ENT. L. REV. 187, 192-93 (2012).

188. *Id.*

189. *Id.* For further discussion of the use of biometrics, see *infra* Part IV.B.

190. *See* FED. TRADE COMM'N, *supra* note 169, at 6.

191. *Id.* at 6, 16.

192. *Cf.* Julia Cohn, *How 'Do Not Track' May Hurt Businesses*, ENTREPRENEUR (Oct. 8, 2012), http://www.entrepreneur.com/article/224611 (positing that companies are paid more for placing targeted, behavioral ads on their websites than they are for placing non-targeted, contextual ads); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS: FTC REPORT 7 (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf ("[M]any commenters raised concerns about how wider privacy protections would affect innovation and the ability to offer consumers beneficial new products and services.").

193. *See* Bianca Bosker, *Facebook Buys Facial Recognition Firm Face.com: What It Wants With Your Face,* THE HUFFINGTON POST (June 19, 2012), http://www.huffingtonpost.com/2012/06/19/facebook-buys-face-com_n_1608996.html.

194. FED. TRADE COMM'N, *supra* note 169, at 5.

What are the potential legal consequences? Litigation will be plentiful. Consumer protection statutes are often written with per violation damages;[195] thus, the repeated surreptitious, undisclosed data collection of intimate details of potentially millions of children's daily activities, whereabouts, and contact information may amount to staggering damage figures.[196]

### *B. Biometrics Combined with Internet Tracking: Money for Private Industry*

For private industry, biometric identification has several advantages over traditional methods of identification such as passwords, personal identification numbers (PINs), and ID cards.[197] A person might lose or forget a password or PIN, or an unauthorized person may find or learn it and misuse it; an ID card may be lost or forged.[198] Biometric identification, by contrast, is not susceptible to these problems,[199] because it is based upon intrinsic characteristics of an individual that are extremely difficult to duplicate and are not dependent on human memory.[200]

What exactly does biometrics do for private industry? Without even using biometrics, a retailer can already buy or figure out the following information from an individual's online activity:

> [Y]our age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit. Target can buy data about your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own.[201]

---

195. *See, e.g.*, Justin Dingfelder & Sandra Brickels, *To Protect Consumers, the FTC Means Business*, 45 FED. LAW. 24, 26 (1998).

196. Victor E. Schwartz & Cary Silverman, *Common-Sense Construction of Consumer Protection Acts*, 54 U. KAN. L. REV. 1, 12 n.46 (2012).

197. *See, e.g.*, SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., NAT'L SCI. & TECH. COUNCIL, *supra* note 145, at 22.

198. *See, e.g.*, *id.*

199. Unless, of course, things develop along the lines of the 2002 Spielberg movie, *Minority Report*, in which the character played by Tom Cruise has his eyes surgically removed and replaced with those of another person so he can fool retinal scanners as to his identity. He keeps his own eyes, too, however, so he can pass as himself when it suits him. MINORITY REPORT (Twentieth Century Fox et al. 2002).

200. *See* SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., NAT'L SCI. & TECH. COUNCIL, *supra* note 145, at 29.

201. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG., (Feb.

Linking such information further to biometric data does not just have huge marketing and retailing implications;[202] it has significant privacy implications. Absent any changes in federal legislation, biometric advances have provided marketers and retailers the opportunity to identify exactly who someone is when they walk into any store that operates surveillance cameras.[203] As discussed below, online search engines, like Google, and social media sites, like Facebook, have already begun gathering, storing, and using hundreds of millions of users' facial biometrics.[204] Under current laws and most social media user agreement provisions, an individual does not always own or retain a right to privacy in his or her biometric data.[205]

Why is this being done? Because collected, stored, and accessible biometric data provides vast potential for financial gain for international, national, and local private entities.[206] Government and private industry's significant investments in biometric technologies and the increasingly vast collection of biometric data appear discordant with fundamental American notions of privacy, but Congress has been silent on the issue.[207]

As mentioned, social media sites, the present and future hub of very targeted and often user-unaware advertising,[208] acquire, organize, store, and access biometric data from users with a particular focus on facial biometrics collected via face recognition software.[209] Consider Facebook: In June of 2011, Facebook launched a "tag suggestion" feature—ostensibly for the benefit of its users—that prompts users with tagging suggestions for images of individuals contained in the photos that Facebook users upload.[210] Although Facebook played coy with the facts, it clearly had already been utilizing some form of face recognition biometric software for some time.[211] Otherwise, it could not have launched a ready-to-go

16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=1&pagewanted=all.

202. *See id.*

203. *See, e.g.*, *Check-ins Get a Facelift*, REDPEPPER, http://redpepperland.com/lab/details/check-in-with-your-face (last visited Nov. 24, 2013).

204. *See, e.g.*, Aguado, *supra* note 187.

205. *See* Joseph Loreno Hall, *Facial Recognition & Privacy: An EU-US Perspective*, CTR. FOR DEMOCRACY & TECH. (Oct. 8, 2012), *available at* https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf.

206. *See* Cohn, *supra* note 192.

207. *See* Aguado, *supra* note 187, at 223. *But see* FED. TRADE COMM'N, *supra* note 192, at 4-5.

208. *See* FED. TRADE COMM'N, *supra* note 192, at 40.

209. *See id.* at 45.

210. Aguado, *supra* note 187, at 188.

211. *See id.* at 198.

tagging tool that provided automatic identification of millions of individuals in photographs and videos uploaded to Facebook.[212] Since the 2011 launch, Facebook has acknowledged that it has gathered, collected, stored, and used the biometric data of millions and millions of individuals around the world through the use of facial recognition software.[213]

When one considers Facebook's use statistics, the sheer quantity of biometric data gathered by Facebook is staggering. Facebook presently boasts 1.15 billion users worldwide;[214] it is the second most-visited site on the Internet;[215] approximately 699 million Facebook users log into their accounts daily;[216] and every twenty-four hours Facebook users upload over 300 million photos. [217] What does this means for privacy and the collection of biometric data? Facebook probably has the largest privately held digital collection of facial biometrics of hundreds of millions of people across the globe.[218] Thus, by using face recognition, Facebook and other social media sites employing face biometrics have gathered a tremendously valuable marketing commodity—your facial biometrics.[219]

Social media's use of facial biometrics is not the future, it is now: "[S]ome companies are already using facial recognition technology to identify clothing in images posted online, and Facebook might wield Face.com's technology to tag brands and retailers shown in users' pictures . . . . That could evolve into a tool that automatically tags Coca-Cola cans or Levi's jeans as a way of increasing visibility for Facebook advertisers."[220]

## V. HOW MODERN SURVEILLANCE TECHNOLOGY CONFOUNDS THE EXISTING PRIVACY LAW FRAMEWORK

### *A. Reasonableness of Intrusion and Reasonable Expectation of Privacy: A Problem*

The line of cases discussed above demonstrates how our judiciary is confounded by new technologies. Consider reasonableness: Courts

212. *See id.* at 188-90.

213. *See id.* at 188.

214. *Key Facts*, FACEBOOK, http://newsroom.fb.com/Key-facts (last visited Nov. 26, 2013).

215. *Top Sites*, Alexa, http://www.alexa.com/topsites (last visited Nov. 26, 2013).

216. FACEBOOK, *supra* note 214.

217. Rick Armbrust, *Capturing Growth: Photo Apps and Open Graph*, FACEBOOK (July 17, 2012, 1:00 PM), https://developers.facebook.com/blog/post/2012/07/17/capturing-growth--photo-apps-and-open-graph/.

218. *See* Aguado, *supra* note 187, at 195-96.

219. *Id.* at 214.

220. Bosker, *supra* note 193.

determine the reasonableness of a search by weighing "the promotion of legitimate governmental interests" against "the degree to which [the search] intrudes upon an individual's privacy."[221] But the current standard to gauge the degree of intrusion upon individual privacy is ill-suited to modern technology. For example, in *King*, the police used a buccal swab inside a person's cheek to obtain a DNA sample. While the method of retrieving the information is "quick and painless," the type of information collected is very intrusive, providing the government with access to one's genetic identity, genetic markers, and family genetic history.[222]

Today, methods for collecting information are considerably more surreptitious yet less intrusive than methods used in the past to gather the same data. Consider the *Jones* decision: The GPS tracking device surreptitiously collected far more data than a "tiny constable" would have ever been able to collect in the past.[223] By considering how intrusive the collection device is, courts fail to grasp that newer technologies require far less intrusion while simultaneously collecting far greater amounts of highly personal data, which a reasonable person would find far more intrusive (provided he or she understood the quantity of data being collected; for instance, consider whether an arrestee understands the quantity of information gathered in a DNA collection via a buccal swab).

