CHAPTER 5

Privacy

Michael Zimmer

Privacy is a difficult concept to singularly define. Its meaning, value, and level of protection vary across cultures and have evolved continuously over time. Yet, from an information policy and ethics perspective, privacy has had a central role to play throughout history, sparking considerable debate, and often rising in importance alongside technological development.*

INTELLECTUAL HISTORY

While the concept of privacy has been central throughout history, its definition has evolved considerably since the eighteenth century. Initially, privacy was largely conceptualized in terms of freedom from physical intrusion into one's personal property or other private spaces, as famously articulated in prominent US jurists Warren and Brandeis's (1890) seminal essay "The Right to Privacy," in which they quote Judge Cooley's view of privacy as the right to be left alone. Later, in the wake of US Supreme Court decisions in *Griswold v. Connecticut* (1965) and *Roe v. Wade* (1973), privacy in US law became associated with freedom from interference into one's personal affairs, including having control over one's entire realm of intimate decisions, including those dealing with physical access to oneself; cognitive access to one's thoughts and one's intimate behaviors (Gavison 1980; Inness 1992). Most recently, building from Westin's (1970) early conception of privacy as the ability to control information about oneself, privacy has been closely identified with concerns affecting access to, and control of, one's personal information, including information about daily activities, personal lifestyle choices, medical history, finances, religious, or philosophical beliefs, distinctive physical descriptions, employment history, personal relationships, and sexual orientation, to name a few.

The vast legal and philosophical discourse on privacy has been summarized in various ways. Clarke (1997), for example, identifies four key dimensions of the concept of privacy in an attempt to reconcile this plurality of conceptualizations: (1) privacy of the person—concerned with the integrity of the individual's body; (2) privacy of personal behavior—relating to all aspects of behavior, but especially to sensitive matters, such as sexual preferences and habits, political and intellectual activities, and religious practices, both in private and in public places; (3) privacy of personal communications—the interest in being able to

* An earlier version of this text appeared in Zimmer, M. (2015). "Privacy Law and Policy." In P. Ang & R. Mansell (Eds.), *The International Encyclopedia of Digital Communication and Society.* Wiley-Blackwell.

communicate with other individuals, using various media, without routine monitoring of their communications by other persons or organizations; and (4) privacy of personal data—the claim that data about oneself should not be automatically available to other individuals and organizations, and that, even where data are possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. Solove (2008) identifies six broad conceptualizations: (1) the right to be left alone-Warren and Brandeis's famous formulation; (2) limited access to the self—the ability to shield oneself from unwanted access by others; (3) secrecy—the concealment of certain matters from others; (4) control over personal information—the ability to exercise control over information about oneself; (5) personhood—the protection of one's personality, individuality, and dignity; and (6) intimacy—control over, or limited access to, one's intimate relationships or aspects of life. And Tavani (2009) reduces the philosophical discourse to four dimensions: (1) physical/accessibility privacy—freedom from unwarranted intrusion; (2) decisional privacy—freedom from interference in one's personal choices, plans, and decisions; (3) psychological/mental privacy—freedom from psychological interference and protecting one's intimate thoughts; and (4) informational privacy—having control over/limiting access to one's personal information.

In addition to the various conceptions of privacy presented above, there are further distinctions that are commonly used to help define privacy. The first is the distinction between descriptive and normative conceptions of privacy. A descriptive, or neutral, conception states what privacy *is* without incorporating into its meaning whether possessing privacy is a good thing or worth legal protection, such as Gavison's (1980) articulation of privacy as the measure of one's ability to control the access others have to oneself. A normative conception of privacy, by contrast, incorporates a presumption that privacy is something inherently worthwhile, valuable, and deserves protection. Here, privacy is defined not as something one simply has, but something one has a right to, such as the view of privacy as the right to be left alone.

Other distinctions focus on whether privacy is an intrinsic value—something desired for its own sake and necessary for human flourishing—or merely instrumental towards achieving higher-order values such as security or autonomy. And, although most conceptualizations of privacy focus on its importance for individuals, distinctions are also made on the social value of privacy (Regan 1995), maintaining that privacy serves not just individual interests but also common, public, and collective principles like freedom of speech, association, and religion. A growing perspective focuses the value of privacy (and, inversely, the level of concern over a privacy violation) on the practices and contexts that are involved in a particular information exchange. The need for privacy protection, in such a view, is not predetermined by overarching conceptualizations of the *de jure* value of privacy, but rather through a normative analysis of expectations of privacy in particular contexts (Nissenbaum 2009).

