PRIVACY CRISIS: THE CURRENT AND FUTURE ISSUES OF RECEDING PRIVACY IN THE TWENTY-FIRST CENTURY

Matt Salcido†

Revised October 3, 2012 from a submission to Santa Clara University School of Law in support of my candidacy for a doctorate of jurisprudence.

Comments/edits welcome and encouraged.

E-mail: msalcido@soe.ucsc.edu

File location: http://alumni.soe.ucsc.edu/~msalcido/privacy

Abstract

Rapid technological change is having a drastic impact on individual privacy rights, both in cyberspace and in realspace. The law reacts slowly to these changes and various countries are taking different approaches to this now global concern. The first section of this paper offers a brief vision of the future and introduces some imminent technologies based on current research. It is followed by a primer on current privacy law and how this has developed in different countries over time. The last two sections discuss current proposals for changes to privacy laws and the legal and social issues of privacy in the twenty-first century. This paper departs from more traditional legal research essays in that it seeks a broad audience comprised of academics and non-academics alike. It seeks to clarify the “jargon” of high tech and explain “legalese” in such a way that professionals from both fields can focus on fashioning solutions, both technical and legal, to our impending privacy crisis.

† Matt Salcido attends Santa Clara University School of Law, where he expects to earn his Juris Doctor in 2013. In 2012, he received Santa Clara High Tech Law Institute's High Tech Excellence Award. He recently studied media policy and Internet regulation at the University of Oxford and holds a B.A. in Legal Studies from the University of California at Santa Cruz, where he also studied electrical engineering. In addition to law school, Mr. Salcido concurrently works full-time as an information technology professional in Silicon Valley, with over 15 years in the IT field.

Thanks are in order to Professor David D. Friedman of Santa Clara University School of Law who provided substantial comment on early drafts and guided the presentation format for the paper. Thanks also to Daniel Ryan Gray, J.D. candidate at the University of Tulsa College of Law, John Niman, J.D. candidate at the William S. Boyd School of Law, Steve Rodriguez, IT Manager for the City of Mountain View, California, and Carl Campos, enlightened luminary, for their thoughtful review and valuable feedback.
I. “Welcome to Cloister. Do you have reservations?”

“Winston, it’s time to wake up,” the thirty-something woman’s voice emanated from the ceiling, “failing to get up now could result in a 39% chance that you will miss your train.” Winston groaned. Somehow he pulled himself out of bed, repelling the strong urge to discount the computer’s calculations as bogus and sleep ten more minutes. He stumbled over to the bathroom and glanced into the mirror. “Time to wake up,” he echoed to his reflection, “the restaurant’s not going to run itself.” “That is correct,” replied the voice in the ceiling.

Winston turned on the faucet and let the water run for a split second before the backlit display embedded in the mirror revealed the current price of water (including the electricity required to pump it) and his current usage. He quickly shutoff the tap; if he wanted to tend his garden this year, he was going to have to save up. Then the mirror lit up with a display of Winston’s vitals. The data was collected by a swallowable capsule no bigger than a tablet of aspirin and containing a host of sensors that streamed real-time data on Winston’s pulse, blood pressure, cholesterol, blood glucose levels, etc. “OFF!” Winston commanded, causing the screen to fade to an advert for the hypertension drug “Rudisill™,” sponsors of the health-monitoring capsule. “Your blood pressure is higher than your doctor recommends,” LISA’s nagging voice informed him. (LISA stood for “Life Interface Systems Accessory” and was the acronym any device that allowed humans to access “the network”). “I’m a chef, what do you expect?” Winston snapped, before LISA cut
him off: “Thank you, however, the additional information does not change your prognosis.”

Winston’s workday began on his commute into the city. The train provided a secure high-speed linkup to the network; one simply placed one’s LISA into the headrest in front of him and pulled down the touchpad tray table. The screen came to life with several notifications. Winston always started by reviewing the analytics generated from last night’s business: profit margin up 0.2% over the day before, average time to get seated without reservations was 88 minutes and 16 seconds, et cetera. Customer sentiment analysis of the kitchen orders showed that, with a reasonable likelihood, 46% of customers selected their entrée based on the recommendations of others by way of a popular restaurant review app, 19% followed the advice of their nutritional advisor app, 18% showed no discernable pattern at all, 9% followed their financial advisor app, while only 8% chose the head chef’s recommendation. “I can’t believe an artificial intelligence accountant is beating me!” Winston thought, harboring a modicum of contempt for his customers. He did not take criticism well. So of course his next action was the most logical one: he checked the aggregated reviews, comments, and mentions from his customers’ network posts.

Predictably, that was a mistake. While many reviews were quite flattering, Winston focused on the criticism from a few scathing rants. His pulse elevated and LISA, sensing the increase in blood pressure, triggered an app aimed at distracting and relaxing the user. “Just because it’s instant, doesn’t mean it’s urgent!” the app interrupted, obscuring the screen with a video of a kitten “hunting” a household
MaidBot. It was stupid, but it worked. Winston tapped the touchpad and queried his daughter’s location on an interactive map. The live video feed from her second grade classroom began to stream to his display. He smiled. “How cute, they’re learning about quantum mechanics,” he thought, “it’s so much simpler at that age.”

A new notification popped up on the screen; it was the app sponsored by his attorney. “You have 8 unread personnel activity reports – I advise that you review your employee’s activities to minimize your liability-” Winston’s index finger vehemently jabbed the “dismiss” button, using more force than necessary; he hated reviewing the cyberspace and realspace actions of his staff – many of whom were his friends. He knew he should, but it just felt… creepy.

A computerized voice interrupted his thoughts, “This train will be arriving six minutes ahead of schedule. We apologize for the inconvenience.” Winston’s fellow passengers groaned (one person swore) at the prospect of arriving early. A popular app that maximized life-workflow efficiency had become the staple of the modern multi-tasker and this early arrival meant that the task allocated for the train ride would have to be rushed, interrupted, postponed, and resumed (or neglected) – and some had great difficulty dealing with this emotionally.

At the station, Winston walked briskly over to the BaristaBot who had his cappuccino waiting for him (the BaristaBot knew of his early arrival, what he would order, and what account to charge it to; LISA had “made the arrangements”).

Winston put the cup up to his lips. He was disappointed to find that it was a bit tepid, but this was his own fault. Yesterday, he complained online after burning his
tongue on the scalding hot coffee and BaristaBot took it “personally,” responding to this recent input.

The taxi Winston took to work was fully automated. The inner city grid was controlled by a central traffic authority that evaluated each person’s destination and priority code and analyzed the city’s traffic loads to maximize efficiency and minimize travel time. Sure, you could drive yourself if you wanted to, but the fees for such a privilege were astronomical, and without AutoNav it was likely to take twice as long. Upon arriving at his stop, the doorman greeted him with a smile and proclaimed, “Sir, we need all the tenants to sign this new building privacy policy.” It popped up on Winston’s LISA for his review; the doorman’s vocalization of the issue seemed irrelevant and left Winston somewhat irked. “Thanks,” he replied dawning a sarcastic smirk, “I’ll read it in the elevator.” Cloister, Winston’s restaurant, was located on the 82nd floor so he had a few seconds to give it a once-over. He recognized many of the user-friendly icons which depicted various information classes and collection methods: the lines projecting from a stick-figure mouth stood for conversational surveillance, the camera lens signified video surveillance, the crosshairs represented his location within the building. . . . all standard stuff.

Winston, already bored with the legalese, skipped to all the way to the bottom and tapped, “I consent.”