This trend will continue. For instance, numerous retail stores employ technology that allows retailers to track, and thereby learn more about, their customers' behavior in their stores.[224] There are many variations of the technology, but most track customers' movements by following the Wi-Fi signals from their smart phones.[225] Unless the store informs the customers that they are being tracked in this manner, there is no reason a customer would know they are being monitored. This is a very nonintrusive collection method; yet it collects detailed information such as a customer's gender and age, whether they are a repeat customer, how long they are in the lingerie section, and what hemorrhoid or vaginal cream they quietly pick up or put down.[226] Regardless of the fact that the collection method is nonintrusive, the scope and extent of information collected would be considered by many to violate their reasonable expectation of privacy and, thus, be a privacy intrusion.

---

221. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

222. Maryland v. King, 133 S. Ct. 1958, 1962 (2013).

223. *See* United States v. Jones, 132 S. Ct. 945, 958 n.3 (2012) (Alito, J., concurring).

224. Stephanie Clifford & Quentin Hardy, *Attention, Shoppers: Store is Tracking Your Cell,* N.Y. TIMES (July 15, 2013), http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html.

225. *Id.*

226. *Id.*

A startling example of biometric-based tracking for advertising purposes is "Facedeals." Redpepper, the advertising agency behind Facedeals, has successfully marketed to businesses small cameras equipped with face recognition software that scan the facial biometrics of every single customer who walks into a business. [227] If the particular customer's facial biometrics are identified from an almost instantaneous cross-comparison with Facebook's vast collection of individuals' face biometrics, the identified individual is sent a "Facedeal," via Facebook, for the particular business.[228] This may be a sale on shirts or a drink special. "The cameras are standalone devices developed around open source technologies including Raspberry Pi, Arduino, OpenCV, and the Facebook Graph API [Application-Programming Interface]. They can be configured remotely and require a standard 110 volt wall outlet and a wifi [sic] connection."[229]

The very nature of the Internet and satellite-based structure upon which modern communication and many digital devices function requires that we overhaul or discard the third party doctrine articulated in *Smith v. Maryland*.[230] Because of the platform upon which cell phone and Internet activity is conducted, there is little to no information undisclosed to a third party.[231]

Justices Sotomayor and Alito both raise this issue in their concurring opinions in *Jones*. Justice Sotomayor explicitly questions the third-party doctrine, stating:

---

227. FACEDEALS, http://redpepperland.com/lab/details/check-in-with-your-face (last visited Nov. 26, 2013).

228. *Id.*

229. WAYBACK MACHINE, http://web.archive.org/web/20130516165234/http://redpepperland.com/lab/details/check-in-with-your-face (containing an archived snapshot of the Oct. 6, 2013 version of the Facedeals website) (last visited Nov. 26, 2013).

230. *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that the defendant's disclosure of telephone numbers dialed out to the telephone provider was a third-party disclosure and, thus, not subject to Fourth Amendment protection).

231. Although users can in some instances control their privacy settings or limit who can access their posted content, because most postings to social media sites such as Facebook and Twitter typically are accessible to large numbers of individuals, courts recognize a reduced expectation of privacy in social media activity. Applying the third-party doctrine, courts rule that the users of social media have voluntarily submitted the data to a third party, and thus cannot claim any expectation of privacy in that data, even in instances where such data (e.g., location data) is being collected surreptitiously. *See, e.g.*, In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 130 (E.D. Va. 2011) (holding that the third-party doctrine destroys any reasonable expectation of privacy in the location data because the Twitter users voluntarily provided that data to Twitter); *see also* People v. Harris, 945 N.Y.S.2d 505, 508 (Crim. Ct. 2012) (finding that a Twitter user did not have a proprietary interest in his tweets upon agreeing to Twitter's terms at the time the account was created).

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[232]

The reasonable expectation of privacy test, first articulated in Justice Harlan's concurring opinion in *Katz v. United States*,[233] has been criticized by scholars throughout its existence. And in *Jones*, Justices Sotomayor and Alito both suggest that the reasonable expectation of privacy standard needs to be reevaluated.[234] Justice Alito condemns the *Jones* majority's use of the trespass doctrine to hold that the physical attachment of the GPS device constituted an unlawful trespass; instead, Justice Alito concludes the Court could have reached the same outcome applying *Katz*.[235] But he acknowledges the difficulties presented in applying Katz to more advanced technologies:

> [T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.[236]

Justice Alito then strongly urges Congress to enact legislation as it did with respect to wiretapping following *Katz* and the events of Watergate.[237]

Our jurisprudence is not the only problem: Justice Alito and Justice Sotomayor's concurrences both make clear that the United States lacks a comprehensive approach to privacy policy, because Congress has failed to pass a technologically-adaptive legislative

---

232. United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring) (citation omitted).

233. To determine one's reasonable expectation of privacy, courts must first consider the subjective prong, which requires that the individual "exhibit[] an actual (subjective) expectation of privacy" in the location searched, and then evaluate the objective prong, which determines whether that "expectation [is] one that society is prepared to recognize as reasonable." Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

234. United States v. Jones, 132 S. Ct. 945 (2012) (Sotomayor, J., and Alito, J., concurring).

235. *Id.* at 962.

236. *Id.* at 963.

237. *Id.*

privacy scheme.[238] Not only has Congress not provided legislative guidance, it has failed to amend existing legislation to reflect the realities of modern surveillance capabilities. In *Quon*, *Jones*, *Jardines*, and *King*, the Justices have made it clear: They are not equipped to develop a judicial approach that preserves traditional concepts of privacy in the face of technological development without legislative guidance.

*B. Government Surveillance and Pending Privacy Legislation*

In the summer of 2013, *The Guardian* released a series of articles revealing NSA programs used to spy on Americans. We learned that the NSA, through a secret order issued by the FISA court, is collecting the metadata of millions of Verizon customers on a daily basis.[239] The revelations also brought to light the vast scale of information that the NSA and the FBI also collect through a program, code-named PRISM, which taps directly into central servers of leading U.S. Internet companies.[240] PRISM collects "audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."[241] But it does so by the surreptitious and warrantless collection of the electronic data of American citizens, ostensibly to keep us safe from foreign nationals and terrorists. The frightening flipside of this surveillance is the Obama Administration's notoriously hard stance towards those individuals who whistleblow about the government's surreptitious surveillance programs. [242]

---

238. *Id.* at 964.

239. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.thegaurdian.com/world/2013/jun/06/nsa-phone-recrods-verizon-court-order.

240. Among them are "Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple." Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013) http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

241. *Id.*

242. Another interesting and noteworthy piece to this puzzle is the Obama Administration's manner in dealing with national security leaks. Since 1971, when Daniel Ellsberg revealed documents known as the Pentagon Papers, very few presidents have gone after whistleblowers as aggressively as President Obama. John Dean, *Dealing with National Security Leaks: Obama's "Plumbers*," VERDICT: LEGAL ANALYSIS AND COMMENTARY FROM JUSTIA (June 14, 2013), http://verdict.justia.com/2013/06/14/dealing-with-national-security-leaks-obamas-plumbers-2. Prior to 2008, President Nixon prosecuted Daniel Ellsberg, President Reagan prosecuted Samuel Morrison (who was later pardoned by President Clinton), and President Bush prosecuted Lawrence Franklin. *Id.* Since Obama has taken office, six whistleblowers have been prosecuted (although two of those six investigations began during the Bush Administration). *Id.* Currently, the Obama Administration is investigating Julian Assange of Wikileaks, Stephen Jin Woo Kim, and Edward

Since the NSA surveillance story broke in June 2013, there have been several knee-jerk legislative proposals.[243] Such pending legislation is more of a band-aid than a solution to the pervasive and secret surveillance conducted by the government. With none of the bills gaining real traction,[244] it is unlikely that meaningful legislation will be passed to address the government's circumvention of the Constitution and statutory law. It seems even more unlikely that legislation will be passed to give consumers greater control over private industry's collection, use, and sale of their personal, private data.