Solove's Taxonomy of Privacy Violations

Evidenced by the complex assemblage of conceptualizations and distinctions summarized above, a single authoritative definition of privacy remains elusive. Concerned that this lack of clarity impedes the ability to create law and policy to ensure appropriate privacy protections, Solove (2005) suggests a shift away from the vague term "privacy" and the attempts to articulate how such a right might exist, and instead moves us toward gaining a firmer grasp on the different kinds of activities that pose privacy violations. Such a framework can

provide more concrete ways to understand and identify potential harms, and thus guide legislative and policy strategy.

Solove identifies four basic groups of activities that threaten to violate privacy, each with different related subcategories of activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion.

Examples of information collection include *surveillance,* the watching, listening to, or recording of an individual's activities, as well as *interrogation,* consisting of various forms of questioning or probing for information.

The second group of activities is information processing, the way information is stored, manipulated, and used after collection. Examples include *aggregation,* the combination of various pieces of data about a person; *identification,* the linking of information to particular individuals; *insecurity,* meaning any carelessness in protecting stored information from leaks and improper access; the *secondary use* of information collected for one purpose without the data subject's consent, and *exclusion,* concerning the failure to allow the data subject to know about the data that others have about her and participate in its handling and use.

Solove's third group of privacy-threatening activities identifies examples of information dissemination, which involve the spreading or transfer of personal data, or the threat to do so. *Breach of confidentiality* is breaking a promise to keep a person's information confidential. *Disclosure* involves the revelation of truthful information about a person that impacts the way others judge her character. *Exposure* involves revealing another's sensitive or personal activities, such as nudity, grief, or bodily functions. *Increased accessibility* refers to the amplification of the accessibility of information. *Blackmail* is the threat to disclose personal information. *Appropriation* involves the use of the data subject's identity to serve the aims and interests of another. And *distortion* consists of the dissemination of false or misleading information about individuals.

The fourth group in Solove's taxonomy involves the invasion into people's private affairs. Examples include *intrusion,* invasive acts that disturb one's tranquility or solitude, or *decisional interference,* the government's incursion into the data subject's decisions regarding her private affairs.

CONTINUING ISSUES AND CONCERNS

Privacy rights are inherently intertwined with information and communication technologies. Warren and Brandeis's argument for privacy as the "right to be let alone" was in direct response to threats posed by the latest technological developments of the late nineteenth century—the "snap camera" and "instantaneous photography"—which allowed people to take candid photographs in public places for the first time. Fast-forward 100 years and similar privacy concerns persist with cellphone cameras and online photo- and video-sharing websites.

In recent decades, digital communication technologies—including, but not limited to, cellphones, personal computers, the internet and World Wide Web, and the rise of social media—have generated powerful new infrastructures for the routine capture and flow of personal information. These flows take many forms and stem from various motivations. Cellphone providers track the geographic location of their customers to provide services and optimize network efficiency. Large-scale web advertising platforms and search engines use robust infrastructures to collect data about web browsing and search activities to provide relevant advertising. Users' consumption habits are captured by online service

providers, such as Amazon and Netflix, fueling powerful recommendation systems meant to improve user satisfaction. Millions of people openly share personal information with friends and colleagues (and strangers) on social networking services, such as Facebook and LinkedIn, and their random thoughts and utterances with the world on platforms like Blogger, Tumblr, and Twitter. As evidenced by the rise of social networking and Web 2.0 platforms, the internet has become a platform for the open flow of personal information—flows that are largely voluntarily provided by users—and, as such, appears to have validated Sun Microsystems CEO Scott McNealy's infamous remark that "You have zero privacy anyway. . . . get over it" (Sprenger 1999).

Notwithstanding McNealy's view, privacy has remained a central concern amid the open information flows in our contemporary digital information society, including worries about the growing size and role of networked databases, the possibility of tracking and surveillance by internet service providers and Web search engines, privacy threats to digital rights management technologies, growing concerns about protecting the privacy of users of social networking sites and related Web 2.0 services, and threats of large-scale surveillance of online communication by law enforcement and other government agencies.

These privacy concerns have evolved far beyond what the framers of the Constitution, Warren and Brandeis, or Prosser (1960) could have envisioned. To focus our understanding–and to identify and address the legal and policy measures to address them—we can return to Solove's taxonomy of privacy violations as a means of organizing this panoply of privacy threats posed by digital information and communication technologies.

