23

DATA PRIVACY

by Mark Sableman

Since the 1960s, Americans have been warned that the development of intrusive technologies was creating a need for new legal protection of information (data) privacy. In works such as Alan F. Weston's *Privacy and Freedom* and Arthur R. Miller's *The Assault on Privacy*, dire warnings were issued about the developing surveillance society, in which ordinary citizens would be subject to intrusive data collection by various means, and the compilers, analysts, and owners of that data would gain extraordinary insights into ordinary citizens' private lives. For five decades, new books, new warnings, and new theories of data-privacy invasions issued forth regularly. Many of these writings were speculative, and they were often not even clear as to who would be collecting and using data—the federal government, local police, criminals, businesses, or others.

Over the years, various laws have been enacted to address real or assumed problems relating to data privacy. In some cases, the laws have been quite specific, drawn up to address very narrow, particularized concerns. In other cases, they have sought to broadly address current and future developments in technology. And in many situations, old doctrines, including common law doctrines, have been used to address modern data-privacy concerns. But even after a half century of thinking about data privacy, the field is still emergent.

Even the concept of data privacy is still unsettled. For example, is the concern one of data collection, data use, or both? Is the key issue whether consumers have advance knowledge and give consent, or are such concepts illusory? Even the interests at stake are still being debated. Do individuals have some personal or property interest in the information that identifies them? Or do the legitimate privacy interests focus more on data about what the person does, including his or her shopping and buying activities? Or is there some yet-to-be-described interest that needs protection when data from different sources are compiled? Are we most concerned about secret data collections and compilations, or with the accumulation of individual pieces of information knowingly provided? Do Internet and mobile device data collections present all new privacy issues?

This essay will consider data privacy concerns, how they fit into the broader framework of privacy rights in the United States, some of the

interesting initial steps that have been taken to address data privacy in the context of the Internet and modern electronic communications, and some of the policy issues implicated by data privacy and its regulation.

The Various U.S. Privacy Laws

The United States has various branches of law that share the name "right of privacy," but no single omnibus "right" of privacy. Privacy rights arise and are recognized in different areas of law in different ways. Data privacy draws on some of these areas (common law torts and intellectual privacy, for example) but is distinct from some other areas.

Common Law Privacy Torts

Among the best-known rights of privacy are the privacy torts recognized by William Prosser in his 1960 *California Law Review* article, "Privacy." Prosser identified four key privacy rights that developed over the years in the common law. These rights, using Prosser's terminology, are (1) intrusion, (2) public disclosure of embarrassing private facts, (3) false light in the public eye, and (4) appropriation of plaintiff's name or likeness. With due respect to this leading tort scholar who broke new pathways in privacy law, these four torts do not really hang together. Two of them relate to privacy in the publication context. One relates to privacy in the information-gathering context. And the fourth relates to a personal property right that really has little or nothing to do with privacy and has most often been characterized as, instead, "the right of publicity."

Information-Gathering Privacy Torts. Information-gathering activities may violate a person's right of privacy if the information gatherer unreasonably intrudes (physically, electronically, or otherwise) upon an area in which that person has a reasonable expectation of privacy. Such activity lies at the heart of the privacy tort that Prosser identified as "intrusion into seclusion." The oldest means of intrusion was trespassing—entering into another person's home, without permission. The modern tort of intrusion is essentially trespass law updated to the age of potentially intrusive devices such as hidden cameras, hidden tape recorders, and parabolic microphones. Whatever the means, an intrusion occurs when an information gatherer breaches another's reasonable expectation of privacy. Practicalities override technicalities in this area. To determine if an intrusion violation has occurred, it is often necessary to examine the totality of a situation and what is practically understood among the parties. For example, even if a news subject invites a reporter into his house or business, an intrusion may nonetheless occur if the reporter uses a concealed camera or recording device during the consented-to interview (see *Dietemann v. Time, Inc.*, 449 F.2d 245, 1 Media L.Rptr. 2417 [9th Cir. 1971]). Even in a public place, intrusion can occur if inappropriate cameras, lights, or techniques are used (see *Le Mistral, Inc. v. Columbia Broadcasting System*, 61 A.D.2d 491, 402 N.Y.S.2d 815, 3 Media L.Rptr. 1913 [1978]).