Instead, Congress is attempting to pass legislation that would directly subvert current limits on the methods by which the government can obtain privately held information.[245] The Cyber Intelligence Sharing and Protection Act bill (CISPA) was first introduced in 2012 and again in 2013.[246] Proponents hail CISPA as a

---

Snowden, who is responsible for the NSA surveillance leaks. *Id.*

243. For example, Sen. Rand Paul (R-Ky.) proposed legislation that would require the federal government to have "a warrant based on probable cause" in order to seize phone records from Americans. *See* Sabrina Siddiqui, *Rand Paul Introduces Bill to Prevent Government Seizure of Phone Records Amid NSA Controversy*, HUFFINGTON POST (June 7, 2013, 4:18 PM), http://huffingtonpost.com/2013/06/07/rand-paul-nsa_n_3404308.html?1370631146. Senators Mark Udall (D-Colo.) and Ron Wyden (D-Ore.), who long warned of the government's surveillance methods, are seeking to limit the government's authority to collect data. *See* Sabrina Siddiqui, *Mark Udall, Ron Wyden Introduce Bill Limiting Federal Government's Authority to Collect Data*, HUFFINGTON POST (June 14, 2013, 4:43 PM) http://huffingtonpost.com/2013/06/14/mark-udall-ron-wyden-nsa_n_3442054.html?utm_hp_ref=politics. Sens. Jeff Merkley (D-Or.) and Mike Lee (R-Utah) co-sponsored a bill that would declassify FISA court opinions. *See* Luke Johnson, *FISA Bill Introduced to Declassify Court Opinions Used to Justify Surveillance*, HUFFINGTON POST (June 11, 2013) http://huffingtonpost.com/2013/06/11/fisa-bill_n_3421407.html. And, on June 24, 2013, Senate Judiciary Committee Chairman Patrick Leahy (D-Vt.) introduced legislation to revisit the Patriot Act Section 215 and FISA Amendment Act Section 702, under which the NSA programs are lawful. *See* Press Release, Senator Patrick Leahy, Statement of Senator Patrick Leahy (D-Vt.), Chairman, U.S. Senate Committee on the Judiciary, On Introduction of the FISA Accountability and Privacy Protection Act of 2013 Senate Floor (June 24, 2013), *available at* http://www.leahy.senate.gov/press/statement-of-senator-patrick-leahy-d-vt-chairman-us-senate-committee-on-the-judiciary-on-introduction-of-the-fisa-accountability-and-privacy-protection-act-of-2013-senate-floor. http://www.huffingtonpost.com/2013/06/28/nsa-bills_n_3516928.html.

244. *See* Sabrina Siddiqui, *NSA Surveillance Prompts Several Bills But Little Action in Congress*, HUFFINGTON POST (June 28, 2013, 5:10 PM), http://www.huffingtonpost.com/2013/06/28/nsa-bills_n_3516928.html (stating that "the Merkley-Lee bill has gained the most traction with 12 cosponsors").

245. *See* Melissa Riofrio, *It's Privacy Versus Cybersecurity as CISPA Bill Arrives in Senate*, PC WORLD, (Apr. 25, 2013, 3:00 AM) http://www.pcworld.com/article/2036328/it-s-privacy-versus-cybersecurity-as-cispa-bill-arrives-in-senate.html.

246. *See* Alina Selyukh and Deboarah Charles, *CISPA Cybersecurity Bill Backers Hope Second Time's a Charm*, NBC NEWS (May 16, 2013, 8:38 AM),

means to prevent cyber-attacks.[247] As currently drafted, however, CISPA makes sweeping changes to the law of electronic privacy because it permits data sharing between private industry and the government on an unprecedented scale and without any penalty for doing so.[248] The limitations of the Fourth Amendment and already existing statutory law are circumvented because the government grants immunity to companies that participate.[249]

The NSA programs are already justified on thin legal grounds.[250] Legislation such as CISPA attempts to codify and make legal the government's circumventing Fourth Amendment privacy rights.[251] The NSA surveillance programs and proposed legislation like CISPA demonstrate the need for comprehensive legislation to protect the collection, use, and sale of consumer private data, and to be effective, such legislation must apply in a parallel fashion to government and private industry.[252] No such legislation exists, however, nor is there any real proposal for such legislation.[253]

It is the result of this legislative and judicial void that private industry, using readily available technologies, tracks individuals.[254]

---

http://www.nbcnews.com/technology/cispa-cybersecurity-bill-backers-hope-second-times-charm-1C9948195.

247. *See id.* (discussing CISPA support from members of the Cabinet and Congress); *see also* Matt Peckham, *5 Reasons the CISPA Cybersecurity Bill Should Be Tossed,* TIME TECH (Apr. 19, 2012), http://techland.time.com/2012/04/19/5-reasons-the-cispa-cybersecurity-bill-should-be-tossed/.

248. *See* Peckham, *supra* note 247.

249. *See* Riofrio, *supra* note 245 ("The bill creates a high level of immunity from lawsuits for . . . private companies that share data.").

250. *See* Gellman & Poitras, *supra* note 240. PRISM was first launched during President George W. Bush's administration. *Id.* After leaks of domestic surveillance broke in 2007, Congress passed the Protect America Act and the FISA Amendments Act of 2008, "which immunized private companies that cooperated voluntarily with U.S. intelligence collection." *Id.* At the same time, FISA courts began to issue surveillance orders differently. *Id.* Under the Bush Administration, FISA judges no longer had to find "probable cause that a particular 'target' and 'facility' were both connected to terrorism or espionage." *Id.* FISA court orders remain secret and largely void of oversight, further complicating legal analysis. *Id.*

251. *See generally* Riofrio, *supra* note 245 (describing overly broad and vague terms of CISPA, government and private industry access to information without express authorization, and permissible information exchange between members of private industry).

252. *See, e.g.*, *id.* (explaining that without reciprocal permissions protecting consumers, the public will never be able to find out if their information has been collected and/or misused).

253. *See generally id.* (describing an ACLU spokesperson's hope that CISPA will encourage the Senate to come up with legislation that protects "the little guy" as much as it does "big data").

254. *See id.*

## VI. THE RISKS PRIVATE INDUSTRY POSES TO PRIVACY

Private industry's unfettered collection, use, and sale of citizens' personal data does pose risks.[255] One of these risks is that information collected will be used for purposes other than those expected by or disclosed to the consumer at the time of collection.[256] This privacy wrong has broad implications, because consumers currently have no choice about the gathering of their own information or its use.[257] Many people unknowingly supply data when a software app gathers it surreptitiously, or they supply information through the Internet or their smartphone for convenience.[258] In the latter case, they do so because their choice is either give information or be precluded from the use of a helpful or popular application.[259] Convenience often outweighs thoughts of privacy, yet when the information given is used for a purpose different from that of the application for which it was provided, the consumer has been wronged.[260]

Some newer technologies remove consumer choice entirely from the equation.[261] Face recognition technology, for example, is used in public and automatically captures one's image without consent, and in most cases, without knowledge that the data capture (and possible subsequent identification) has even happened.[262] A consumer cannot expect to have any semblance of control over their information and their identification if they do not realize their image has been taken or if the image was taken without consent.

Consumers are unaware of the quantity of information provided to and gathered by third parties through smartphones and Internet activity.[263] For example, by combining a consumer's likes and other

---

255. *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 878-84 (2003) (outlining both the "personal or private wrongs and public or societal wrongs" associated with the invasion of privacy).

256. *Id.*

257. *See id.* at 881-82.

258. Nicole Perlroth and Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. TIMES BITS BLOG (Feb. 15, 2012, 9:05 AM), http://bits.blogs.nytimes.com/2012/02/is/google-and-mobile-apps-take-data-books-without-permission?_r=0 (noting that "some of the most popular applications for the iPhone, iPad and iPod . . . tak[e] users' contacts and transmit[] it without their knowledge").

259. *See id.*

260. *See* Reidenberg, *supra* note 255, at 82.

261. *See* Alexei Oreskovic, *Facebook Facial Recognition Technology Sparks Renewed Concerns*, REUTERS (June 8, 2011, 5:26 AM), http://www.reuters.com/article/2011/06/08/uk-facebook-idUSLNE75701C20110608 (discussing reports of Facebook users that the company "enabled the facial recognition option the last few days without giving users any notice").

262. *See id.*

263. *See* Ian Truscott, *When Mobile, Location, and Content Converge – I'll Have a*

personal information with face recognition technology, a previously anonymous person in public could be identified and then targeted with specific marketing based upon the combination of that identification with the already-collected personal information.[264]

A second risk—and the privacy issue probably felt by most consumers—is the "lack of understanding" of how personal information is collected and used by private industry.[265] Data collection and use practices are "invisible to consumers."[266] Most consumers are unaware of exactly how information is collected and what is done with that information.[267] The fear that one's personal information is "out there" without any control over who has it or where it is going may be a harm that is less tangible than other harms, such as physical economic loss, but it is just as real.[268] Consider how a consumer's tracked preferences may impact search results for information, not just for targeted product marketing. The question of how collected personal data (i.e., tracked preferences) may impact search results is a serious one. Could a conservative individual's political preferences (easily known from tracking his online activity) result in his receiving a different Google search result than a liberal individual who ran the same query? The answer is "yes."[269]

Consumers who do make an attempt to understand how their information is used are often met with an impenetrable wall in the form of a privacy policy.[270] The FTC describes privacy policies as being too long, too complex, and in "too many instances,

---

*Guinness*, READWRITE BLOG (Dec. 26, 2011), http://readwrite.com/2011/12/26/when_mobile_location_and_content_converge_-_ill_ha (observing that "the general public doesn't seem to mind" the "large-scale information gathering").