Information Collection

One common type of information collection that is currently the subject of public debate is using surveillance for the collection and processing of personal data, whether identifiable or not, for the purposes of influencing, managing, or protecting individuals. Surveillance, of course, has existed for centuries, and its methods have been continuously refined to broaden its reach and effectiveness. Clarke (1988) coined the term *dataveillance* —a portmanteau of "data" and "surveillance"—in recognition of the power of advanced digital information technologies and computer databases to facilitate the collection and exchange of information about individuals.

The role of digital information and communication technologies within infrastructures of dataveillance cannot be understated: store loyalty cards connect purchasing patterns to customer databases, intelligent transportation systems enable the tracking and recording of vehicles as they travel the highways, electronic key cards manage access to locations while creating a record of one's movements, and biometric technologies digitize one's intrinsic physical or behavioral traits for automated identification and authentication. More recently, the internet has emerged as not only a revolutionary technology for communication, commerce, and the distribution of information, but also as an ideal infrastructure of dataveillance, enabling the widespread monitoring and collection of personal and identifiable information about its millions of users. The privacy and surveillance concerns with various internet technologies have been well-documented and debated, ranging from the use of web cookies and tracking bugs, the emergence of spyware and digital rights management systems, workplace monitoring of electronic communications, the aggregation and data mining of personal information available online, and the widespread monitoring of internet traffic by law-enforcement agencies.

In the United States, limits on government surveillance and related information collection practices have been based on applications of the Fourth Amendment, most notably in *Katz v. United States* (1967), which made government wiretapping of communication subject to the Fourth Amendment's warrant requirements. With the emergence of new digital information and communication technologies, Congress revised wiretapping laws with the Electronic Communications Privacy Act (ECPA) in 1986, which restricted the interception of transmitted communications and the searching of stored communications. By specifying standards for law enforcement access to electronic communications and associated data, ECPA afforded important privacy protections to subscribers of emerging wireless and internet technologies. Although ECPA was a forward-looking statute when enacted in 1986, digital information and communication technology has advanced dramatically since its passage. It was enacted before web-based email became ubiquitous, before individuals began using cloud-based providers to store and share documents, and before individuals relied on social media platforms to share and archive personal histories, messages, and photos. Under ECPA, it is relatively easy for a governmental agency to demand service providers to hand over these types of personal information that has been stored on their servers. Efforts have increased in recent years to update ECPA to better reflect the contemporary digital information and communication environment.

Notably, US laws regulating information collection were considerably loosened with the passage of the USA PATRIOT Act (an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) following the September 11, 2001, terrorist attacks. The PATRIOT Act effectively amended the ECPA, expanding the authorized use of wiretapping and electronic surveillance, ostensibly to intercept and obstruct terrorism. Provisions included expanding the definition of pen registers and trap and trace devices to apply to addressing information on emails and to IP addresses, allowing enforcement officials to read the addresses of all the emails that are sent from a computer and see all websites visited. The Act also provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communications providers, and expanding the application of the Foreign Intelligence Surveillance Act (FISA) to make gaining foreign intelligence the "significant" purpose of FISA-based surveillance, where previously it had been the "primary" purpose, thus loosening the standard for utilizing the secret approval process for engaging in surveillance actions. Although the PATRIOT Act has generated a great deal of controversy, it has withstood challenges and been reauthorized by the US Congress.

Other digital information collection methods have met some resistance, although it is often the presence of comprehensive global privacy laws that spark new privacy protections for users. The widespread use of web cookies by search engines, social media platforms, and advertising networks to track users' online activities has drawn considerable attention from privacy advocates and policymakers. While users in the United States have little legal protection from such threats to their online privacy by private companies, pressure from European regulators has resulted in improved privacy protections. For example, Google's practice of retaining personally identifiable information (e.g., IP addresses and cookie information) indefinitely came under fire by the Norwegian Data Inspectorate. Google relented and limited the length of time it would retain identifiable information on its users. Similarly, Facebook was investigated by Canada's Privacy Commissioner and was found to be in violation of Canadian privacy laws. In response, Facebook agreed to add significant new privacy safeguards. In both these cases, large multinational digital information companies were forced to respond to strong privacy laws from relatively small countries (in terms of

their user base) in ways that benefited all users across the globe, irrespective of their provincial regulatory landscape.

Information Processing

The increase in information collection further exposes individuals to the privacy harms caused by new forms of information processing. New digital information processing technologies and techniques make aggregation more efficient and combining data and analyzing it certainly can be put to beneficial uses. Amazon.com, for example, uses aggregated data about a person's book-buying history to recommend other books that the person might find of interest. Credit reporting allows creditors to assess people's financial histories in a world where first-hand experience of the financial condition and trustworthiness of individuals is no longer possible.