Other modern techniques raise intrusion-like issues. Extended surveillance can under some situations become an invasion of privacy. For example, if the surveillance was conducted in

such a way as to be deliberately bothersome to the subject and apparent to others with whom he or she associated, it might be considered an unlawful intrusion (see *McLain v. Boise Cascade Corp.*, 533 P.2d 343, 346 [Ore. 1975]). Similarly, both federal and state statutes set limits on electronic eavesdropping, including recording of conversations; these modern laws are among the most important privacy laws affecting information gathering. The federal eavesdropping statute, 18 U.S.C. §§ 2510–2520, is generally considered a "one-party consent" statute. That is, if one party to a conversation consents to recording it, it is lawful to record it even without the other party's consent. State laws are varied, however, and eleven states, including some large and important states such as California, Illinois, and Florida, have two-party consent eavesdropping statutes, in which all parties to a conversation must consent, or the conversation cannot be recorded.

Publication-Related Violations. Two of Prosser's privacy torts relate to publications of private information, and are based on the concern that some facts about people are so intimate, embarrassing, and private, or so misleading and offensive, that they should not be published.

Public Disclosure of Private Facts. This tort is designed to protect individuals from the embarrassment that would result from public disclosure of intimate and offensive—but true—facts about themselves. The private facts tort comes closest of all the privacy-based legal claims to most people's ordinary understanding of privacy. The danger in this tort, however, stems from its subjectivity, because it requires courts (and juries) to make difficult judgments as to the offensiveness of the publication and the *legitimacy* of the public's interest in it. Most court rulings have found violations of this tort only in cases of disclosure of matters of highly intimate nature such as health, sexuality, or nudity.

False Light. This tort is designed to cover published statements that give an inaccurate and offensive picture of a person. As with private facts, false light is measured by what is highly offensive to an ordinary person. Private facts claims are based on *truthful* publications that are highly offensive; false light deals with *false* publications that are highly offensive. The situations most likely to lead to false light include publications placed in an offensive context, and publications making a false but favorable attribution.

Fourth Amendment

The Fourth Amendment to the U.S. Constitution prohibits police from conducting unreasonable searches and seizures. This right is clearly the most important privacy right in the context of criminal law, and thus Fourth Amendment issues are sometimes referred to as involving a "right of privacy." Many courts measure the reasonableness or unreasonableness of a search or seizure based upon whether the defendant had "a reasonable expectation of privacy" when and where the search was conducted.

Reproductive Rights

In *Griswold v. Connecticut*, 381 U.S. 479 (1965),

Justice William O. Douglas described for a Supreme Court plurality a number of provisions of the Bill of Rights that, in his view, created a "penumbra" suggestive of a right of privacy. The Supreme Court in *Griswold* applied that penumbral right of privacy to invalidate a Connecticut statute that criminalized use of contraception among married couples. Later, the *Griswold* privacy penumbra was extended in the landmark case of *Roe v. Wade*, 410 U.S. 113 (1973), to recognize a limited constitutional right of a woman to choose to have an abortion. Particularly after *Roe* became a centerpiece of a spirited public policy debate, the phrase "right of privacy" was used, chiefly by proponents of the decision, to refer to *Roe-Griswold* reproductive rights. This branch of privacy law, however, is quite different from civil privacy rights relating to information and data.

Government Surveillance

Government surveillance has always raised serious privacy concerns. Concerns about government surveillance led, for example, to the particular rules and regulations relating to wiretapping in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Government surveillance was also at issue when the USA Patriot Act in late 2001 amended Title III and other laws restricting or affecting government data collection.

Intellectual Privacy

Some scholars have suggested that one of the most important privacy concerns of the modern era is "intellectual privacy," referring to privacy in records of one's intellectual activities. When, for example, it was thought that investigators might have examined the video rental habits of proposed Supreme Court nominee Robert Bork, Congress passed the Video Privacy Protection Act, prohibiting disclosure of such information except under certain specified conditions. In fact, Mr. Bork's video records have never been examined, but the broad concern about such an intrusion made the resulting legislation popular. Similar legislation protects records of library book checkouts, for example. It has been suggested that increasing amounts of data collection, and improved technologies for sifting and analyzing data, make possible intellectual privacy intrusions more likely in the future, and hence this subject is one of the important emerging data-privacy topics.

Data Privacy

The final subarea of privacy rights relates to technological data collection and its uses and abuses, though it clearly overlaps with some of the other areas. The concern here is that modern data-processing technologies make available collection, sorting, aggregation, analysis, and use of data in ways never before possible. Modern technologies take privacy intrusions to a new level. The tort of intrusion could have occurred in a small town with someone looking through a window. Intellectual privacy violations could have occurred in a small town library if the librarian let the wrong person look at a user's records. But data privacy for the most part is an issue of the modern age, enabled by modern data-processing technologies. And indeed, though it has been predicted and analyzed since

the 1960s, data privacy came into its own as a real and pervasive issue most strongly in the Internet era beginning in the mid-1990s. This is the arm of the right of privacy that promises to get the most scrutiny, attention, enthusiasm, and concern as time goes forward.