264. *See id.* Ian Truscott advances a plausible scenario that could result from such data usage:

> [I]f Smith & Wollensky in New York had a party of six just cancel their reservation, and knew that five of my colleagues and I were at an industry event around the corner, the combination of these data points (my location, my likes, what I'm doing and at what time of day) could allow them to create an offer that brings them a customer immediately.

*Id.*

265. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS: PRELIMINARY FTC STAFF REPORT 25 (2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf.

266. *Id.* at 25-26.

267. *Id.*

268. Reidenberg, *supra* note 255, at 881.

269. *See id.* at 882 (discussing how the use of personal information leads to solicitation).

270. FED. TRADE COMM'N, *supra* note 265, at 19-20.

incomprehensible to consumers."[271] There is an additional difficulty when privacy policies are viewed on a mobile device. Smaller screen size makes it unlikely that a consumer is going to scroll through multiple screens to read the full policy.[272] Even if they are understood, privacy policies are used more for limiting the liability of a company "than to inform consumers about how their [personal] information will be used."[273] Additionally, privacy policies do not allow any amount of choice.[274] A consumer is essentially given the option to use the service or not.[275] Whatever the service provides usually trumps the fear of information collection.[276]

There are some clear benefits to the consumer. Some consumers desire and prefer targeted advertising. If given the choice, many companies have found that consumers want to control and limit some forms of information collection while allowing collection for advertising in certain instances.[277] Consumers may prefer targeted advertising as opposed to an all or nothing approach to receiving advertisements because it means more efficient advertising and less of a barrage of unwanted solicitations.[278]

This is important to incorporate in legislation because many privacy guidelines, including "Do Not Track," have been described as bad for business and the Internet. Mike Zaneis, the Interactive Advertising Bureau's senior vice president and general counsel for public policy, argues that mechanisms like "Do Not Track could affect 80 percent of web ads" and eventually "forc[e] free content sites to charge subscription fees."[279]

But are these claims overblown? Do Not Track can still sell "'non-targeted' ads"[280] or "contextual ads,"[281] as opposed to targeted advertising that uses cookies to track an Internet user's history.[282]

---

271. *Id.* at 19.

272. *Id.* at 70.

273. *Id.* at 19.

274. *See id.* (noting that "while many companies disclose their practices, a smaller number actually offer consumers the ability to control these practices").

275. *See id.* at 19-20 ("[C]onsumers face a substantial burden in reading and understanding privacy policies and exercising the limited choices offered to them.").

276. *Id.* at ii.

277. *Id.* at 68.

278. *See id.* at ii.

279. Cohn, *supra* note 192.

280. Examples of non-targeted ad include random advertisements such as "Click to win an iPad!" *See id.*

281. Advertisements based on a company's own content as opposed to the content of its users' cookies are considered contextual ads. *Id.*

282. There may be other ways to use cookies without tracking. Jonathan Mayer and Subodh Iyengar may have created an approach that allows for targeted advertising without tracking. Jonathan Mayer & Subodh Iyengar, *Tracking Not Required: Behavioral Targeting,* 33 BITS OF ENTROPY (June 11, 2012, 2:42 PM),

Still, there may be even less harm to private industry with greater choice options for consumers. This should play an important role in legislation so that business is not stifled while still ensuring consumers are protected.

Privacy legislation that regulates data retention and limits data use is more likely to create trust between industries and their consumers. An auditing mechanism would reinforce this trust and perhaps lead more consumers to employ choice and allow desired types of targeted advertising. FTC studies support the idea that consumer privacy legislation does not have to be an all-or-nothing proposition adverse to private industry. Reports and examples[283] from the European Union (EU) prove it is possible to grant consumer privacy protections without crippling private industry.

*A. Current Voluntary Guidelines*

The United States lacks any meaningful legislation to regulate and/or protect how private industry collects, uses, and sells the personal information it obtains, often surreptitiously.[284] In the face of an increasing number of technologies that allow for the dragnet collection of consumers' personal information, the EU has been more aggressive in its protection of personal information and data, enacting the Data Protection Directive as early as 1995.[285]

---

http://33bits.org/2012/06/11/tracking-not-required-behavioral-targeting/.

283. The EU passed the "Cookie Law" with varying degrees of compliance by EU member states. *Cookie Law Frequently Asked Questions,* THE COOKIE COLLECTIVE, http://www.cookielaw.org/faq.aspx (last visited Nov. 26, 2013). In the United Kingdom, the Cookie Law went into effect in 2011 with a one-year grace period. *Id.* The law requires websites to provide notice that they are using cookies and obtain user consent to do so. *Id.* Some critics have said implementation of the Cookie Law has resulted in a diminished user experience without increasing privacy. *Id.* Some scholars argue that this is a problem with the implementation of the law rather than with the concept. The United States has an opportunity and should seize upon it to learn what type of implementation works and what has failed. One mechanism to give users control over cookies is "Optanon." *Optanon Privacy Preference Center*, THE COOKIE COLLECTIVE, http://www.cookielaw.org/optanon.aspx (last visited Nov. 26, 2013). Through Optanon, whenever a user visits a website, a small bar is opened at the top or bottom of the page informing the user that the website uses cookies and including a link for more information. *Id.* A tool bar can also be used to control what types of cookies are implemented while a user is on that website. *Id.* The tool bar includes a menu of five choices including an overview about controlling one's privacy and then four choices that directly allow the user to determine which cookies to allow. *Id.* "Strictly Necessary Cookies," for example, when clicked, explain what they do and are automatically on to ensure the website functions. *Id.* On the other extreme are "targeting cookies." *Id.* These cookies are briefly described as including relevant information about targeted advertising and also include an option to allow or disable those particular cookies. *Id.*

284. *See supra* notes 62-63 and accompanying text and Part V.B.

285. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L28131)

Although legislatively, the United States has failed to protect consumer information, there have been some moves in the United States towards providing personal data and privacy protections.[286] For instance, the FTC issued voluntary guidelines for commercial use of face recognition technologies, and some marketing industries have issued codes of conduct as a form of self-imposed regulation.[287] The FTC has issued a report urging consumer privacy online, the most notable portion of which is its "Do Not Track" guidelines.[288] These FTC guidelines illustrate what rapidly advancing surveillance and tracking technology is capable of and how to implement use of the same technologies with privacy in mind.[289] While a useful theoretical starting point, the FTC guidelines lack teeth. They do not provide an enforcement mechanism, and companies that have willingly imposed self-regulation measures are only subject to FTC enforcement if they break their own adopted code of conduct.[290] These guidelines and codes of conduct do not do nearly enough to protect Americans. Because the FTC's Do Not Track proposal and face recognition technology guidelines are sources to consider when adopting future legislation, they bear closer analysis.

1. FTC Do Not Track Guidelines

A preliminary 2010 and updated 2012 FTC Report entitled *Protecting Consumer Privacy in an Era of Rapid Change* supports a Do Not Track approach.[291] The FTC suggests that Do Not Track be implemented through a cookie or a setting on a user's Internet browser that would allow the consumer choice in (1) whether to allow Internet websites to track them and (2) whether to receive targeted advertising.[292]

Some companies and browsers already offer some form of a Do Not Track mechanism.[293] Current Do Not Track programs, however, have not been adopted industry-wide, and many consumers are unaware such programs exist.[294] Moreover, the Do Not Track choices being offered to consumers are often unclear in explaining the scope

---

[hereinafter Council Directive 95/46/EC].

286. *See, e.g.*, FED. TRADE COMM'N, *supra* note 192, at 4-5 (prefacing recommendations with a review of attempts to enact consumer privacy laws and voluntary private sector adoption of Do Not Track standards).

287. FED. TRADE COMM'N, *supra* note 265, at 45-48.

288. *See id.* at 66-67.

289. *See id.* at 39-40.

290. FED. TRADE COMM'N, *supra* note 192, at 10 n.47.

291. FED. TRADE COMM'N, *supra* note 265, at vi-vii; FED. TRADE COMM'N, *supra* note 192, at v.

292. FED. TRADE COMM'N, *supra* note 265, at vii.

293. *Id.* at 63-64.