Finally he arrived at Cloister, his baby. Winston served only the best gourmet cuisine; many of the recipes were his own and he personally sourced only the freshest ingredients. Despite its culinary excellence, the primary allure of his establishment was the “digital dead zone” he offered his patrons. He was one of the
only ones in the district with this license, passed onto him by his father. An old research facility, the dining room was surrounded by layers of copper mesh that acted as a giant Faraday cage and blocked out nearly all electromagnetic signals. It had been remodeled several times for aesthetics, but there always remained an exposed patch of worn-down copper near the door, which the clientele (mostly politicians, big-shot executives, fancy lawyers, celebrities, and the like) would superstitiously swipe on the way out for good luck. Upon entering, patrons were required to check their LISAs into the soundproof device check (like a coat check) where they could be protected from the tempting (or more accurately, addictive) compulsion of the owner to check it every five seconds. Within Cloister, having one’s LISA out during dinner was the height of bad manners. The result was a distraction-free dining experience where one could come to escape the barrage of instantaneous information and engage in the fine “lost” art of human-to-human conversation.

“Chef!” a voice shouted, interrupting his concentration, “the delivery of eggs is late again!” Winston shook his head, “It’s fine, they always get here in time.” It was time to get to work; lots of important clients coming in today to enjoy his delicious cuisine, escape the engulfing pestilence of modern gadjety, and engage in intimate, focused conversation uninterrupted by their LISAs
II. A Primer on Current Privacy Laws

Our world is rapidly becoming more information-rich. Increasingly, information about what we say, where we go, and what we do is more abundant in digital form. It is instantaneously available and presented in a comprehensible form thanks to machines that aggregate, digest and compile data about our lives and make statistical models of our behavior. We are inundated with information produced by millions of data-producing, data-sharing devices that were not part of the human experience one or two decades ago. In the coming decades we will certainly see even greater data collection, processing, and dissemination. We have entered the Era of Big Data. This paper explores some of the implications of this flood of information and how it affects individual privacy. Specifically, what are the current privacy laws, what laws are being proposed and what legal issues may we face in the future?

Today, individuals face various regional privacy regulations. A nation’s privacy scheme falls into one of two general categories of regimes: comprehensive or sectoral. Comprehensive privacy laws, also called omnibus laws, regulate protected data across broad contexts and across most industries. Private and public sector are sometimes regulated together as in the European Union, as opposed to the sectoral approach, taken by the United States which is more piecemeal; different regulations cover different contexts and industries. The public and private sectors are governed by different regulations and each state or territory has its own law.
For the most part, the states’ laws adopt the federal regulatory framework and often provide further protections to their citizen.

A. A Brief History of the Constitutional Right to Privacy in the U.S.

The Federal Constitution is the supreme law of the land in the United States and provides the basis for some basic rights to privacy. Though nowhere in the Constitution is an explicit right to privacy enumerated, the Bill of Rights has been interpreted to protect certain invasions into areas of people's lives traditionally considered to be private. For example, the First Amendment protects one's right to speak anonymously and the right to keep the identities of the groups with which one associates private. The Third Amendment protects against the quartering of troops in one's home. The Fourth Amendment protects against unreasonable search and seizure, while the Fifth Amendment provides for a privilege against self-incrimination in the context of a government inquiry. In the most general of summaries, the above Constitutional rights protect the freedom of speech, freedom of association, freedom from government intrusion of one's home, and protection against self-incrimination.

---

1 “This Constitution, and the Laws of the United States which shall be made in pursuance thereof... shall be the supreme law of the land....” U.S. Const. art. VI, § 2.
2 “[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.” Griswold v. Connecticut, 381 U.S. 479, 484 (1965).
3 “Congress shall make no law... abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble....” U.S. Const. amend. I.
4 “No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.” Id. at amend. III.
5 “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....” Id at amend. IV.
6 “No person... shall be compelled in any criminal case to be a witness against himself....” Id. at amend. V.
Over the years, the Supreme Court has wrestled with extending these rights to other areas of individuals' personal lives. The Court expanded the right to privacy in 1877 by declaring that sealed letters sent through the mail were protected by the Fourth Amendment. However, in 1928, the Court did not find the same right to privacy when it came to telephone conversations. The Court upheld wiretapping in *Olmstead v. United States*, but not before Justices Holmes and Brandeis weighed in on the matter. “I think it a less evil that some criminals should escape than that the government should play an ignoble part,” wrote Holmes. Justice Brandeis declared:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness . . . . They conferred, as against the government the right to be let alone – the most comprehensive of rights and the right most valued by civilized men . . . . Our government is the potent, omnipresent teacher. [I]t teaches the whole people by its example. If the government becomes a lawbreaker it breeds contempt for the law . . . .

*Olmstead* was eventually overruled in 1967. In *Katz v. United States*, the court embraced Brandeis' dissent in *Olmstead* and found that Fourth Amendment protections apply to wiretapping. The court has adopted the “reasonable expectation of privacy test,” laid out in Justice Harlan's concurring opinion, to

---

7 See, *Ex parte Jackson*, 96 U.S. 727 (1878) (reading sealed letters sent through the mail constituted an illegal search that was in violation of the Fourth Amendment).
9 *Id.*
10 *Id.* at 470.
11 *Id.* at 478, 485 (emphasis added).
13 *Id.* at 362.
determine if a search receives Fourth Amendment protection. To trigger the “reasonable expectation of privacy,” (1) one must exhibit an “actual (subjective) expectation of privacy” and (2) that expectation must “be one that society is prepared to recognize as ‘reasonable.’”

This “reasonable expectation of privacy” is one of the most important concepts in modern privacy law. Courts have found the expectation of privacy to be “reasonable” when one has a conversation over a telephone, seals a letter and places it in the mail, in one’s home, in one’s personal bags or containers, on one’s personal computer, and in one’s office desk at work.

Like any Constitutional “test”, several exceptions have been carved out as well. For example, no reasonable expectation of privacy exists on one’s work computer where the user has been notified that the use was subject to monitoring, when one dials a phone number, where one’s property, is visible from a public vantage point, or where one has revealed the information to a third party.

---

14 Id. at 361.
15 Id.
16 Id.
17 Jackson, 96 U.S. 727. Postcards, however, do not receive the same protection, as anyone can see the content in transit. The same goes for unencrypted e-mail (almost all e-mail is unencrypted).
20 See Turlock v. Freeh, 275 F.3d 391 (4th Cir. 2001).
22 See United States v. Angebine, 281 F.3d 1130 (10th Cir. 2002).
23 See Smith v. Maryland, 442 U.S. 735 (1979) (the numbers dialed do not contain the content of the communication and one assumes the risk that revealing information to a third party (the phone company) could result in the third party conveying it to another).
25 This is known as the “Third Party Doctrine.” United States v. Miller, 425 U.S. 435 (1976) (one does not have a reasonable expectation of privacy where one reveals records to a third party, for example revealing financial records to an accountant).
The Constitutional right to privacy has also been found to protect individuals from intrusion into their marital and reproductive lives. In *Griswold v. Connecticut*, Justice Douglas’ majority opinion found that “specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.” The 7-2 majority of the court found that a Connecticut law banning contraceptives invaded the “right to marital privacy.” In *Roe v. Wade*, the court upheld the legality of abortions, reasoning that one’s right to privacy included a “woman’s decision whether or not to terminate her pregnancy.” The court has also recognized a constitutional right to informational privacy. An “individual has [an] interest in avoiding disclosure of personal matters,” the court held in *Whalen v. Roe* in 1977.

### B. The States and the Privacy Torts

States have addressed privacy concerns as well. For example, the Constitution of California declares that “[a]ll people are by their nature free and independent and have inalienable rights... [and among these are] safety, happiness, and privacy.” States have enacted their own criminal laws to address social and economic ills of privacy violations such as “peeping Toms,” unconsented recording of nude images, and blackmail. All states in some form or another have incorporated into their tort laws the “right to be let alone” introduced in Justices

---

26 *Griswold*, 381 U.S. at 484.
27 *Id.* at 486.
Warren and Brandeis’ seminal Harvard Law Review Article, *The Right to Privacy*, published in 1890. Most states recognize causes of action that indirectly protect privacy like negligence, breach of confidentiality, intentional infliction of emotional distress, and defamation. Besides these, the tort of “invasion of privacy” provides four specific causes of action.