Data privacy is often understood to cover the desire of consumers to limit or control personal information that is recorded on mailing lists, credit reports, and business data banks. Another aspect of data privacy involves so-called data-breach laws that require notification of consumers when personal data stored in databases are lost.

Data in the Internet Age

In the Internet age, data has become an important business asset. It has become useful to businesses in the course of product development, marketing, and sales. Indeed, it is not just that data can help companies develop, promote, and sell new products and services. For many companies, data itself has become a saleable product. Some have characterized data as "the new oil" or "the new soil" of the Internet age.

Data privacy seems to be a popular issue, as illustrated by the broad interest in an influential *Wall Street Journal* series about data privacy, which began running in 2010 under the ominous series title, "What They Know." The *Journal* series dramatized behavioral advertising, making both consumers and policymakers better aware of what had until then been something of an insider debate. A *Journal* animated graphic, "A Short Guide to Cookies," for example, portrayed cookies as little animated Lego animals that carry information back and forth between a user's computer and the Internet, and explained that third-party ad networks conduct tracking on hundreds of thousands of sites. Even more importantly, the *Journal* series described research concerning flaws in the tracking system. For example, while users can, in theory, delete (or refuse to accept) normal cookies if they do not want to be tracked, in many cases, Flash cookies (a different technology, often associated with online videos) were often dropped on to user computers, even if the user had attempted to refuse cookies. Even worse, Flash cookies sometimes "respawned" traditional cookies that the users had attempted to delete. While the Flash cookie problem probably arose more from technological conflicts than malicious intent, the *Journal's* story raised eyebrows. Forty-nine of the top fifty U.S. websites used a total of 3,180 tracking files, the *Journal* reported. (The *Journal's* own website used trackers, too, the series acknowledged.) The *Journal* similarly found and described research regarding "referrer header tracking," which it described as "history tracking." Class-action lawyers responded with various suits alleging that use of Flash cookies and referrer header tracking was illegal.

While government collection of data through technological means certainly occurs, as the 2013 Edward Snowden revelations of NSA documents showed, the general focus of data-privacy regulation has been on business entities that collect, use, and sell data in the course of their commercial activities. The regulating activities have focused on two fronts: (1) stat-

utes or regulations on data collection, use, and transfers, and (2) court actions claiming various practices and activities as invasions of privacy.

Statutory Privacy Rights

While data privacy is often considered a matter to be regulated by statute or regulation, as opposed to judicial case-by-case decision making, until recently almost all data-privacy legislation was piecemeal, designed for particular industries or particular situations. Beginning in 2010, however, proposals surfaced for broad-based privacy regulation.

The Existing Patchwork

Most federal laws regulating data privacy focus on particular industries. The Cable Communications Policy Act, 47 U.S.C. § 551, addresses cable television operators. The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*, regulates financial institutions. The Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160–164, regulates healthcare-covered entities such as healthcare providers, health plans, and healthcare clearing houses.

Other federal data-privacy laws focus on particular interests. The Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506, relates to collection of personal information from children under the age of thirteen. The Video Privacy Protection Act, 18 U.S.C. § 2710, generally prohibits video sale and rental companies from disclosing personally identifiable information regarding customers except under certain situations. The Telephone Consumer Protection Act, 47 U.S.C. § 227, regulates telemarketing, unsolicited fax advertisements, and related marketing communications.

Even the broader data-privacy statutes are tailored to particular concerns and apply in only limited situations. The Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.*, protects wire, oral, and electronic communications while those communications are being made, or in transit, and when they are stored on computers. This was a telephone-era statute designed to address wiretapping and similar concerns, although it is written broadly enough so that its provisions apply, clumsily, to e-mail and other electronic communications. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is a broad statute primarily designed to address computer hacking, although it covers a much broader array of unauthorized access of computers and networks, and access beyond the scope of authorization.

State laws address data privacy in various ways. Most states have a computer-hacking statute similar to the federal Computer Fraud and Abuse Act. Additionally, most states have data-breach statutes that require businesses to notify consumers when a data breach has occurred and may also specify other requirements related to data breaches and/or notification. Finally, some states have specific Internet privacy laws such as, for example, California's Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575–22579, which requires operators of commercial websites that collect personal information from California residents through the Internet to conspicuously post a privacy policy on their

website meeting certain specifications.