294. *Id.* at 25, 33, 43, 64-67.

of the tracking that actually occurs and the limitations of current, voluntary, and self-regulated Do Not Track mechanisms.[295] Do Not Track is a mechanism that can be legislated in language that is non-technology specific. Such legislation should protect an individual's right to not be tracked in his or her online activities, regardless of the technology through which an individual is engaging in online activity and regardless of what technologies are or become available to track the individuals' online activity.[296] Moreover, any Do Not Track legislation should address uniformity, public awareness, and consumer choice in tracking.[297]

2. The FTC Face Recognition Technology Guidelines

As previously discussed, face recognition technology has opened a new platform for companies to market their products. The FTC has correctly identified the privacy implications of using face recognition technology.[298] One of the main dangers to privacy by face recognition technology is the ability to identify previously anonymous people by matching anonymous images with prior images in which that person had been identified. With an exception,[299] the use of face recognition technology for commercial purposes is unregulated. Because face recognition technology use has expanded significantly in the past decade,[300] it is important to pass privacy legislation that protects biometric identifiers (such as one's facial biometrics) in language independent of specific biometric identification technologies. Biometric identification technology is evolving so rapidly that any law passed with language or application specific to a particular biometric identification technology (as opposed to protecting the biometric information itself) will be obsolete within months.

Consider currently used or planned face recognition uses: Companies such as Kraft and Adidas plan to use in-store digital signs equipped with face recognition cameras to target ads specifically tailored for the customer walking near the sign.[301] This raises serious privacy concerns. The face recognition cameras will

295. *Id.* at 64-65.

296. *Id.* at iii.

297. *Id.* at 70, E-6-7.

298. *Id.* at 14-16.

299. *See* 740 ILL. COMP. STAT. 14 (2008) (passing the Biometric Information Privacy Act); TEX. BUS. & COM. CODE ANN. § 503.001 (West 2009) (requiring notice and consent to use biometric identifiers for a commercial purpose).

300. This is well demonstrated by the number of patents issued by the U.S. Patent office. In the twenty-five years between 1970 and 1995, the Office issued fewer than ten patents for facial recognition technology. Donohue, *supra* note 150, at 410. Between 1995 and 2000 the number of patents jumped to twenty. *Id.* Between 2001 and 2011, the number of patents skyrocketed to 633 patents relating to facial recognition technology. *Id.*

301. FED. TRADE COMM'N, *supra* note 291, at 5 n.20.

identify the age and demographics of the person to target an ad, but what if the camera is used to identify the individual as opposed to the demographic group? Current face recognition technology now makes the identification of the individual possible.[302] How would notice be provided? Can the sign be avoided if desired by the customer? Is the image taken retained and stored by the company or sold to a third party?

Such practices and scenarios are currently unregulated by federal legislation or through mandatory guidelines.[303] While some companies do self-regulate and have in place privacy policies that consider consumer concerns, there is no mechanism to ensure that privacy policy changes are approved by or acceptable to consumers, or that private industry is required to provide consumers with an opt-in or opt-out choice.[304]

Companies that do have aggressive consumer-focused privacy features can market themselves as the privacy friendly company, but such self-imposed acts do nothing to set standards for the industry as a whole, nor does it mean that a company is actually applying adequate consumer privacy protections.

In its 2012 report, the FTC sums the problem up well: "[C]onsumers face a landscape of virtually ubiquitous collection of their data."[305] And the FTC makes an important point to consider when legislating to protect consumer data: "Whether such collection occurs online or offline does not alter the consumer's privacy interest in his or her data."[306] In the FTC's report and in other industry and privacy advocate reports, there are similarly proposed privacy protection measures.[307] While some suggestions are specific as to a particular type of web or mobile applications or technology, the proposals all include instituting "privacy by design," which entails: data security measures, reasonable retention and storage practices, clear notice and transparency, simplified choices, and accountability.[308] The practices proposed and identified by the FTC should be incorporated into legislation in such a way as to apply to data collected off and online.

---

302. *Id.* at 4.

303. FED. TRADE COMM'N, *supra* note 265, at 19-20 (describing the limitations of existing legislation).

304. *Id.* at 70-72, 76-77 (recommending that such regulations come into existence).

305. FED. TRADE COMM'N, *supra* note 192, at 19-20.

306. *Id.* at 18.

307. *Id.*

308. Privacy By Design means companies should "build in privacy at every stage of product development." *Id.* at i. When companies are designing products, applications, or methods to collect personal information, they should consider initially how to make their practices transparent and give greater choice to consumers. FED. TRADE COMM'N, *supra* note 291, at ii-iii.

3. The European Union Model

The EU has the most comprehensive set of principles pertaining to the protection of personal data.[309] The 1995 Data Protection Directive[310] focuses on the protection of data that is processed, used, or exchanged "by automated means," such as "a computer database of customers."[311] The principles encompassed in the EU Directive include: notice to the subjects whose data is collected;[312] notice about the purpose for which the data is collected;[313] the data should be used for that limited purpose only;[314] the personal data should not be disclosed to third parties without consent from the subjects whose data is collected;[315] collected personal data should be kept secure;[316] the identities of the entities collecting data should be disclosed to the subject of collection;[317] subjects should be granted access to the information as a way to control their information and ensure accuracy;[318] and subjects should have redress in order to hold collectors accountable.[319]

Eighteen years after its passing, the EU is working to revise the Directive.[320] The European Commission says the proposal is meant to give users greater control of their data and to cut costs for businesses.[321] The proposal, due out in 2014, focuses on creating a single set of rules and alleviating unnecessary administrative requirements; it also gives greater enforcement power to independent data protection authorities.[322]

The EU's new proposed standards have generated some criticism. One version of the proposal includes the "right to be

309. Personal data is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." Council Directive 95/46/EC, *supra* note 285, at art. 2(a).

310. *Id.* at 31.

311. *Protection of Personal Data,* EUROPA, (Feb. 1, 2011), http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm.

312. *See* Council Directive 95/46/EC, *supra* note 285, at ch. II, § IV, art. 10.

313. *Id.* at ch. II, § IV, art 10(b).

314. *Id.* at ch. II, § I, art. 6(b).

315. *Id.* at ch. II, § III, art. 8(d).

316. *Id.* at ch. II, § I, art. 6(1)(c).

317. *Id.* at ch. II, § IV, art. 10(a).

318. *Id.* at ch. II, § IV, art. 12(b).

319. *Id.* at ch. II, §§ VII, art. 14(b); IV, art. 23(1).

320. *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses*, EUROPA, (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en.

321. *Id.*

322. *Id.*

forgotten."[323] The right to be forgotten would make it mandatory for social media companies to delete all information previously collected on a user upon the user's request.[324] This would enable the user a chance to wipe the slate clean. Such provisions are consistent with the goal of the revisions, which is largely a response to social media companies' unfettered gathering and retaining vast quantities of intimate user data, including messages, photos, likes and dislikes, friends, preferences, et cetera.[325] Critics, however, contend that the right to be forgotten proposal will create a "new layer of regulation for [a large number] of businesses that have nothing to do with social media."[326] Another proposed requirement is that businesses ask for and obtain "explicit prior consent" from consumers before engaging in targeted advertising.[327]

The Directive is meant to protect the right to privacy, which is recognized in Article 8 of the European Convention on Human Rights.[328] The United States has much to learn from the EU's experience in implementing privacy legislation.[329] Unlike the problem of disparate protections amongst EU member states, the United States has the benefit of being able to set the floor for privacy legislation and allow states to, at a minimum, meet that floor or implement greater privacy protections.[330] Additionally, the United States can learn from the successes and failures of the independent data protection authorities when considering how much enforcement

---

323. Sally Annereau, *Are New Data Protection Proposals for a Right to Be Forgotten Workable?,* THE GUARDIAN (Apr. 22, 2013, 8:24 AM), *available at,* http://www.theguardian/media-network/media-network-blog/2013/apr/22/data-protection-right-to-forgotten.

324. *Id.*

325. Council Directive 95/46/EC, *supra* note 285, at ch. I, art. 1.

326. Kevin J. O'Brien, *Firms Brace for New European Data Privacy Law,* N.Y. TIMES, May 14, 2013, *available at* http://www.nytimes.com/2013/05/14/technology/firms-brace-for-new-european-data-privacy-law.html.

327. *Id.*

328. European Convention on Human Rights, art. 8, Sept. 3, 1953, www.echr.coe.into/Documents/Convention_ENG./pdf.

329. *See Facial Recognition & Privacy: An EU-US Perspective,* CENTER FOR DEMOCRACY AND TECHNOLOGY 6-7 (Oct. 8, 2012), https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf (discussing how EU member states have enacted a "patchwork of regulations for image-data processing" and stating that there is "an uncertain regulatory environment for facial recognition" technology because the Directive "merely sets high-level principles for [the technology]").