Alongside these benefits, however, aggregation can cause privacy harms because of how it unsettles expectations. People expect certain limits on what is known about them and on what others will find out. Aggregation upsets these expectations because it involves the combination of data in new, potentially unanticipated ways to reveal facts about a person that are not readily known. From a law and policy perspective, the United States has done little to limit or regulate information processing in this way. The European Union's (EU's) Data Directive, however, has specific provisions intended to limit unwanted information processing. It mandates that personal data shall be obtained only for specified and lawful purposes and shall not be further processed in any manner incompatible with those purposes without specific consent. The EU's rules on information processing have impacted how companies like Facebook and Google handle and process personal information, forcing changes to features like automated tagging of faces in uploaded photos and the automated targeting of advertising based on user data.

One form of digital information processing receiving considerable attention from US regulators and lawmakers is online behavioral targeting. Behavioral targeting involves the collection of information about a consumers' online activities to deliver advertising targeted to their potential upcoming purchases. By observing the web activities of millions of consumers, advertising networks can closely match advertising to potential customers. Data collected includes what websites users visit, how long they stay there, what pages they view, and where they go next. The most well-known method for tagging consumers is with cookies, although methods such as web beacons and Flash cookies are actively used. Generally, the data that behavioral advertisers collect is not personally identifiable because it does not include the consumer's name, physical address, email address, or other personal identifiers that could translate directly to the offline world. Nonetheless, numerous threats to informational privacy persist. Online behavioral targeting results in the compilation and processing of a sizable array of potentially sensitive data about the consumers that exists outside their ability to protect, control, or monitor that data. By merely participating in the internet economy, consumers lose control over which details about their private lives are known, and they have little control over who gets to learn of these details after the data passes into a profiler's hands.

In response to these privacy concerns, the US Federal Trade Commission issued the report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* in 2010, which proposed a framework to balance the privacy interests of consumers with innovation that relies on consumer information to develop beneficial new

products and services. The report also suggested the implementation of a "Do Not Track" mechanism—likely a persistent setting on consumers' browsers—so consumers can choose whether to allow the collection of data regarding their online searching and browsing activities. Some online advertising providers, such as Google and the Digital Advertising Alliance, a group of digital advertising trade organizations, have adjusted their behavioral targeting procedures as a result, offering consumers more transparency and access to information on how they are being profiled, and the ability to opt-out of tracking altogether.

Information Dissemination

Digital communication and information technologies have made information dissemination easier, faster, broader, and harder to reverse. The privacy harms that accompany disclosure and exposure are amplified when personal information can be disseminated via the internet and World Wide Web. With blogs and social networking sites, personal information is being posted online at a staggering rate, and given the ease at which information can be digitally recorded and spread, information previously contained within particular contexts or circles easily escapes out of one's control. Further, once personal information has been disseminated across digital networks, it is nearly impossible to recover or remove it. The proliferation of personal data on the internet can have significant effects on people's reputations, dignity, and privacy.

The fundamental premise behind most so-called Web 2.0 applications and services—characterized by popular websites, such as Flickr, Wikipedia, del.icio.us, Facebook, and YouTube, which feature user-generated content, opportunities for collaboration and harnessing collective intelligence, and relatively open platforms where anyone can participate, modify, or share content—is the open flow of personal information online. The wide-scale dissemination of personal information powered by Web 2.0 is further fueled by search engines that actively incorporate the information flows from Web 2.0 applications directly into searchable indexes. For example, a Google search for an individual's name routinely returns Facebook and LinkedIn profile pages, and Yahoo's purchase of Web 2.0 properties including Flickr and del.icio.us results in the possible integration of personal photos or bookmarks directly into its search engine results.

A similar privacy threat stems from the increased accessibility of archival information in a digital environment. Powerful web search engines can put pieces of information hidden in the most obscure websites at one's fingertips, information brokers provide detailed background checks and digital dossiers of personal information that are only a click away, and large databases of public records are increasingly placed online, removing any practical obscurity previously enjoyed by individuals who presumed only the most diligent researchers would find personal details of their lives hidden away in government archives.

Invasion

The privacy threats stemming from Solove's "invasion" category permeate many of the preceding examples. The collection of personal information through various digital surveillance technologies, web tracking cookies, or data mining algorithms all lead to a feeling of "digital intrusion" into our activities and lives—both online and off. New and innovative features of our digital landscape—such as Google's Street View cameras, Facebook's desire

to track online purchases and automatically post such activities to a consumer's public profile, the ability for individuals to digitally record and process everything they "see" with the Google Glass wearable computer—present invasions to our personal spaces and activities in much the same way as the instant photography Warren and Brandeis fought in the late nineteenth century.