Constitutional Limits on Data Privacy Legislation

One of the questions of the data age is the extent to which data collection and use can be prohibited or, to put it another way, whether the First Amendment protects the gathering and use of data just as it protects, for example, newsgathering. This issue was presented to the U.S. Supreme Court in *Sorrell v. IMS Health Inc.*, 131 S.Ct. 2653 (2011). Because of consumer complaints about prescription-drug marketing, legislatures in several New England states banned sale of data concerning prescribing habits of physicians. (The data was required to be collected by law, and had been available for years to those who were willing to pay for it.) These statutes made it far more difficult for the drug companies to market particular drugs to the physicians who would be most interested in them, and thereby inhibited sales of new pharmaceutical products. The states intended this, for they sought to discourage sales of expensive inpatent pharmaceuticals and to encourage use of less-costly generic medicines. In short, the legislatures sought to influence commercial activity (prescribing of new prescription drugs, which was presumed to drive up healthcare costs) by imposing controls on collection and use of data (information about past prescribing activity).

The company whose practices were specifically targeted by these laws, IMS Health, challenged the laws on various grounds. The case from New Hampshire was the first case to reach an appeals court, and in that case the U.S. Court of Appeals for the First Circuit ruled against IMS Health, and showed hostility to the argument that collection and sale of data was protected by the First Amendment, in a memorable passage comparing regulation of data to regulation of "beef jerky," holding that one was equally as permissible as the other.

The Supreme Court, however, in a 6–3 decision written by Justice Anthony M. Kennedy, found a similar Vermont law unconstitutional, and held that states have limited powers in regulating information collection and commercial advertising. More specifically, the Court held unconstitutional the law at issue, because it attempted to restrict speech (collection, dissemination, and use of prescriber-identifying information) in order to promote its own viewpoint (disfavoring sales of costly new drugs and favoring use of generic drugs).

On the data-collection point, the Court's majority opinion characterized the state law restricting data collection as an attempt to "tilt public debate in a preferred direction." Significantly for news and information gatherers, Justice Kennedy noted that gathering and assembling data is an essential, and thus protected, part of the communicative process: "Facts … are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."

Despite the Court's limited holding (directly addressing only data restrictions integral to viewpoint discrimination), Justice Kennedy's decision includes a number of suggestions that

future cases involving restrictions on data use are also likely to be critically examined under First Amendment free-speech principles:

- He rejected Vermont's characterization of the data use and transfer involved in the case as "conduct" rather than constitutionally protected speech, noting that even "dry information" is an essential ingredient in protected communications.
- He stated that First Amendment protection applies even when states merely "burden" but do not actually ban certain communications—meaning that states cannot do what Vermont did, and burden data collection and use as an indirect means of preventing disfavored communications based on those data.
- He strongly rejected the argument that Vermont could ban certain data because of concerns about what will happen when they are used: "If pharmaceutical marketing affects treatment decisions, it does so because doctors find it persuasive. Absent circumstances far from those presented here, the fear that speech might persuade provides no lawful basis for quieting it."

Justices Stephen G. Breyer, Ruth Bader Ginsburg, and Elena Kagan dissented, opining that the Vermont statute was "inextricably related to a lawful governmental effort to regulate a commercial enterprise" and thus should have passed the First Amendment standard for commercial speech.

Proposed Omnibus Data Privacy Regulation

In May 2010, U.S. Representative Rick Boucher (D-VA), then chair of a House subcommittee that considered Internet laws, announced a proposed omnibus data-privacy bill—that is, a federal law that would cover all aspects of data privacy, in every industry. This announcement set off a flurry of other data-privacy proposals, and the congressional focus on data privacy continued in 2011 even after Representative Boucher lost his seat in the 2010 Republican electoral sweep. One proposal, by Representative Jackie Speier (D-CA), would mandate "Do Not Track" rules for Internet browsing. A more modest bill, proposed by Representative Clifford Stearns (R-FL), would require clear and full disclosures of privacy practices, and recognize the opt-out methods that are in general use today. Yet another bill, jointly sponsored by Senators John Kerry (D-MA) and John McCain (R-AZ), would mandate "robust" notices to consumers of Internet data-collection practices, give individuals broad rights to opt out of having information about themselves collected or used, and impose even stronger controls (such as opt-in requirements) on sensitive medical and financial information. The Kerry-McCain bill would also seek to minimize use of data—for example, by requiring limited use, in accordance with the original purpose of the data, in cases where data are transferred to third parties.

Independent agencies and the executive branch also proposed data-privacy regulations of various kinds. Most of the proposals involved solutions that would give users more under-

standing (in data privacy lingo, "transparency" or "notice") of data-collection practices, and more control ("choices") with respect to them. Some looked beyond traditional ways of thinking, by incorporating privacy considerations into all business conduct ("privacy by design") or by setting new national standards ("codes of conduct").