330. *See* U.S. CONST. art. VI, cl. 2 (providing that "the Laws of the United States . . . shall be the supreme Law of the Land . . . anything in the . . . Laws of any State to the Contrary notwithstanding"); *Facial Recognition & Privacy*, *supra* note 329, at 10 (noting that "the most sensible solution is setting a floor of privacy protections, with one comprehensive framework").

power to give a similar oversight body.[331]

*B. Legislative Solutions*

As hopefully this Article has demonstrated thus far, despite our country and our courts' unique roles in developing and recognizing the modern concept of an individual's inalienable right to privacy, the United States continues to lack a legislative framework to adequately protect its citizens' personal data from the extraordinary advances in technology that permit government and private industry's surreptitious, non-intrusive acquisition of that data.[332]

In theory, the Fourth Amendment and Title III should provide citizens protection from the government's warrantless electronic surveillance and collection of our personal data; but as this Article has outlined, rapid advances in technology and the NSA's warrantless surveillance programs call the efficacy of the Fourth Amendment and wiretapping laws' protections into question.[333] Moreover, even though some aspects of Title III, including the ECPA and the SCA, apply to private individuals and private industry, the Fourth Amendment and the federal electronic surveillance scheme do nothing to protect citizens from the pervasive information collected by private industry.[334]

But the United States has the ability to correct these problems. We have the benefit of model legislation in the EU privacy directive, and we can learn from the redundancies and administrative burdens that businesses in the EU have faced.[335] Thus, we will be able to implement a streamlined form of legislation that protects consumers while having a minimal prohibitive effect on business.[336] Moreover, federal regulators at the FTC and many advertisers support the implementation of privacy legislation that protects both the personal information of consumers while balancing the needs of businesses and ensuring continued innovation.[337] By creating uniform standards, legislation could ultimately save businesses money.

What is the proper framework for a legislative solution? For reasons discussed above, a legislative framework that relies upon one's reasonable expectation of privacy is not ideal for potential legislation.[338] Nor is legislation that is specifically geared towards

331. *See Facial Recognition & Privacy*, *supra* note 330, at 11-13.

332. *See* discussion *supra* Part II-VI.A.

333. *See* discussion *supra* Part II.A; *see also* U.S. CONST. amend. IV; Electronic Communications Privacy Act, 18 U.S.C. § 2510 (2006).

334. 18 U.S.C. §§ 3121-3127 (2006).

335. *See* discussion *supra* Part VI.B.

336. *See supra* notes 308-319.

337. *See generally* FED. TRADE COMM'N, *supra* note 265 (discussing ways in which this balance may be met).

338. For instance, the FTC Guidelines consider possible uses of facial recognition

one particular technology.[339] In fact, one consistent failing in privacy legislation has been that legislation is drafted in technology-specific terms or technology-specific application; given the pace of advancements in technology, this has resulted in outdated and inapplicable portions of law.[340] Rather, legislation should focus on protecting types or categories of data. This would foster new technology designs to adapt to legislative protections as opposed to legislation slowly and inconsistently adapting to new technology. It will create greater uniformity and result in clearer standards for private industry to follow because the way the information is collected is not at issue; rather, the type and breadth of the information collected is protected.

The most important aspect of any legislation designed to protect citizens' privacy, however, is that it be applicable in parallel ways both to private industry and to government. The disparate ability of private industry to collect vast quantities of data versus the

---

technology and address how the FTC Guidelines would apply to these possible scenarios. FED. TRADE COMM'N, *supra* note 291. In one scenario involving digital signs equipped with facial recognition technology, the FTC suggests that notice should be given because "the use of these technologies within digital signs is not currently consistent with reasonable consumer expectations." *Id.* at 14-15. This is precisely the type of standard however, that should be avoided when implementing legislation. Although non-binding, the FTC's suggestion that notice is only required when consumers do not have a reasonable expectation of privacy, suggests that once this technology is pervasive, notice will no longer be required because consumers will know that signs are equipped with facial recognition software. But the FTC's reliance upon the reasonable expectation of privacy test is problematic. As Justices Sotomayor and Alito have suggested, the reasonable expectation of privacy standard needs to be reevaluated. *See* United States v. Jones, 132 S. Ct. 945, 954, 957 (2012) (Sotomayor, J., and Alito, J., concurring).

339. *See Facial Recognition & Privacy*, *supra* note 330, at 1 (acknowledging the wide variety of technology that may result in abuses and the need for a comprehensive framework to combat privacy invasion).

340. The Electronic Communications Privacy Act (ECPA) for example, was an extension of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. ELECTRONIC COMMUNICATIONS PRIVACY ACT AMENDMENTS ACT OF 2013, S. REP. NO. 113-14, at 2 (stating that the Electronic Communications Privacy Act amended the Omnibus Crime Control and Safe Streets Act). When Title III was enacted, computers, email and other technologies were not available. By 1986, though, such technologies were becoming widespread, which lead to new protections under ECPA to protect "electronic communications" and stored wire communications among other updates. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (1986). ECPA is considered a good law; however, over a quarter of a century later ECPA is overdue for an update once again. Senate Judiciary Committee Chairman Patrick Leahy and Sen. Mike Lee introduced the Electronic Communications Privacy Act Amendments Act of 2013 to update the law to reflect "new privacy concerns and new technological realities." Press Release, Senator Patrick Leahy, Lee Introduce Legislation to Update Electronic Communications Privacy Act (Mar. 19, 2013), http://www.leahy.senate.gov/press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

government's ability to collect the same data has deleterious consequences on several fronts. On the one hand, our privacy is not meaningfully protected because private industry is able to collect, retain and sell our intimate personal data. On the other, the government is hamstrung in its abilities legally to monitor activities in a way that does not chill First Amendment rights or violate the Fourth Amendment.[341] And regardless, the NSA surveillance leaks demonstrate that if private industry is lawfully collecting the data, the federal government will find ways to access the data.[342]

1. Proposal for Legislation

The following is a rough framework for proposed legislation to protect an individual's right to privacy in the modern era; this legislation would be applicable in the same or a parallel fashion to private industry and to government.[343]

a. Transparency

Transparency is a significant obstacle to consumer privacy rights because consumers are simply unaware of or uninterested in understanding what private industry is capable of.[344] Beyond seeing targeted ads on their computers or receiving targeted marketing information, there is not enough understanding of where, when, and how companies collect consumer information.[345] Transparency is essential to furthering the needs and rights of consumers.

Strong legislation must include a requirement for companies collecting consumer information to be clear and concise about who is collecting the information, what information is collected, how that information is collected, the purpose for which data is used, whom the data is shared with, with what information the collected data is combined, how the company secures data, how long the data is retained, choices consumers have with regard to that data, how to correct that data, and a company contact for problems and

341. U.S. CONST. amend. I; U.S. CONST. amend. IV.

342. Madrigal, *supra* note 2.

343. The framework is the result of this Author's almost two decades of researching, writing, practicing law, and teaching about privacy, federal and state wiretapping and privacy laws, as well as from reviewing and considering other sources, including the EU Data Protection Directive, FTC Guidelines, and proposed drone legislation. In addition, my thoughts have been shaped over the years by the opportunity to work with so many brilliant, amazing privacy scholars through the yearly Privacy Law Scholar's Conference, through working with many fine panelists at various law school events, and the Professors at The Catholic University of America, especially Clifford S. Fishman, and Mary Leary, among others.

344. DIGITAL SIGNAGE FEDERATION, *supra* note 291, at 4-6 (explaining the need for privacy policies and notice for the sake of transparency).

345. FED. TRADE COMM'N, *supra* note 291, at iii (demonstrating how information can be gathered on an individual without his or her knowledge).

feedback.[346] This information should be given by something other than a privacy policy. This should be written to apply in both online scenarios as well as offline scenarios. For example, if a kiosk or sign is placed in a public area and uses facial recognition technology, consumers should be able to easily avoid the area, receive multiple forms of notice prior to falling within the sign's purview, and have the option to access further information explaining the previously required material.[347] A generic form of notice, such as "[t]hese premises are under video monitoring" would not comply because it fails to provide enough transparency.[348]

b. Storage and Data Retention

Data should not be stored or retained once the initial purpose for which that data was collected becomes obsolete.[349] This provision may include an exception if the company receives informed consent from the consumer whose image or information is being retained.[350] Furthermore, companies should not only explain their storage and retention policies, but ensure those policies are reasonable.[351] Legislation must include a time limit for when companies must dispose of stored information, unless the company demonstrates that the retention of such information continues to serve its initial purpose.[352]

c. Choice

Legislation must require companies to give consumers a choice as to what types of advertising to receive. More importantly, legislation must require that companies provide consumers a meaningful choice as to how and to what extent their information is collected and used. As previously discussed, consumer behavior suggests that consumers want granular or delineated choices as opposed to an all or nothing form of information collection.[353] The EU has a similar provision in place and several member states have

346. DIGITAL SIGNAGE PRIVACY STANDARDS, *supra* note 291, at 4.

347. FED. TRADE COMM'N, *supra* note 291, at 15.

348. DIGITAL SIGNAGE PRIVACY STANDARDS, *supra* note 291, at 6.

349. In the digital sign equipped with facial recognition technology this would mean that the image would not be stored once the consumer has received the targeted advertisement. *See* FED. TRADE COMM'N, *supra* note 291, at 14.