Invasion of privacy encompasses: (1) public disclosure of private facts, (2) intrusion upon seclusion, (3) the false light doctrine, and (4) appropriation of name or likeness. The first, a public disclosure of private facts, is a cause of action for disclosing a matter that is “highly offensive to a reasonable person” and is not of legitimate public concern. Where someone tries to limit what another is saying by claiming that it is private matter, a common theme of privacy law arises: the balancing of the speaker’s First Amendment freedom of speech, or in this case, freedom of the press, and the privacy of the individual. For this reason, courts have devised the “newsworthiness test” to protect First Amendment interests. Courts are split however, between the “leave it to the press approach” (giving deference to editorial boards), the “community customs approach” (giving deference to social standards, customs, and norms) and the “nexus approach” (which requires a nexus between the invasion of privacy and a legitimate public interest).

The tort of intrusion upon seclusion provides a cause of action against one who intrudes “upon the solitude or seclusion of another or his private affairs or

---

32 Restatement (Second) of Torts § 652D (1977).
concerns” if the intrusion is “highly offensive to a reasonable person.”\textsuperscript{34} To be actionable, the plaintiff must have a privacy interest and show that the intrusion was highly offensive. A “privacy interest” includes privacy against involuntary exposure in public,\textsuperscript{35} activities occurring within one’s home,\textsuperscript{36} and extensive harassment in public.\textsuperscript{37} Actions that have been found to be “highly offensive” include peeping through one’s windows,\textsuperscript{38} snooping through one’s mail,\textsuperscript{39} secretly recording conversations,\textsuperscript{40} and disclosing confidential medical data\textsuperscript{41}. One distinguishing factor of the intrusion upon seclusion tort is that the information disclosed does not have to be published or used in any way; it is enough that the breach of private information happened. For example, even though one does not have a reasonable expectation of privacy in public, overzealous surveillance can be actionable if it is unreasonably intrusive, like extensive public photography and video recording and using mechanical and electronic means to eavesdrop and record private conversations.\textsuperscript{42} Using false pretenses to enter one’s home and secretly record them is actionable as well.\textsuperscript{43}

The false light doctrine provides a cause of action for publicly disclosing information that places the victim in a false light that is highly offensive to a

\begin{itemize}
  \item[\textsuperscript{34}] Restatement (Second) of Torts § 652B (1977).
  \item[\textsuperscript{35}] See Daily Times Democrat v. Grahm, 162 So. 2d 474 (Ala. 1964).
  \item[\textsuperscript{36}] See Dietmann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971).
  \item[\textsuperscript{38}] See Pritchett v. Bd. of Comm’rs of Knox Couty, 85 N.E. 32 (N.D. Ga. 1951).
  \item[\textsuperscript{40}] See Fischer v. Hooper, 732 A. 2d 396 (1999).
  \item[\textsuperscript{42}] See Nader v. General Motors Corp., 255 N.E.2d 765 (N.Y. Ct. App 1970) (seeking information of a confidential nature through overzealous public surveillance violated Plaintiff’s privacy).
  \item[\textsuperscript{43}] See, Dietmann, 449 F.2d.
\end{itemize}
reasonable person.⁴⁴ Similar to cases of libel and slander, the interests of the victim must be balanced against the First Amendment rights of the speaker. The speaker’s right to free speech protects him from false light cases unless he speaks with reckless disregard for the truth or actual knowledge of falsehood.⁴⁵

The last of the common privacy torts involves the appropriation of a person’s name or likeness. The victim has a cause of action against one who appropriates “to his own use or benefit the name or likeness” of another.⁴⁶ This tort shares commonalities with the legal concept of the right of publicity, namely that famous people have a right to exploit their own image. Johnny Carson, the popular comedian and host of The Tonight Show from 1962 to 1992, was known for the oft-repeated tagline “Here’s Johnny!” During the height of his career, Mr. Carson was aghast to see his catchphrase used in a television commercial to introduce portable toilets. In the ensuing litigation, the Sixth Circuit Court of Appeals held that Mr. Carson had a right of publicity to this catchphrase and the defendant misappropriated it when they used it in their commercial.⁴⁷

C. Privacy in Cyberspace and the Role of the FTC

The major Supreme Court cases mentioned above firmly establish a Constitutional right to privacy, at least against the government. The constitutional right to privacy against state action, while it is there, is also nebulous, “emanating” from the “penumbras” of the Bill of Rights as applied through the Fourteenth

---

⁴⁴ Restatement (Second) of Torts § 652E (1977).
⁴⁶ Restatement (Second) of Torts § 652C (1977).
Amendment. For a citizen to have a private right of action against a non-state actor, she must turn to state tort law. The introductions of the tort theories above give individuals some measure of protection with regards to their privacy. One common theme in these legal theories presented thus far is that they deal primarily with privacy of the person in realspace: one's written communications, one's home, one's marital bedroom, one's body, one's self, etc. These cases also deal with traditional methods of communication such as postal mail and telephones and traditional forms of media including newsprint and television. To engage in a discussion of privacy in cyberspace, we must turn to a different body of law. Specifically, since data about us in digital form can circle the globe many times over in the blink of an eye, what protections does an individual have against irresponsible collection, processing, and use of that data? The most concise way to address this issue is through a combination of changes to technology, human behavior, and the law. Technology itself will provide a good measure of privacy. Examples of such technical protections include data encryption, a public key infrastructure, and randomized, anonymous e-mail and Internet proxy servers all of which make it uneconomically difficult to decrypt or trace sensitive information. The other part to this is human behavior; users of the technology must not compromise their own privacy, either by protecting their data with the technological tools at their disposal or by not disseminating it in the first place. The

48 "No State shall. . . deprive any person of life, liberty, or property, without due process of law. . . ." U.S. CONST. art. XIV, § 1. In the 20th Century, the Supreme Court began to incorporate almost all of the amendments of the Bill of Rights as applicable to the states by virtue of the due process clause of the Fourteenth Amendment. Prior to that, the Bill of Rights only applied to the federal government.
focus here will be on the law that governs individuals’ sensitive data in cyberspace. Of course this will make for a tedious discussion since most people revel in the fine print and abundant legalese when diligently reading through the privacy policies of the web services and gadgets they use every day.

In the U.S., consumer privacy law is largely a matter of federal administrative law adjudicated by the Federal Trade Commission or state law. Courts have been reluctant to apply traditional notions of contract or tort law to modern-day privacy violations. For example, tort law has not produced much precedence in privacy policy litigation, aside from cases where gross negligence is present.49

Suits for violations of a company's privacy policy have not been brought successfully under theories of contract either. In Dyer v. Northwest Airlines Corp., an airline gave passenger information, including names, addresses, and credit card numbers to the government without seeking the passengers’ permission.50 The court ruled that “broad statements of company policy [(the privacy policy)] do not generally give rise to contract claims.”51 Victims who bring privacy actions based on contract theory also have trouble establishing damages that flow from the breach of an alleged contract. JetBlue passengers whose personally identifiable information (PII) was released to the government could not recover because the court reasoned that this information did not have “any compensable value in the economy at

49 See, e.g., Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. 1995) (plaintiffs whose personally identifiable information was released lacked a cause of action for the torts of intrusion upon seclusion or appropriation of name or likeness) and Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975) (public disclosure of private facts claim unavailable without showing of mental shame or humiliation).
51 Id. at 1200.
Absent a formal contract, the legal doctrine of promissory estoppel could come into play, but when it comes to privacy policies, a lack of promises and a lack of damages mean consumers cannot avail themselves to protection under contract law.

Most states have consumer protection laws, almost all of which mirror the Federal Trade Commission Act of 1914. Federal Trade Commission (FTC) decisions have been used as guiding precedence in many state courts. Thus in the U.S., the FTC has been the leading enforcer of privacy law and considers an act or practice that “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or corporations” as “unfair or deceptive.” Unfair or deceptive trade practices include any act or omission that leads to false or misleading claims. In contrast to contract or tort claims, injury does not have to result; action can be brought against a company for simply engaging in a deceptive practice.