The Federal Trade Commission, in various staff reports, addressed both online behavioral advertising (discussed below) and other data-privacy interests. In its December 1, 2010, report, "Protecting Consumer Privacy in an Era of Rapid Change," it suggested that a totally new legal "framework" was needed for privacy protection —a "privacy by design" framework in which privacy considerations and assurances would be built into a company's default mode of operations. Around the same time, the Department of Commerce noted its support of industry self-regulation but suggested that government was needed to assist or prod industry participants into setting appropriate standards. Commerce also suggested that it could help coordinate and harmonize foreign and domestic data-privacy standards—an important issue for international businesses that need to transfer data across national boundaries.

Judicial Enforcement of Data-Privacy Rights

Data-privacy issues are addressed through court cases in many ways. Because the impact of alleged data-privacy violations is generally relatively small on each individual, but cumulatively large, class-action lawsuits are generally utilized. Depending on the circumstances, they may allege a variety of common law, statutory, and contract causes of action. While few such cases have gone to trial and judgment, the threat of class-action cases, and settlements of many of them, has prompted significant changes in many privacy practices.

Inadequate Privacy Disclosures

Privacy Policy Noncompliance. In the normal course of Internet activities, significant amounts of data are regularly collected. Internet users register with websites. They provide their name and credit card information on shopping sites when they make purchases. They plug in personal information to various websites in order to get feedback and benefits from those websites. Except in relatively rare cases, the law imposed no particular restraints on how information would be used, and it was up to each Internet site operator to set its own practices. However, activists insisted that Internet sites should disclose and follow written published "privacy policies." Most consumer-focused Internet sites did so.

In the first decade of the Internet, these privacy policies led to many problems. For example, many young Internet companies, in the late 1990s, promised their customers a great deal of privacy. Often, for example, Internet companies promised that they would maintain their customer databases privately and never use them for external purposes. However, when the dot-com bubble burst in 2000, many of these companies found that their only real asset was their customer database—which some of them

promptly sold to third parties. This action led to class-action lawsuits in which the plaintiffs accused the company of breaching its own contractual covenants in its privacy policies, and thereby violating the legitimate privacy expectations of its users. These lawsuits taught Internet companies a compelling lesson: because privacy policies set enforceable contractual expectations, their provisions must be thought out carefully in advance, and should never promise more than what the company would actually in practice do.

Similarly, even long after the Internet bubble, Gateway Learning Company displayed a company "Promise" to users that it did not "sell, rent or loan any personally identifiable information regarding our consumers with any third party unless we receive a customer's explicit consent." When the FTC caught the company doing just that—renting customer information—it had to enter into a consent decree and cease that practice.

Inadequately Disclosed Policies. Even when a company discloses its practices, it may be claimed that the policies promised more than they delivered, or were not sufficiently clear so that they could be understood by consumers. For example, when Google launched its Google Buzz social media service in February 2010, that service allowed Gmail users to share their photos and posts with others. The Buzz service, however, automatically created a list of each user's "followers" from the user's Gmail contacts. Google then posted user photos and other information that previously had been posted to YouTube and Picasa (two other Google services) in connection with the user's Buzz pages. All of this information was public, and the users had made it all available to Google. But many users complained that they had not read or understood the terms and conditions of the Buzz program, which Google had set up on an "opt out" basis. Any user who clicked "yes" to a new long legal disclosure was automatically placed in an activated Buzz account. Plaintiffs further claimed that they had not understood that Buzz would assemble their posts and contacts as it did. After complaints, Google revised the program several times and eventually terminated it.

In a similar case, the FTC alleged that Sears Holdings hid significant provisions in its revised policies, by essentially presenting consumers with several layers of disclosures, which only the most intrepid users would fully examine or understand. The agency insisted that companies must make their important new disclosures sufficiently prominent that users will see them, and they must ensure that marketing materials do not mislead users or contradict their legal policies.

Increasingly, lawmakers are specifying what kinds of privacy disclosures must be made and how they must be made. The California Online Privacy Protection Act effectively requires companies that market nationwide to disclose a basic set of privacy policies. FTC guidelines and enforcement actions and developing industry fair information practices are setting further expectations.

Suits alleging deception in privacy practices are

usually brought on multiple claims. Contract claims are common, because privacy policies and website terms of use generally create contractual commitments. Consumer Fraud and Abuse Act violations can be alleged on the theory that information was obtained from user computers without authorization, or beyond the scope of authorization. Public disclosure of private facts can be alleged where a user's private information was disclosed without the user's approval. Various other statutory claims can be, and usually are, alleged, although often the claims read like strained attempts to shoehorn the facts of the case into the few available privacy statutes. The most obviously applicable statute, the Federal Trade Commission Act, with its command against "unfair trade practices," is not available, because only the FTC can enforce it, although state "Little FTC" consumerprotection acts are often alleged, as many of them permit private rights of action.