350. *Id.* at 12.

351. *See id.* at 11.

352. *See id.* at 11 (stating that a company "should implement a specified retention period and dispose of stored images once they are no longer necessary for the purpose for which they were collected").

352. *See* FED. TRADE COMM'N, *supra* note 265, at ii (discussing the differences in consumer opinions on collection of certain categories of information).

353. *See id.* at ii (discussing the differences in consumer opinions on collection of certain categories of information).

already instituted choice mechanisms.[354] Some methods of implementation have been more successful than others. Regardless, U.S. legislation should require that consumers are given choices and companies can look to EU companies as to how this can be most successfully implemented.

d. Consent

Consent is inextricably connected with notice and choice. For instance, a company may not need to obtain consent to collect a consumer's contact and credit card information following a purchase or for first party marketing.[355] Amazon.com, for example, recommends products based on prior purchases and offline retailers may provide coupons for previously purchased merchandise.[356] Websites and retailers using first party marketing, however, should receive consent if that data is shared with a third party or affiliate.[357] The type of consent required should be based on the type of information sought to be collected and used. The Digital Signage Federation (DSF) partnered with the Center for Democracy and Technology to create categories based on how information is collected, what type of information is collected and what is done with that information.[358] Based on the category the type of collection falls within, the DSF determines whether opt-in or opt-out consent is required.[359] While this particular model is not necessarily what

354. EUROPA, *supra* note 312, at 2 (noting the "right to object" to data collection and storage).

355. FED. TRADE COMM'N, *supra* note 265, at 54.

356. *See generally* Amazon, http://www.amazon.com (last visited Nov. 26, 2013).

357. FED. TRADE COMM'N, *supra* note 265, at 55.

358. DIGITAL SIGNAGE PRIVACY STANDARDS, *supra* note 291, at 6-7. "Level I: *Audience counting*. Information related to consumers is gathered on an aggregate basis, but are not used for tailoring advertisements in real time (i.e., as the consumer walks by the sign). No retained information, including images, links to individuals or their property." Example: Facial recognition systems that only track gazes or record passerby demographics, but do not tore facial images or unique biometric data points. The advertisements are not tailored to demographics in real time. "Level II: *Audience targeting*. Information related to consumers is collected on an aggregate basis and is used for tailoring contextual advertisements to individuals in real time. No retained information, including images, links to individuals or their property." Example: Facial recognition systems that record passerby demographics and contextualize ads accordingly as the consumer walks by. "Level III: *Audience identification and/or profiling*. Information related to consumers is collected on an individual basis, regardless of whether or when the information is used to tailor advertisements. Information is retained that links to individual identity, unique travel or purchase patterns, or an individual's property (such as a mobile phone). Example: combining a digital signage system with social networking, RFID tracking, mobile marketing.

Example: combining a digital signage system with credit card receipts, online browsing habits, purchases, or third party marketing data.

DIGITAL SIGNAGE PRIVACY STANDARDS, *supra* note 291, at 7.

359. *Id.* at 7. The DSF specifies that: "Levels I and II should implement opt out

should be adopted, a similar type of framework may be appropriate to determine what type of consent is required. Consent should be revocable at any time and a mechanism should be in place so that this can easily and efficiently be done.

e. Data Security

The FTC already has some enforcement power under Section 5 of the FTC Act. Since 2001, the FTC has brought actions in thirty-six cases against businesses that have failed to appropriately protect consumers' personal information.[360] Companies such as Google and Twitter have already responded to such actions by increasing data security by encryption of consumer communication and data.[361] However, legislation applicable to online providers as well as those in public using facial recognition and other technologies is required. Legislation must require companies to take reasonable measures to protect collected data from hacking and security breaches. Failure to do so should result in penalties for the companies. What is reasonable could be determined based on current industry standards.

f. Auditing/Oversight

Enforcement is necessary to ensure that companies are in compliance with legislation. The EU Directive for example, requires each member state to create an independent supervisory board or authority to oversee the implementation of the privacy directive as well as enforce and bring suits against companies found to be in violation of the Directive.[362] For purposes of U.S. legislation, there should be a body[363] charged with the investigation or auditing of private industry as well as the power to enforce any violations of the requisite statute. In the United States, the FTC could be charged with the investigation and there could be an FTC-based or independent government enforcement body against companies that violate privacy legislation. But providing a civil remedy for statutory

---

consent. At minimum, opt-out consent can be accomplished via notice. Notifying consumers that a particular signage unit collects information gives consumers the opportunity to avoid that signage unit.

Level III requires opt-in consent, which should be issued after the consumer has the opportunity to examine the applicable privacy policy." *Id.*

360. FED. TRADE COMM'N, *supra* note 192, at 24.

361. *Id.* at 25-26.

362. Council Directive 95/46/EC, *supra* note 285, at ch. VI, art. 28.

363. This could be the FTC. The FTC is already granted enforcement power over a variety of consumer protection statutes such as the Equal Credit Opportunity Act, Truth-in-Lending Act, and the Fair Credit Reporting Act among several others. *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FED. TRADE COMM'N, http://www.ftc.gov/ogc/brfovrvw.shtm (last visited Nov. 3, 2013).

violations is also necessary.[364] It is frequently American civil trial attorneys who most aggressively protect individual privacy rights.[365] Our civil trial attorneys have a demonstrated record of using the existing legal system to help enforce statutory provisions that protect individuals, consumers, and businesses.[366] One such example of this is the Computer Fraud and Abuse Act, which permits civil actions to be brought when a person accesses a protected computer without authorization or in excess of authorization.[367] Using the CFAA's statutorily provided civil cause of action, trial attorneys are able to protect data and intellectual property in new ways.[368]

g. Damages/Penalty

Legislation must provide a criminal violation *and* a civil cause of action or civil remedy to any individual who has been damaged under the statute. In addition to the FTC or other body charged with investigating and enforcing the statute, courts should have the means to provide injunctive relief and place other fines or penalties for violations of the statute. For example, the proposal for revisions to the EU Directive includes a provision for graduated fines.[369] Another option may be to impose graduated fines, but have those fines be proportionate to the size and profit of the business that committed the violation. Such a system may create the desired deterrent effect without crippling smaller businesses with lower profits, while also providing a meaningful fine to companies with immense profits. Permitting a civil cause of action for violation of the statute, if certain conditions are met, would allow trial attorneys to ensure businesses and individuals comply with statutory provisions

364. *See* Kristin M. Beasley, *Up-Skirt and Other Dirt: Why Cell Phone Cameras and Other Technologies Require a New Approach to Protecting Personal Privacy in Public Places*, 31 S. ILL. U. L.J. 69, 92 (2006) ("Civil suits are necessary because vindication of an individual's right to personal privacy benefits a society as a whole by protecting all citizens' expectations of personal privacy from erosion.").

365. *See, e.g.*, *id.* at 93 ("[C]ivil plaintiffs may be more motivated than criminal prosecutors, for whom this type of behavior may seem relatively harmless . . . .").

366. *See id.* at 92-93 ("If courts become accustomed to extending the right to personal privacy into public areas in circumstances in which a person has a reasonable expectation of privacy in criminal suits, victims may have a better chance at recovery in a civil suit for invasion of privacy . . . . Therefore, under the private attorney general theory, individual plaintiffs should be encouraged to bring civil suits to protect important rights that traditional law enforcement may be unable to adequately protect.").

367. 18 U.S.C. § 1030(a)(2), (g) (2006).

368. *Id.*

369. Judy P. Schmitt & Florian Stahl, *How the Proposed EU Data Protection Regulation is Creating a Ripple Effect Worldwide*, PRIVACY ASSOCIATION.ORG (Oct. 11, 2012), https://www.privacyassociation.org/media/presentations/A12_EU_DP_Regulation_PPT.pdf.

to protect consumers or face a civil lawsuit.

h. An Individual's Access to Data

The EU Directive includes the right of individuals to access the information that has been collected about them and to have some amount of measurable control over it.[370] The purpose is to ensure accuracy of the data.[371] There have been similar suggestions for U.S. legislation. Consumer access to collected data does have many benefits. While it improves transparency of collection practices, it also creates issues with data security and may require companies to create consumer profiles when they do not already do so. These issues may bring prohibitive costs to companies.[372] The FTC suggests that one option is a "sliding scale approach"[373] in which consumer access would be proportionate to the "intended use and sensitivity of the information."[374] Such a provision may also be applicable to certain formats, such as social media sites. In the context of social media for example, the user creates and in theory controls his or her profile. For that reason, the user should have greater access and control of that information and how it is used.

i. Other Considerations: Use, Protection, and Education

The creation of parallel standards to govern private industry and government's collection, retention, and use of personal data would address the current problem of government use. The recent "Prism"[375] revelations exemplify why Congress should pass legislation that provides for "government use" in compliance with the Fourth Amendment and other statutory law before it can access personal information obtained by private companies. Congressional legislation could provide for exceptions for national security or monitoring of foreign nationals. The EU Directive, for example, provides exceptions to the Directive in cases of national security and the "prevention . . . of criminal offences."[376]

---

370. Council Directive 95/46/EC, *supra* note 285, at ch. II, § IV, art. 10.

371. *Id.* at ch. II, § I, art. 6(d).