For example, in 2002 the FTC filed a complaint against Microsoft for making representations that its online “Passport” technology (like an online “wallet”) held personal information in a manner that was both secure and confidential. Microsoft further claimed that using their technology to make purchases online was more secure than the traditional method that did not utilize the digital “passport.” Additionally, Microsoft’s privacy policy stated that it did not collect information on

---

54 Id. § 45(n).
the websites users visited. It turned out, however, that all of these claims were untrue. The FTC settled with Microsoft, who agreed to implement a comprehensive security program, conduct third party audits, and to cease further misrepresentation.\textsuperscript{56}

That same year, the FTC entered into a consent decree with the pharmaceutical company Eli Lilly for one of its employee’s technical gaffes.\textsuperscript{57} The company, maker of the popular antidepressant Prozac, maintained an e-mail service to which people could subscribe in order to receive reminders to take their medication or refill their prescription. The employee sent an e-mail message to all 669 subscribers, but mistakenly put the e-mail addresses in the “To” field – allowing everyone receiving the notice to see the e-mail address of all subscribers.\textsuperscript{58} The FTC and several state attorneys general took issue with this and filed complaints. Like \textit{In re Microsoft}, Eli Lilly had to implement a comprehensive security policy that included an employee training program, conduct third-party audits, and refrain from further misrepresentation with regards to how it handles sensitive consumer data.\textsuperscript{59}

In response to the Microsoft and Eli Lilly cases, companies sought to reduce the risk of litigation posed by their privacy policies by tactfully removing any promises of security. The FTC responded by expanding the unfairness doctrine to include inadequate security of PII. Case in point, DSW, Inc., who made no promises

\textsuperscript{55} FTC File No. 012 3240, \textit{In the Matter of Microsoft Corp.} (2002).
\textsuperscript{56} Id.
\textsuperscript{57} FTC File No. 012 3214, \textit{In the Matter of Eli Lilly and Co.} (2002).
\textsuperscript{58} Id.
\textsuperscript{59} Id.
of security in their privacy policy, maintained an insecure wireless network, kept files with personal data long after there was a business need to do so, and operated their database using a default, commonly known password. Another action was taken against software company Gateway Learning for making retroactive changes to its privacy policy. Gateway’s online privacy policy stated that personal information was not shared with third parties without the user’s consent. Customers were also put on notice that Gateway could change the privacy policy at any time. After collecting PII from consumers, Gateway began renting out the data, including information about children under the age of thirteen, without seeking or obtaining customers’ consent. Two months later, Gateway changed its privacy policy to allow the data-sharing that had already occurred and notified customers, giving them a post office address where they could opt-out. Predictably, this drew the ire of the FTC, who entered into a consent decree with Gateway. Gateway was banned from further misrepresentation, was required to acquire affirmative (opt-in) consent before sharing data gathered under the old policy, was barred from applying materially different privacy policies retroactively unless it gained opt-in consent, and was disgorged of the profits from the sale of the personal data.

Other FTC enforcement actions have centered around the failure to disclose the extent of the data collection. Vision I Properties, LLC. licenses its software called “CartManager” to small businesses to provide online shopping and checkout services. The CartManager websites are designed to look like the merchants’ own

---

62 Id.
websites (though they are hosted by Vision I), so any reasonable customer would assume the privacy policies of the merchant still applied when they entered their credit card number, home address, etc.\textsuperscript{64} Vision I Properties maintained its own privacy policy, which did allow for the sharing of data. Since the merchants were largely unaware of Vision I’s practices it was only Vision I who faced sanctions from the FTC (otherwise the merchants would be liable under § 45 as well).\textsuperscript{65} Another e-commerce site, Toysmart.com, had filed for bankruptcy and planned to sell its customer database to satisfy its creditors which was in violation of its promise not to share customer information with third parties. The FTC intervened and agreed to let Toysmart.com sell the database only if the bankruptcy court approved the buyer and with express limits on how the buyer could use the information.\textsuperscript{66} In a more sneaky practice, ReverseAuction.com harvested customer information from a competitor, E-bay.com, and sent SPAM e-mails with a misleading and false notice: the users were told that their E-bay logins would expire soon and solicited their business.\textsuperscript{67} ReverseAuction.com was barred from making further representations and required to inform the notified customers of the falsehood of their e-mail.\textsuperscript{68}

Besides failing to disclose data collection to licensees and end-users, notification that is ineffective can be actionable as well. In 2009, Sears operated a website that opened a pop-up window which invited users to enter their e-mail

\textsuperscript{63} Id.
\textsuperscript{64} FTC File No. 042-3068, \textit{In the Matter of Vision I Properties, LLC} (2005).
\textsuperscript{65} Id.
\textsuperscript{68} Id.
address if they wanted to join a “dynamic and highly interactive on-line community. . . where your voice is heard and your opinion matters, and what you want and need counts!” A follow up e-mail described a program where users got paid to download software to their computers that would track their Internet browsing, usage, and history. Despite a lengthy end user license agreement that detailed the extensiveness of the tracking, the FTC found that Sears engaged in a deceptive practice. Not only did the software track traffic to Sears and related-merchants’ websites, but it tracked all Internet traffic, plus e-mail headers and offline computer usage data as well. Sears settled with the FTC, agreeing to destroy all data collected under the program and to clearly disclose the scope of tracking separately from the license agreement.

D. More on the Sectoral Approach in the U.S.

As one can discern from the FTC files above, online consumer privacy is primarily regulated by the Federal Trade Commission Act. Obviously, congress has passed other laws that regulate privacy in different sectors and industries. To delve into great detail here would go beyond the scope of this paper and would, in all likelihood, have a sleep-inducing effect of the reader. Instead, here are some illustrations of such legislation:

- The Children’s Online Privacy Act limits a website’s use of data gathered from children under thirteen years of age.

---

70 Id.
• The Privacy Act of 1974 provides individuals with the right to access and verify the accuracy of records concerning personal information kept by the federal government.\textsuperscript{72}

• The Fair Credit Reporting Act limits the use of personal data by credit reporting agencies and entitles consumers to obtain a free credit report every year so they can verify its accuracy.\textsuperscript{73}

• The Gramm-Leach-Bliley Act is why banks always include those privacy and marketing opt-out notices in their credit card statements.\textsuperscript{74}

One sector that is receiving more attention at present is healthcare. Much more data on individuals’ health, medical history, and genetic composition will be available in digital form very soon. A great deal of health data is already online. The primary law governing this data is the Health Insurance Portability and Accountability Act (HIPAA). Passed in 1996, HIPAA authorizes the Department of Health and Human Services to promulgate regulations regarding the handling of health information.\textsuperscript{75} The two major privacy tenets of these regulations are the Privacy Rule and the Security Rule. The Privacy Rule requires patient authorization for all disclosures of patient data beyond what is needed for “treatment, payment, and health care operations activities.”\textsuperscript{76} Health care operations include a broad range of activities including case management, quality and competency assurance,

\textsuperscript{72} 5 U.S.C. § 552a (amended 2010).
\textsuperscript{74} 15 U.S.C. §§ 6801-6809 (amended 2010).
\textsuperscript{75} 45 C.F.R. §§ 160-164 (amended 2010).
audits, legal reviews, insurance underwriting, health plan performance evaluations, and “de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.” 77 It also requires patient authorization for third party marketing and provides patients with the right to access their data and request restrictions. The Security Rule only applies to electronic data and requires covered entities to “protect against reasonably anticipated threats or hazards to the security and integrity of [the data.]” 78 The rule also compels organizations to designate a security officer, institute security procedures, and train personnel accordingly. HIPAA only applies to “covered entities” which include “health plans, healthcare clearinghouses and healthcare providers” and their business associates. 79 Business associates perform “certain functions or activities on behalf of, or provide[] certain services to, a covered entity that involve the use or disclosure of individually identifiable health information” and contractually agree to the safeguards set forth in the rule. 80

Although states often have tougher laws, HIPAA has set a national baseline which provides some level of protection. De-identified data (data that supposedly cannot be traced back to the individual) does not fall under these restrictions and can be distributed freely. HIPAA also does not provide a private right of action; the regulations are enforced by the Department of Justice (for criminal violations) or the Department of Health and Human Services, Office of Civil Rights (for civil actions).