Hidden Data Collection. Many class actions have alleged that user data has been collected without any disclosure to consumers, or in violation of stated policies. For example, when research revealed that "Flash cookies" sometimes caused deleted http cookies to "respawn," thereby re-creating identifying information that a user had sought to shield, a number of suits were filed. In those cases, creative class-action lawyers invoked the Video Privacy Protection Act, in part because the Flash cookies usually originated with video content displayed through the Flash application. Another example of alleged hidden data collection came when Google was sued for making its customer search queries known to third parties when it shared "referrer headers" with search engine optimization companies. Similar claims were asserted against Facebook and Zynga for allegedly collecting and using private Facebook IDs.

Data Breach. When a database containing personally identifiable information is inadvertently disclosed, this can violate state data breach laws, and lead to civil liability to those persons whose personal data was compromised. Most states have databreach laws, requiring special notices to consumers of data breaches— that is, when personal information, in unencrypted form, is accessed by or improperly disclosed to an unauthorized person. The various state laws have different definitions, thresholds, limits, and notice requirements. Data breaches can occur because of criminal hacking, but also because of negligence—leaving a laptop with unencrypted databases where it can be lost or stolen, for example. Claims may be brought if identity theft results, or even if customers face inconveniences and uncertainties from the breach. Companies involved in data breaches have found that even just sending out notices and taking other statutorily required steps can be very costly.

Particular Issues in Data Privacy

Data privacy can present many new issues because, as commentators have been noting for the last fifty years, the collection, analysis, and use of large amounts of electronic data often presents altogether new situations and concerns. Thus, in considering data privacy issues, one must consider some of the unique characteristics of data-privacy and how they raise

both concerns and benefits. The transformation of aggregated and collated data to reveal new information is one of the key concerns in data privacy. The ability to use information gathered through data monitoring, such as tracking of Internet users, is another, and the debate over online behavioral advertising dramatizes the different issues involved in such new and unprecedented data-based technologies. Data collection through mobile devices also raises unique concerns. Finally, in all data-privacy situations, one must assess the value and utility of the services enabled by data collection and use.

Data Aggregation Concerns

One of the big concerns relating to data privacy is the modern capability of tying together many different data sets. That is, even if one has no objection to data collection for certain purposes, if that data are aggregated with other data, the combination database may raise concerns. A database of names and addresses of persons who live in a particular neighborhood, standing on its own, may raise few or no privacy concerns. If that database is compiled with records of sexual offenders, and the result is a list of where sexual offenders live in your neighborhood, that combination reveals new, previously unavailable, information. That compilation may be useful for one who wants to know where sexual offenders live. But if the name-and-address list were combined, for example, with a list of buyers of anti-HIV drugs, the conclusion about the resulting database may be different, since it would reveal who in the neighborhood was likely to have a certain medical condition, AIDS. Whether the result is useful or intrusive, there can be no question that combining two or more different databases can indeed lead to startling new information.

The concerns of aggregating data were heightened when it became apparent that even so-called anonymized and aggregated information can be analyzed in such a way that individuals can be particularly identified. This result was dramatized when Netflix, the movie rental company, conducted its "Netflix Prize" competition, in which it opened up its supposedly anonymized database to various analysts who were challenged to develop better algorithms for predicting movies that users would like to see in the future.

In a paper titled "Robust De-Anonymization of Large Datasets (How to Break the Anonymity of the Netflix Prize Dataset)," two researches at the University of Texas determined that they could make correlations between the anonymized Netflix database and other publicly available databases, thus enabling them to de-anonymize portions of the Netflix database. For example, they used the publicly available Internet Movie Database, and by linking together information from that database with the anonymized Netflix records, they were able to successfully identify known users of Netflix, even uncovering their apparent political and sexual preferences and other sensitive information. In their study, they concluded, "Even if identifying information such as names, addresses, and Social Security numbers has been removed, the adversary can use contextual and background knowledge, as well as cross-correlation with publicly available databases, to re-identify individual data

records." After the researchers' revelations, Netflix cancelled its prize competition. But the incident stands as an example of the ability to develop potentially intrusive information through correlation of disparate databases.