372. FED. TRADE COMM'N, *supra* note 265, at 73-74.

373. FED. TRADE COMM'N, *supra* note 192, at 29.

374. *Id.* at 29-30.

375. Prism is a surveillance program operated by the NSA under the supervision of the FISA court. Stephen Braun et al, *Secret to Prism Program: Even Bigger Data Seizures*, THE ASSOCIATED PRESS, (June 15, 2013, 2:53 PM), http://bigstory.ap.org/article/secret-prism-success-even-bigger-data-seizure. The Associated Press reports that Prism is actually a small part of a much more expansive eavesdropping program. *Id.*

376. Council Directive 95/46/EC, *supra* note 285, at ch. II, §VI, art. 13(d). The EU standard, however, may provide too few limitations on government. U.S. legislation should include some meaningful limitations on the Government's collection power and provide more transparency about the government's use of data "collected by private

Legislation should also include a provision devoted to protecting certain vulnerable groups, such as children. The proposed revisions to the current EU Directive include a provision that requires consent given by a child's parent or guardian to use data collected from children under the age of thirteen.[377] Similar provisions should be considered in U.S. legislation, including the protection of children and other vulnerable parties, such as those with certain disabilities or diminished mental capacity.

Finally, there should be a provision encouraging further consumer education. Many companies have already undertaken efforts to explain what is done with consumer data.[378] Such programs should be expanded to educate consumers so individuals can make an informed decision on how much personal information to divulge to private companies.

### 2. Recent Events Demonstrate Why Parallel Standards Must Be Part of Legislation

Facebook recently announced changes to its user and privacy policies under the guise of clarifying its practices; however, upon closer inspection, it was astonishing to read what the privacy policy changes were actually about. According to *The New York Times*, Facebook's new provisions "essentially give the company blanket permission to use the name, photo and other personal content of its users in advertising or sponsored content."[379] Also troubling, the changes permit Facebook to "automatically assumes that the parents of teenagers using the service have given permission for their names and images to be used in Facebook advertising."[380] And the changes document Facebook's aggressive expansion of its use of face recognition technology.[381]

As a result of continued reliance on third-party doctrine and the reasonable expectation of privacy standard, it has been unclear what, if any, protections our Fourth Amendment jurisprudence would afford an individual's Facebook activities from private industry via common law privacy protections and from government snooping. Court holdings are inconsistent.[382] In their concurrences in *United*

---

industry."

377. Schmitt & Stahl, *supra* note 369.

378. FED. TRADE COMM'N, *supra* note 192, at 78.

379. Vindu Goel & Edward Wyatt, *Facebook Privacy Change Is Subject of FTC Inquiry*, N.Y. TIMES, Sept. 11, 2013, at B1.

380. *Id.*

381. Steve Henn, *Facebook's Latest Privacy Changes: Tag, You're You*, NAT'L PUB. RADIO (Aug. 30, 2013, 4:03 PM), http://www.npr.org/blogs/alltechconsidered/2013/08/30/217281470/facebooks-latest-privacy-changes-tag-youre-you.

382. *Compare* United States v. Meregildo, 883 F.Supp.2d 523 (S.D.N.Y. 2012)

*States v. Jones*, we see Justices Alito and Sotomayor grapple with this very problem.[383] But a recent Ninth Circuit ruling demonstrates that some courts are unwilling to accept private industry's arguments that their data collection, use and sale activities are not constrained in some fashion. In this recent case, it is alleged that Google's "Street View" mapping vehicles, in addition to taking photographs, "secretly collected e-mail, passwords, images and other personal information from unencrypted home computer networks."[384]

Google's activities led to a handful of lawsuits by U.S. citizens who argued that Google had violated their privacy and had engaged in illegal wiretapping. These cases were ultimately consolidated in *Joffe v. Google*.[385] At trial, Google moved to dismiss, arguing that the Wi-Fi communications its Street View vehicles captured were "readily accessible to the general public," and therefore the Wiretap Act's exemption for electronic communication that "is readily accessible to the general public" exempted Google's activities and required dismissal.[386] The federal district trial court rejected Google's argument, permitting plaintiffs to proceed. Google appealed to the Ninth Circuit and on September 10, 2013, a Ninth Circuit panel held that the Wi-Fi network data collected by Google was not a "radio communication" under the Wiretap Act, and thus was not by definition readily accessible to the general public.[387] The panel also held that data transmitted over a Wi-Fi network is not readily accessible to the general public under the ordinary meaning of the phrase as it is used in Section 2511(2)(g)(i) of the Wiretap Act.[388]

Challenges to Google's data collection practices have not ended

---

(denying defendant's motion to suppress evidence obtained when cooberating witness showed police defendant's Facebook profile because, although he believed law enforcement would not have access, defendant "had no justifiable expectation that his 'friends' would keep his profile private") *with* Ehling v. Monmouth-Ocean Hosp. Service Corp., 872 F. Supp. 2d 369 (D.N.J. 2012) (finding that the plaintiff in the case "may" have a reasonable expectation of privacy in her Facebook posts based upon her privacy settings and that her employer's viewing of those posts may have constituted a common law invasion of privacy).

383. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (opining that in a "digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . information voluntarily disclosed to some member of the public for a limited purpose" may nevertheless be entitled to Fourth Amendment protection); *id.* at 962 (Alito, J., concurring) (noting that the expectation of privacy test "rests on the assumption that th[e] hypothetical reasonable person has a well-developed and stable set of privacy expectations[,] [b]ut that technology can change these expectations").

384. David Streitfeld, *Court Says Privacy Case Can Proceed vs. Google*, N.Y. TIMES, Sept. 11, 2013, at B1.

385. Joffee v. Google, Inc., No. 11-17483, 2013 WL 4793247 (9th Cir. Sept. 10, 2013).

386. *Id.* at 1081.

387. *Joffee*, 2013 WL 4793247, at *5.

388. *Id.*

with the Street View litigation. In the case of *In Re Google Inc. Gmail Litigation*, which involves allegations that Google's email practices violate the federal wiretap act and privacy laws, the United States District Court for the Southern District of California ruled on April 1, 2013, that Google's policies may violate the federal wiretap act.[389] Google routinely intercepts, reads, and acquires the contents of email users for advertising purposes.[390] A few months later, Judge Koh found this practice problematic.[391] "[T]he court finds that it cannot conclude that any party—Gmail users or non-Gmail users—has consented to Google's reading of e-mail for the purposes of creating user profiles or providing targeted advertising."[392] Judge Koh further stated, "Google has cited no case that stands for the proposition that users who send emails impliedly consent to interceptions and use of their communications by . . . other than the intended recipient of the email."[393]

## VII. CONCLUSION

As this Article has attempted to demonstrate, emerging technologies and a legislative void have combined to permit private industry to surreptitiously collect, retain, use, and sell staggering quantities of intimate, personal, individual data. Our constitutional and jurisprudential privacy protections and standards (e.g., the third-party doctrine and the reasonable expectation of privacy test) were developed long before the advent of the Internet and afford little functional protection from private industry's activities. In turn, the fact that the data has been collected and stored makes it far more easily accessible to government.

Unless and until legislation is passed that preserves and protects an individual's privacy in the same way from private industry *and* from government's ability to collect, retain, and use such information, our courts will continue to face legal conundrums, and all concepts of privacy will be functionally eroded. By regulating what data can be collected, how it can be collected, what can be done with it once it is collected, and permitting an individual the right to know what has been collected, and by applying these regulations equally to private industry and government, we can preserve our fundamental concepts of privacy. But doing so requires action. Congress . . . hello?

---

389. *In re* Google, Inc. Gmail Litigation, MDL No. 2430, 2013 WL 1400369, at *1 (J.P.M.L. 2013).

390. *Id.*

391. *In re* Google, Inc. Gmail Litigation, No. 12-MD-02430_LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013).

392. *Id.* at *13.

393. *Id.* at *14.