77 Id.
78 45 C.F.R. §§ 164-306 (a).
79 45 C.F.R. § 160.120.
E. International Privacy Law

Outside the U.S., attempts have been made to protect the privacy interests of individuals at the international level. In 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights, which set forth wonderfully idealistic, albeit non-binding, principles. Among these are the principle that “all people are born free and equal in dignity and rights.” Everyone “has a right to life, liberty, and security of person.” “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondences, nor to attacks of his honor or reputation.” It is no mistake that this sounds like an embodiment of the legal principles laid out above. Even the freedom of speech is addressed: “Everyone has a right to freedom of opinion and expression [including] … the right to hold opinions without interference and to seek, receive, and impart information and ideas through any media regardless of frontiers.”

In 1980, the Organization for Economic Co-operation and Development (OECD) approved guidelines that established the eight main principles in modern privacy law. First, data is to be collected lawfully and with the consent of individuals. Second, the notion of “data quality” was introduced: data should be relevant to a particular purpose and it should be accurate. Next, the purpose must be specified for collecting the data, stated at the time of collection, and use of the

---

80 *Summary Of The HIPAA Privacy Rule, supra* note 76, at 3.
81 *Universal Declaration of Human Rights, G.A. Res. 217A (Dec. 10, 1948).*
82 *Id.* art. 1.
83 *Id.* art. 3.
84 *Id.* art. 12.
85 *Id.* art. 19.
data should be limited to the stated purpose. Fourth, the data must be kept secure, using all reasonable protections. Fifth, individuals must be informed about the practices and policies of those handling their personal information. Likewise, those individuals should be entitled to access to the data about them and provided an opportunity to correct inaccuracies. Lastly, the concept of accountability came into play; she who controls the data should be held responsible for following these guidelines.

The OECD guidelines gave rise to some significant pieces of national legislation that attempted to incorporate these principles. Australia, New Zealand, and South Korea passed laws that reflected the OECD agreement. In the U.S., Congress passed the Cable Communications Policy Act of 1984, which provides safeguards for customers’ data, based on these principles. The Asia Pacific Economic Cooperation (APEC) guidelines of 2004 mirrored the OECD recommendations; however the APEC guidelines are advisory only and not binding on signatories.

A decade after the OECD guidelines, in 1990, the U.N. General Assembly passed the Guidelines for the Regulation of Computerized Personal Files. These reiterated the OECD principles above and added the principle of non-discrimination. The principle of non-discrimination states that data must not be compiled if it is likely to cause unlawful or arbitrary discrimination. The regulation lists specifically, data on “racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade
union.”86 This resolution carves out exceptions to protect “national security, public order, public health, or morality, as well as inter alia, the rights and freedoms of others.”87 It also requires countries to designate an authority to supervise compliance. Recognizing the increasing volume and need for data flowing across borders, the principle was set forth that data should move freely between two countries that offer comparable legislative safeguards to protect privacy. It further stipulated that “[i]n the absence of ‘reciprocal safeguards,’ a country may not restrict circulation of information ‘unduly’ and may do so ‘only in so far as the protection of privacy demands.’”88

To deal with the problem of data sharing across borders, the European Union enacted the E.U. Data Protection Directive (hereinafter referred to as the Directive).89 As the demand for data sharing increased, individual countries enacted divergent regulations with regards to the handling of data. The Directive sought to harmonize legislation between member states by setting out the common principles that would protect personal data. It required countries to enact legislation pursuant to the privacy principles, but left the drafting of the language of the actual laws to the individual legislative bodies in each country. While the Directive promised to enable the free flow of data across borders, companies and individuals still must navigate a myriad of different national regulatory regimes, statutes, and court opinions.

87 Id.
88 Id.
Article 7 of the Directive sets out the conditions under which data processing is legitimate. “Data processing” includes almost anything involving personal data including collection, use, disclosure, storage, retrieval, erasure, or posting it online.\(^90\) First, the processing of data is only acceptable if the person to whom the data pertains (known as a “data subject” under the Directive) has given their consent. Besides consent, other conditions that qualify data processing as legitimate include satisfying a contract, carrying out a task in the public interest, or protecting a vital interest of the data subject. Data can also be processed if the keeper/processor of the data (known as a “data controller”) is required to meet a legal obligation or fulfill some legitimate interest for itself or a third party, “except where such interests are overridden by the interests for fundamental rights and freedoms of the data subjects which require protection under Article 1 (1).”\(^91\)

Article 8 designates special protection for sensitive data categories similar to the ones set forth in the U.N. guidelines for computerized personal files\(^92\) including racial and ethnic data, religious or philosophical beliefs, health and sex life, etc.\(^93\) Member states may make exceptions to the special categories when in the “substantial public interest.”\(^94\) Data controllers must provide notice when collecting data\(^95\) and the data subject has the right to access and correct data about her.\(^96\) Data controllers must also ensure an “[a]ppropriate technical and organizational

\(^{90}\) Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12992.
\(^{92}\) G.A. res. 44/132 Supra note 73.
\(^{93}\) Id. art. 8.
\(^{94}\) Id.
\(^{95}\) See Id. arts. 10-11.
\(^{96}\) Id. art. 12.
measure” of data security. If the controller fails to comply with the directive, Data subjects have the right to erase or block the data in noncompliance.

The Directive provides for judicial remedies and compels data controllers to compensate people if they suffer damages “as a result of any act incompatible with the national provisions adopted pursuant to this directive.” To supervise the adherence to the principles of the Directive, each country established independent national data protection authorities. Each member state also sent a representative to the Working Party on the Protection of Individuals with Regards to the Processing of Personal Data (Working Group) established by Article 29. The Working Group is an independent advisory body charged with providing expert opinion and recommendations for carrying out the Directive.

To handle the transfer of data outside the E.U., the Directive specifies that personal data may only be disseminated to organizations that provide an “adequate level of security.” “Adequacy” is to be assessed “in light of all the circumstances surrounding a data transfer operation or set of data transfer operations.” The Working Group has determined that the “current patchwork of narrowly focused sectoral laws and voluntary self-regulation in the U.S. is not adequate.” As a result of this finding, the E.U. and the U.S. Department of Commerce negotiated a Safe Harbor Agreement in 2000. The agreement sets standards that organizations wishing to share data with E.U. countries must follow. These include notice, choice

---

97 Id. art 17.
98 Id. art 22.
99 Id. art. 23.
100 Id. art. 25 (1).
101 Id. art. 25 (2).
102 Art. 29 Working Group, Opinion 1/99.
(opt-in/opt-out), security, relevancy, accuracy, access, guarantee of protections upon transfer to third parties, and enforcement. To date, only seven countries including the U.S. have been “whitelisted” by the Working Group.

Shifting to the other side of the globe, some Latin American countries have embraced a unique legal concept centering on individual privacy. “Habeas data,” which translates roughly to “[we command you] have the data” is a judicial remedy and an individual complaint before a constitutional court. It permits a person to know the content and purpose of data pertaining to him in public records and, sometimes, in private ones. The concept was introduced in Brazil’s 1988 Constitution. The right can also be found in Argentina’s Constitution, where a person has a right to “obtain information on the data about himself and their purpose” in public or private records104 and Mexico’s Federal Data Protection Act of 2010.

---

103 Article 5 explicitly protects privacy and contains a constitutional right to habeas data. C.F. art. 5 (Brazil 1988)
104 Argentina Const. art. 43.
III. Privacy Laws of the Near Future: Proposed Changes

It takes no expert analysis to recognize that the rate of technological change far outpaces the changes in the law to account for it. This is not a new problem and, as some legal scholars would proffer, it is not a problem at all – changes in law should be deliberate and not made in haste. Privacy law is rapidly changing because of our increasingly digitized world. Here is a synopsis of some recently proposed laws and regulations that would affect the way we interact with our data – and with each other.