Online Behavioral Advertising

Online behavioral advertising ("OBA" for short) comes in several varieties. Broadly speaking, OBA refers to tracking an individual's online activities in order to deliver advertising tailored to the individual's interests. Or, to use the vivid image of one expert, Ashkan Soltani, "It's like you walk into a town and the merchants put a sticker on your back that tells everyone your shopping habits."

OBA first came to public attention in 2008 through the so-called Deep Packet Inspection technique. It could have also been called "ISP-based behavioral advertising." Essentially, a user's Internet Service Provider allows an advertising network access to all of the user's activities. The advertising network thus learns all of the user's interests, by seeing the websites and other Internet services that the user patronizes. Then, using that information, the advertising network can direct ads to that user, directly targeting the user's interests suggested by his or her browsing activities. The ISPs and advertising providers obtain consent from ISP customers through various notices and agreements—though, of course, as with many such agreements, consumers do not read them and hence are not really aware of them.

Deep Packet Inspection (DPI) became the first face of the behavioral advertising industry to the public. And it was not a pretty face. As described in a decision in one of the after-the-fact class-action suits against a DPI provider, NebuAd:

> NebuAd contracted with Internet Service Providers ("ISPs") to install devices on their networks that monitored ISP subscribers' Internet activity and transmitted that data to NebuAd's California headquarters for analysis. That data was used to sell advertising tailored to subscribers' interests, which appeared in place of more generic advertisements on Web pages visited by subscribers. The advertising profits were split by NebuAd and its ISP partners.

Data collection under DPI most likely exceeded most Internet users' expectations. In Deep Packet Inspection, in contrast to first-party and third-party OBA discussed below, every aspect of the user's browsing activity is open to tracking, whether or not the visited sites have arrangements with ad networks, and whether or not the user has configured his settings to refuse cookies. Essentially, solely because a user obtains Internet access through a service provider that has contracted with an advertising network using DPI, every aspect of that user's Internet browsing activity would be examined, and used to produce targeted advertising. Consumer-advocacy organizations did not like DPI, nor did certain Congressional leaders, who critically examined it in late 2008 hearings. The practice ended soon thereafter.

In first-party online behavioral advertising, an Internet user who browses a trusted website

will, in the course of that browsing, be monitored through one or more "cookies." Cookies are data phrases that gather and save information about a user's preferences, so that different Web applications can tailor their information to those preferences. (Among other things, cookies allow users to save particular designs and content, to save and correctly place usernames and passwords, and to utilize "shopping cart" programs at e-commerce sites.) Cookies are central to most OBA. To take an oversimplified example, a user of a sports website who checks baseball scores and articles may prompt that website to post a cookie to the user's computer, recording that interest. The website then posts baseball-related ads to that user. That is basic first-party online behavioral advertising.

First-party OBA has been generally viewed as customary and acceptable. In its February 2009 report, the FTC staff defined OBA (i.e., the activities that it felt needed supervision and possible regulation) to exclude first-party behavioral advertising. The FTC staff noted that in first-party OBA no data are shared with any third parties, and it found the practice generally appropriate and permissible: "The staff agrees that firstparty behavioral advertising practices are more likely to be consistent with consumer expectations, and less likely to lead to consumer harm, than practices involving the sharing of data with third parties or across multiple websites."

Put simply, users generally are assumed to trust the websites they frequent, and to assume and understand that that trusted websites will monitor their activities, and websites try to post helpful content in response to the user's apparent interests.

Third-party online behavioral advertising is the step beyond first-party OBA. In third-party OBA, cookies are used to track Internet users across different sites. That is what makes third-party OBA different, and controversial. In third-party behavioral advertising, the suppliers of behavioral advertising (chiefly advertising networks) collect and use consumer information *across various websites* by placing "cookies" on user computers, and then generate ads in response to those cookies and what they know about the consumer identified by the cookies. As a consequence of information about a user's activities on website A, ads may be placed to that user weeks later, when he or she is visiting unaffiliated website B.

Ad networks place their behavioral ads based on information about particular users' browsing activities. More precisely, they use cookies to identify users with certain interests, as revealed by past browsing activity. In an example presented by the Center for Democracy and Technology, a consumer advocacy group that lobbies for privacy legislation, an ad network initially saw that a particular user visited a hotel review website (sf-hotel-review.com). The ad network placed a cookie on that user's computer. Then, as the consumer visited other websites (dog-zblogs.com and social-network.net), the ad network learned more about that user's interests, by tying that cookie to the visited websites. By the time the user visited the third website, the ad network was able to place a travel-related ad there, knowing that travel was one of the con-

sumer's interests. Although oversimplified, this example describes how advertising networks work—they take note of user interests as found on various websites, and they then arrange for posting of targeted ads when those users visit websites where the ad networks have contracts to place ads. The FTC has so far concluded that this kind of cookie-based behavioral advertising across unaffiliated websites should be subject to either government regulation or robust self-regulation.