Perhaps the most potent example of digital invasion in the early twenty-first century is the discovery of, and reactions to, the US National Security Agency's robust globalized mass surveillance programs. Through a series of disclosures by Edward Snowden in 2013, the general public became aware of a variety of digital and electronic surveillance programs. The NSA's PRISM surveillance program, for example, combined many of the information collection, processing, and dissemination concerns outlined above through its massive aggregation of private electronic data belonging to users of major internet providers like Gmail, Facebook, AOL, Microsoft, and others. The NSA also reportedly routinely collected metadata on the phone records of more than 300 million Americans, and each day collects contacts from an estimated 500,000 buddy lists on live-chat services as well as from the inbox displays of web-based email accounts. Taken together, the data enables the NSA to draw detailed maps of people's lives based on their personal, professional, religious, and political connections.

The level of privacy invasions felt by these wide-scale digital surveillance programs and techniques has sparked considerable global concern and outrage. Various members of the US Congress have called for reform of existing surveillance laws and policies, and members of the European Parliament have proposed a measure that, if enacted, would require US companies to seek clearance from European officials before complying with US warrants seeking private data about European citizens. These reactions have met some resistance by those arguing for the need for advanced surveillance measures for national and global security, highlighting the ever-present tension between security and privacy.

Primary Source Materials

Warren, S., and Louis Brandeis. 1890. "The Right to Privacy."
***Harvard Law Review* 4: 193–200.**

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life

> has come to mean the right to enjoy life—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible. . . . Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration.

REFERENCES

Clarke, Roger. 1988. "Information Technology and Dataveillance." *Communications of the ACM* 31 (5): 498–512.

_____. 1997. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms." www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.

Federal Trade Commission. 2012. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers.* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Gavison, Ruth. 1980. "Privacy and the Limits of Law." *Yale Law Journal* 89 (3): 421–71.

Inness, Julie. 1992. *Privacy, Intimacy, and Isolation.* New York: Oxford University Press.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

Prosser, William. L. 1960. "Privacy." *California Law Review* 48: 383–423.

Regan, Priscilla. 1995. *Legislating Privacy: Technology, Social Values, and Public Policy.* Chapel Hill, NC: University of North Carolina Press.

Solove, Daniel. 2005. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154: 477–564.

Solove, Daniel J. 2008. *Understanding Privacy.* Cambridge, MA: Harvard University Press.

Sprenger, Polly. 1999. "Sun on Privacy: Get over It." *Wired,* January 26. https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

Tavani, Herman. 2009. "Informational Privacy: Concepts, Theories, and Controversies." In *The Handbook of Information and Computer Ethics,* edited by Kenneth Himma and Herman Tavani, 131–64. New York: John Wiley and Sons, Inc. http://onlinelibrary.wiley.com/doi/10.1002/9780470281819.ch6/summary.

Warren, S., and Louis Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4: 193–200.

Westin, Alan F. 1970. *Privacy and Freedom.* New York: Atheneum.

ADDITIONAL RESOURCES

Bennett, Colin J., and Charles D. Raab. 2006. *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: MIT Press.

boyd, danah, and Alice Marwick. 2011. "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies." *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.* http://papers.ssrn.com/s013/papers.cfm?abstract_id=1925128.

Capurro, Rafael. 2005. "Privacy: An Intercultural Perspective." *Ethics and Information Technology* 7 (1): 37–47.

DeCew, Judith. 2015. "Privacy." In *The Stanford Encyclopedia of Philosophy,* edited by Edward N. Zalta, Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/spr2015/entries/privacy/.

Givens, Cherie L. 2014. *Information Privacy Fundamentals for Librarians and Information Professionals.* Lanham, MA: Rowman and Littlefield Publishers.

Gormley, K. 1992. "One Hundred Years of Privacy." *Wisconsin Law Review,* 1335.

Jones, Meg Leta. 2016. *Ctrl + Z: The Right to Be Forgotten.* New York: NYU Press.

Krotoszynski, Ronald J. 2016. *Privacy Revisited: A Global Perspective on the Right to Be Left Alone.* New York: Oxford University Press.

Richards, Neil. 2015. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age.* New York: Oxford University Press.

Solove, Daniel J., and Paul M. Schwartz. 2011. *Privacy, Information, and Technology.* Aspen Publishers.

Zimmer, Michael. 2008. "The Externalities of Search 2.0: The Emerging Privacy Threats When the Drive for the Perfect Search Engine Meets Web 2.0." *First Monday* 13 (3). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2136/1944.