In the year 2015, the number of smartphone and tablet app downloads could reach 182 billion. In February of 2012, California Attorney General Kamala Harris met with the six largest web app providers to agree on standards for displaying data use information and privacy options. Consumers should see “prominent and easy-to-understand privacy disclosures” to which they explicitly consent before downloading and using the app. The aim of the meeting with Google, Apple, Hewlett-Packard, Microsoft, Amazon, and Research in Motion (maker of BlackBerry devices) was to propose standards to clarify California’s existing Online Privacy Protection Act of 2003, which applies to app developers and distributors. Together the six companies distribute about 95% of apps downloaded by consumers onto mobile devices. Since many of the companies are based in

---

106 Id.
108 Swift, Supra note 92.
California and the state is home to a large number of app customers, Attorney General Harris predicts this agreement will have a global impact.\textsuperscript{109}

When it comes to online privacy, the Federal Government is taking a more central role. In March of 2012 the FTC released a report recommending a framework that would give consumers better control over what information is collected about them online and rights to access the data held by data brokers.\textsuperscript{110} One such issue raised was the tracking that web browsers do on user activity without users’ knowledge. The online service industry has “grown up around the collection and sale of information about people’s online interests.”\textsuperscript{111} The companies say the information collected is what allows them to provide users with free services such as e-mail, social networking, and the like. Federal regulators and some politician would like to see a one-click check box that would enable a “Do Not Track” feature on any web browser.\textsuperscript{112} There is some debate on whether the law should prevent the collection of all data, even when anonymous, or simply restrict targeted advertising.

The FTC report also focused on making it easier for consumers to access data relating to them. A possible step would be for congress to enact a law creating a centralized website where data brokers would have to report what information they collect and what they are doing with that information.\textsuperscript{113} Consumers would have rights to access data being collected about them and see what choices they had with

\textsuperscript{109} Id.  
\textsuperscript{111} Mike Swift, ‘Do Not Track’ for Web browsers debated, San Jose Mercury News, Apr. 12, 2012 at D1.  
\textsuperscript{112} Id.  
\textsuperscript{113} Mike Swift, Feds lay down privacy rules for Web giants, San Jose Mercury News, Mar. 27, 2012 at A1.
respect to that data. The FTC is not alone in seeking legislative action to protect privacy – The White House is planning to send a “Consumer Privacy Bill of Rights” to Congress that embodies many of the principles discussed above.\textsuperscript{114}

Perhaps the biggest change under consideration was proposed in Europe in early 2012. Vivien Reding, Vice-President of the European Commission, has proposed a new privacy regulation to replace the current directive.\textsuperscript{115} Since the Treaty of Lisbon in 2009, European leaders are taking a new look at E.U. institutions and authority is being consolidated into a more federal structure. The old privacy directive would be replaced by a privacy regulation, the difference being that the regulation is adopted as-is and is directly binding on member states. Europe would have one central data protection authority (DPA) instead of a national authority in each member state, although presumably each country would keep a national office under the auspices of the central DPA. Notification and accountability are brought to the forefront under this framework. The DPA would also play a more direct role in enforcing adherence to the privacy regulations. For example, if a data breach occurs, the data controller must notify the local data protection authority within 24 hours, if possible.\textsuperscript{116} The DPA will perform audits and hold companies accountable with proposed fines of up to 2% of worldwide revenue.\textsuperscript{117} Two new rights are created as well. The “right to be forgotten” (from the French “right to oblivion”)

\textsuperscript{114} Larry Magid, \textit{Online privacy rights get needed protection}, San Jose Mercury News, Feb. 27, 2012 at D1.
\textsuperscript{116} \textit{Id.}
\textsuperscript{117} \textit{Id.}
would give people the right to remove content they posted and now want deleted.¹¹⁸

The “right to data portability” gives one the right to take down all their data off of one website and move it to another (e.g. move their data from Facebook to Google+, competing but similar social networking systems).¹¹⁹ Companies also would have to implement “privacy by design” when bringing a product or service to market by building-in and enabling privacy protections and “privacy by default” whereby the default setting of a data-sharing device, website, etc. is to share the least amount of data with others, even though the consumer might opt to share her data to a broader audience.¹²⁰

---

¹¹⁸ Id. It is yet to be seen how such a scheme would work, either legally or technically. Legally, if I post a picture of myself on Facebook, I should have the right to take it down. But what if my friend (or enemy) downloads my picture, alters it or includes it in another post, and now I want her content (in which I am the subject) removed. Does not she have a free speech right to post it, at the very least in a journalistic capacity? Technologically speaking, the servers hosting services like Facebook are located all over the world and the picture will have been replicated to several countries (this is how large Internet companies achieve high-availability and redundancy to prevent outages) and probably backed up onto some backup storage media hidden away in yet another location. The thought that I could leverage the law to delete every instance of that image everywhere is, technically speaking, balderdash. As for servers hosting files in countries outside the jurisdiction of the E.U., well, it’s worth remembering that electric signals cross borders freely, bypassing customs and immigration.

¹¹⁹ Id.

¹²⁰ Id.
IV. Privacy Issues in the Twenty-First Century

By the end of the century the word will undoubtedly be very different. Technological change will shape individuals and cultures in new ways, providing new opportunities and presenting new challenges. We humans constantly build new technology only to be fundamentally changed by it. “No generation seems to behave precisely like the former generation. Rates of change, comparing one people with another or one aspect of culture with another, show great differences, but the outstanding fact of constant change nevertheless remains.”¹²¹ Vast new sources of data will produce mountains of information on scales never before imagined. As computers become faster, more powerful, and data storage becomes cheaper, the question of how we analyze the information becomes more poignant. We will have the data; what will we do with it? How will our concepts of privacy change in such a world?

Evidence suggests that the human population is shifting away from the rural environments where we have always lived and concentrating in cities; more than half of the world’s population already does so.¹²² The support systems of cities will need to become much more interconnected to maximize efficiency of scarce resources. The infrastructure of the city itself will include systems to gather and share information in various ways. This includes the increased use of sensors,

tracking devices\textsuperscript{123}, real-time intercommunication, and smart machine-to-machine (M2M) data sharing. The obvious fears of a "Big Brother" type society aside, the possibility will exist for data to be aggregated and computer modeling to be used to deduce certain facts about a person. Innocent collections of thousands of data points could be combined to paint a picture of a person's activity without their knowledge.

To illustrate this concept, imagine a gentleman living in his apartment in the future. Vibration sensors indicate he walked into the kitchen. The energy consumed on the stove suggests that the occupant boiled the 2.3 liters of water (measured as it flowed from the tap). There is a 56\% chance that this was to make spaghetti (the RFID-tagged kitchen inventory contained all the necessary ingredients) and there was a 90\% chance a bottle of red wine would be opened (the gentleman always had wine with dinner – his purchasing habits gave him away). Any one of these sources of data would not lead to the conclusion that the gentleman was preparing food (at least not with any reasonable certainty). Taken in aggregate however, the many sources of data combine and provide new dataset that suggests with a reasonable amount of certainty that the gentleman is making dinner. There is nothing necessarily private about making dinner, other than the fact that the activity is being performed inside one's home, but combined with more input (a room with more than one human-equivalent heat source could indicate that a he was not alone, the ratio of carbon dioxide to oxygen could indicate heavier

\textsuperscript{123} In 2010 it was estimated that there is already 5 radio frequency identification (RFID) tags for every human on the planet – more than 33 billion. Susanne Dirks, Mary Keeling, & Jacob Dencik, \textit{How Smart is your city?}, 1, (2009).
respiratory activity, and increased activity on the vibration sensors...) and now the dataset suggest a different possible conclusion. Like the paparazzi’s snapshots of old, this digital dataset could be sold to an online tabloid, which could blast the headline, “Governor has affair! Data ‘practically certain!’” Datasets like this could be much more valuable than scandalous photos because they contain much more information. Data collection of this type may violate future privacy torts, statutes that were almost assuredly passed to prevent such collection, and possibly the Fourth Amendment.

More traditional forms of surveillance and tracking are sure to keep track of our every movement in public. Cameras are presently in abundant use in public and private establishments such as office buildings, parking garages, schools, and retail establishments. Suppose that cameras are as ubiquitous as streetlights, made possible by their low cost and software that processes the huge amount of data generated from them. Facial recognition software could identify hundreds of individuals in a thousandth of a second and deduce their activities.124 Humans would generally not bother watching the video feed – most of the time people are boring in public. But when the software detects the face of a woman wanted by police or captures the image of a handbag being separated from its owner (and the

body language of the actors suggests it was involuntary) the authorities would be notified.\textsuperscript{125}

Geolocational tracking will be even more ubiquitous than it is now. With smartphones that track our geographical location by way of three separate technologies, will our physical security be jeopardized by the public nature of this data?\textsuperscript{126} The law may change to provide people with greater geolocational privacy in the future, but at present this protection is very weak.\textsuperscript{127} What’s interesting about our location is that it is an aspect of our privacy that is not strictly private. Anyone in public can see where we are, however the odds are that we do not care if a small number of random people know this information. It is from those who would harm us that we seek to keep things private or when the only harm done would be to our reputation (\textit{i.e.}, visiting or just passing through a location that is less-than-reputable). How public do we want our “public” locations? Might people in the future care less about their physical privacy and more about online privacy or vice versa? It is difficult to argue that one had a reasonable expectation to privacy when one posts one’s location on a social networking website for the world to see as millions of users do every day with services like Facebook, Twitter, and Foursquare.

\begin{footnotesize}
\textsuperscript{125} An example of this is the new public safety surveillance system in Chicago that allows “faster more effective response times to emergencies.” Susanne Dirks & Mary Keeling, \textit{A vision of smarter cities}, 11 (2009).

\textsuperscript{126} Current mobile phone and GPS device technology is highly insecure. In a recent case study, a journalist exploited vulnerabilities in a mobile phone and in a vehicle security module and proved “that an attacker could easily issue commands to the target module, bypassing authentication and authorization.” Don A. Bailey, \textit{Moving 2 Mishap: M2M’s Impact of Privacy and Safety}, IEEE Security & Privacy, Jan./Feb. 2012, at 84.

\textsuperscript{127} See, \textit{e.g.}, Kaonzinski, \textit{infra} note 116 and United States v. Jones, 10-1259 (01/23/2012) (electronic tracking of vehicle may be Constitutional if it does not involve physical trespass) So, essentially, the police can call the mobile phone company or car company and get your location, \textit{without a warrant or even probable cause.}
\end{footnotesize}
This brings us to the biggest question of privacy in the future: what will a “reasonable” expectation of privacy look like? The test as it stands today asks whether or not the individual thought she had a reasonable expectation to privacy and whether or not society is willing to accept the expectation as “reasonable.” In the case above, the person who posted their location on the social networking website could not have reasonably expected to keep that information private. (In reality, a vast number of people are woefully uninformed about the ramifications of their online activities, but for the sake of this argument, assume that the individual is informed of the risks and posts their location anyway. But if this becomes common practice and enough people are posting their location online for the world to see, does not that suggest that this is a privacy interest that society no longer reasonably expects to have? If that happens, then your location could not be considered to be private, even if as an individual one wanted to keep it from the public eye.

If one looks at the technological and cultural transformation that has transpired since Katz, one can see this trend manifested in palpable detail. Katz had a reasonable expectation of privacy for his telephone conversation... *that took place in a phone booth, with the door closed, in 1967*. The mobile phone has completely changed that. Today, people walk around in public and speak at annoyingly high

---

128 A was a recent app scandal involving an app for smartphones that linked the poster’s location and time of post with images of them and their Facebook profile. The result was an “outcry” from consumers who called the display of public data “creepy.” The app, called Girls Around Me, would display anyone who was nearby (of any gender) and allow the user to browse the proximal person’s Facebook profile. All this app did was aggregate and display data that Facebook users had *already voluntarily made public*. The “outcry” caused Google and Apple to pull the app from their respective online marketplaces and goes to show the lack of understanding about privacy in the age of Big Data. Amy Hubbard, *iPhone app pulled after ‘creepy’ debate*, San Jose Mercury News, Apr. 5, 2012 at D4.
volumes, without regard for the proximity of their fellow citizens. The technology of voice communications has changed, evolving from the antiquated notion of phones being tied to fixed locations to the expectation that one has their mobile communicator on their person wherever they are at all times. When it comes to telecommunications, the expectation of privacy has considerably weakened. There are many reasons for this, including the decreasing cost of making phone calls, the introduction of e-mail, text messaging, and the integration of web-based technologies into smartphones. “Twenty years ago [determining your location via your mobile phone] would have been considered private; you would have needed a warrant,” opined Judge Kaonzinski at a Stanford University privacy symposium in 2012.129 This is not the case today.

In order to manage the privacy protections of the future, we will need to classify types of data based on content. At first glance, the sectoral approach taken by the U.S. seems to achieve this: health data protected by HIPAA, financial data protected by Gramm-Leach-Bliley, etc.... Dig deeper however, and the protections only go so far. For example, HIPAA security rules only apply to electronic files controlled by “covered entities.” Our personal data still is personal, even if it finds its way to a non-HIPAA-covered entity. Another issue we will have to face in the future is that through our classifying different types of data and assigning protections to them, we must also be careful about the value judgments that naturally attach to those classifications.

As an illustration of this, because we place such a high value on the privacy of our health data we have passed correspondingly strong privacy laws not found in other areas of the economy. In the future, technology will produce (and is already producing) a “tsunami of data” about the inner workings of our bodies. Soon, we will be able to swallow a pill that contains instrumentation to collect all sorts of data on the inner workings of our bodies. But here, privacy has a dark detrimental downside. Medical researchers are at a grave disadvantage because they have to transgress miles of red tape in order to gain access to datasets – including in some cases, seeking and obtaining opt-in consent for every single patient who has data in the database. As one can imagine, this can take years and is extremely expensive. In the meantime, people are suffering and dying. In the future, we must determine how to strike a balance between protecting privacy interests and allowing necessary medical and genetic research to proceed unhindered. Perhaps, one day, we will judge a datum not by the classification of its controller, but by the content of its bits.

---

130 One reason to do this is ensure that health insurance companies do not deny coverage or raise premiums for those with preexisting conditions. However, if the patients have this information and the insurance companies do not, then the higher-risk people will be the ones taking out insurance policies and rates will go up anyway because of increased utilization and the fewer number of healthy payers. In theory, to prevent this adverse selection from happening, you would need to prevent insurance companies from setting rates based on preexisting conditions and require everyone to have health insurance to defer the costs. This is one of the goals of the Patient Protection and Affordable Care Act of 2010.
133 Frustration with the slow progress of medical research has led some parties to take matters into their own hands. The website http://www.patientslikeme.com/ was founded by frustrated sufferers and is a social networking site (of sorts) where patients can upload as much data as they wish into a dataset for their particular medical condition. Interestingly, the dataset starts out being public until it reaches a critical threshold and then access is cut off. The dataset now has value in the marketplace and can attract the needed researchers. David Winickoff, Professor of Bioethics and Society, University of California, Berkley, Remarks at the University of California, Santa Cruz conference: Are You My Data? (May 8, 2012).
Defining privacy and classifying what information we keep private is no simple task.\textsuperscript{134} I put the question of defining privacy to three fascinating individuals in order to get a unique perspective on the issue. The first was an “Internet censor” who works at a Silicon Valley Internet company and spoke on the condition of anonymity (all the interviewees did – to protect their privacy). His job is to review content that has been flagged as “inappropriate” by users of a website and decide whether it violates the company’s privacy policy. If it does, he removes it. When asked if he ever takes into consideration the content-poster’s free speech rights in deciding to remove content, he responded, “That is a big issue... but it’s not my job [to set the policy].” He “just implements it.” What an awesome responsibility he had in making this decision on the thousands of complaints he reviews every week. Monotonously mechanical, one could see this job being replaced by software in the future – software that would be making decisions affecting the legal rights of others.\textsuperscript{135}

Next, an Iraqi émigré shared his thoughts on the importance of privacy and free speech. “Under Saddam [Hussein], there was no Internet access,” he recalled. If you wanted e-mail, you took your computer to a government office, where they installed the modem. And then, all you got was e-mail access – no Internet. “It took two days just to send an e-mail that said ‘Hi, how’s it going?’” The government “read


\textsuperscript{135} Is it preferable to have a human review such decisions as opposed to having them be automated? Human review is expensive and biased. Machine review, if the technology is good enough, would weigh all the available data and make an instantaneous, unbiased decision... But is it really unbiased? Who writes the algorithm? Humans.
every e-mail and rejected it if they didn't like it.” Privacy is vital to free speech.\(^{136}\)

Now, he lives in the U.S. and is an active Facebook user; at least now he feels like he has more control over those aspects of his private life that he releases into cyberspace, and that makes all the difference. Instead of being monitored by government mandate, he provides the information voluntarily and therefore feels in “control” of the content. In the future, online surveillance will be vitally important to governments wishing to keep tabs on people. Already, the governments of the United States and the United Kingdom are ramping up their legal and technical abilities to monitor their citizens.\(^{137}\)

Lastly, I conversed with someone who used to forgo physical privacy voluntarily: a former stripper whom I will call Chastity. I explained to Chastity the concept of *Katz*: that Katz had a “reasonable expectation of privacy” when he closed the door to the phone booth. With a sharp wit, Chastity replied, “Yeah, but Clark Kent changed into Superman in a phone booth – *and it’s all glass!*” I had never thought about that before. Privacy of your body “is all a matter of if you’re comfortable with [it],” Chastity opined, “privacy of a conversation is personal, it’s emotional. . . it’s on the whole other side of the spectrum.” Just because one chooses

\(^{136}\) *See also*, Jamilah King, *Activists Worry That Mobile Phones Could Do More Harm Than Good*, Colorlines.com, March 6, 2012, [http://colorlines.com/archives/2012/03/verizon_vodafone.html?ak_proof=1](http://colorlines.com/archives/2012/03/verizon_vodafone.html?ak_proof=1). (cell phone company compelled by former Egyptian President Mubarak to turn over information on protesters, who used their mobile phones to send photos and texts of anti-government demonstrations, which resulted in arrests and convictions).

\(^{137}\) The U.K. government has proposed a nationwide system of electronic surveillance to track “any message [phone and e-mail] sent to anyone at any time [and] . . . every post and every tweet.” Ralph Satter, *UK government reportedly planning surveillance program*, San Jose Mercury News, Apr. 2, 2012 at A8. In the U.S., officials are taking a more clandestine approach. The Obama administration has “relaxed” the length of time data gathered on citizens can be “retrieve[d], store[ed], and search[ed]” for “purposes other than national security.” The “relaxed restrictions” allow data (that previously
to forego privacy in one sphere of their life does not mean they are willing to give up privacy in other spheres of life. The context is important, too. It would have been a violation of privacy if the nudity were involuntary. Given that the Supreme Court has recently ruled that strip searches are allowable for any offense, no matter how minor, what will our concept of privacy of the body be in the future?\footnote{The 5-4 ruling allows officials to “strip search people arrested for any offense, however minor, before admitting them to jails even if the officials have no reason to suspect the presence of contraband.” Adam Liptak, \textit{High court rules strip searches OK}, San Jose Mercury News, Apr. 3, 2012 at A6. (emphasis added). Justice Breyer dissented, writing that this decision was “a serious affront to human dignity and to individual privacy” and that officials should not be allowed to conduct strip searches for people convicted of minor offenses unless the official has reasonable suspicion of contraband. \textit{Id.} The concept that in order to violate individual privacy the government must have a sufficiently strong interest in doing so, dates back to before the Revolutionary War. \textit{See, e.g.}, Wilkes v. Wood, 98 Eng. Rep. 489 (K.B.) (1763) and Entick v. Carrington, 95 Eng. Rep. 807 (K.B.) (1765). These cases repudiated the use of general warrants to search people’s homes and read their diaries to look for seditions libel and were influential in the creation of the Fourth Amendment.}

I asked all three what they thought about the E.U.’s proposed “right to be forgotten,” as it would seem an important legal protection to have, especially in the future, but also carries with it severe free speech implications. The Internet censor replied without hesitation, “Yes,” and explained how much of the content posted online is done so without any consent whatsoever of the data subject – so this would act as a safety net. The Iraqi expatriate thought this was a silly idea. “If someone posts something that embarrasses you, it’s probably because you were doing something embarrassing.” You are responsible for controlling your actions in the presence of others. Chastity’s gut response was “Yes,” but after thinking for a moment, she articulated that it depended on the situation. “If you’re at a party and doing something [in front of others with cameras], you should know that [it] can end up on Facebook and you can choose to act differently.” But if you are in a room with

had to be deleted after 180 days) to now be kept for five years. Charlie Savage, \textit{White House relaxes some counterterrorism restrictions}, San Jose Mercury News, Mar. 23, 2012.
the door closed, “that’s a clear violation of privacy – you closed the door for a reason.” In the future, it will be interesting to see if the E.U.’s “right to be forgotten” gains traction or if it will be forgotten itself.

Technology can be used as a tool for us to share information and it can also find new ways to invade the privacy of others. It has an effect on both prongs of the reasonable expectation of privacy test; the same technology both exposes that which was once protected and in doing so, alters society’s perception of whether or not it should have ever been protected in the first place. “The machine of innovation is critical to our evolution and the advancement of science. However, a machine that runs too fast is an uncontrolled, volatile object – one that might unintentionally harm the privacy and security of those who rely or depend on these technologies.”¹³⁹ The world of tomorrow will be very different when it comes to what is public and what is private. We only have as much privacy as we expect to have – and we can only expect privacy for that which we safeguard and that which we vouchsafe only unto ourselves.

______________________________________________________

“Chef!” a voice rang out from the kitchen, “the eggs are here!” Winston wiped his hands on his apron and nervously responded, “I’ll fetch them myself… I need some fresh air anyway.” Winston spent the brief elevator ride down to street level straitening his uniform, wiping the sweat off his brow, and dusting the flour off his
forearms. “Today is the day!” he declared, trying to psych himself up in the empty elevator car. “Today I will let them know I’ll have no part in this any longer!” The elevator stopped and Winston stepped out onto the loading dock.

The man with the eggs was there. Winston approached and was about to open his mouth when the man took an egg from the top of the crate and tossed it gently in the air. A shot rang out and the egg exploded, covering the two men with yoke. The echo from the sniper’s gun was still reverberating between skyscrapers when the man barked, “So today’s the day, huh?” Winston was paralyzed. “You got something to say?” All Winston could muster was a quivering shake of his head. “That’s what I thought... and you’ll keep it that way, or else we may have to break another egg,” the man warned. Winston’s stomach churned as he thought of his daughter, sitting in her classroom. They had him. He had no choice.

Winston took the crate of eggs. Hidden inside was a small chip containing untraceable anonymous e-cash which was his payment for handing over the secrets of the rich and powerful to the mafia, who used this info in various ways to influence or control politicians, judges, businesspeople, celebrities... you name it. When customers left their LIsAs at Cloister’s device check and ate dinner, the data was being dumped off of their devices and into unsavory databases. His customers paid for and expected privacy; they got the exact opposite.

139 Bailey, supra note 113, at 87.