The Digital Advertising Alliance, created by four advertising industry groups, has propounded detailed principles for industry self-regulation of OBA. The self-regulatory principles, based on an opt-out model, call for notifying consumers of third-party behavioral advertising practices through either in-ad notices or other notices placed on Web pages containing behavioral ads. A special trademark, a small "i" and triangle design, was created as the "Advertising Option Icon," to identify behavioral ads and where a consumer could click for more information and choices. After clicking on the Advertising Option Icon, or other notices, users would be given various ways that they could express their preferences as to what behavioral ads they wished to receive or not receive—for example, by completing forms on the aboutads.info website used by many ad networks. The program is regulated in part through decisions of the Advertising Self-Regulatory Council.

Mobile Device Data Privacy

The increasing use of mobile devices, including smartphones and tablets, has focused attention on some particular mobile device privacy issues. One important concern is how geolocation data are collected and used. Mobile devices send out various signals that allow their geographic location to be identified, and tied to particular communications or activities. Is that geolocation data just another form of data that can and should be collected and used freely, or does it carry particular sensitivity, such that it deserves special regulation and protection? The Federal Trade Commission has suggested that it should be presumptively considered sensitive, such that enhanced notices should be given, and possibly opt-in consent required, before it is collected and used.

Mobile devices also raise concerns about how fair and adequate notice about data collection and use practices can be given to users, particularly on small smartphone screens. It has been noted that often legal terms of use will take up scores, or even more than a hundred, screens full of text. It seems highly unlikely as a practical matter that any consumer will read and understand such lengthy disclosures thst are so difficult to access. The Commerce Department sought to address this problem in its first "multi-stakeholder" meetings, in 2012 and 2013, setting standards for disclosures on mobile devices. Although the industry group did draft and endorse a model set of summary disclosure forms, it remains unclear whether such forms can or will be followed (particularly considering the many different situations that often need to be addressed), and whether consumers really understand even the simplest and clearest stated disclosures.

Assessing Benefits of Data Collection and Use

Much of the data-privacy literature focuses on the potential perils of the database era. Privacy policy, however, is inherently about balance. Almost every aspect of modern civilization interferes with personal privacy to some extent— requirements for drivers' licenses, Social Security registration, license plates, filing of tax returns, disclosure of addresses and phone numbers, and even, in today's world, walking on the sidewalk in a city with surveillance cameras. The real privacy-policy question, in almost all cases, is not whether a privacy interest exists in a particular situation, but whether, in that situation, that privacy interest trumps the benefits of the use of the information.

Thus, the benefits of data collection need to be considered and put in the balance. In fact, there are many benefits of data collection to society, and even to the individuals from whom data are collected. Data collection for online behavioral advertising, for example, gives Internet users the benefit of receiving relevant, rather than irrelevant, ads, which studies not surprisingly show that consumers want.

Similarly, the perils of curbing data collection must be considered. For example, the creation of rights of "ownership" in personal information, as proposed by some privacy advocates, could interfere with basic freedom-of-expression rights. The "ownership" theory, often based on intellectual-property analogies and paradigms, is fundamentally flawed when applied to personal information, which in most cases has no economic value in isolation and is not maintained in secrecy or treated by its "owner" as valuable confidential property. Even focusing solely on the online world, where privacy interests are claimed to be most acute, a report of the Technology Policy Institute suggests that online collection of personal information may help provide consumers with useful information, support new services, and facilitate lower prices and/or differential pricing. Other industry sources claim that overregulation of data collection could impede mobile computing, cloud computing, and valuable statistical and predictive modeling.

Recognition of benefits in data collection and use will not necessarily mean that privacy interests cannot be addressed. But understanding of those benefits can help legislators achieve the right balance. In particular, it could influence the debate between the European model of privacy protection, which imposes blanket prohibitions on certain kinds of data processing, absent express consent (i.e., opt in), and the United States model, which generally allows collection on an opt-out basis, and focuses more on addressing the misuse of information that is collected.

Data-Privacy Policy Issues

As data-privacy rules are considered, many thorny issues will need to be addressed:

Who will set the rules? More specifically, will we rely on industry self-regulation, agency rules, congressional enactments, or some combination? Industry self-regulation would likely

provide more flexibility and room for techniques like OBA, but government regulation would likely give consumers stronger protections.

What data will be protected? While in the past there may have been a consensus as to what constituted "personally identifiable information" that needed protection, today even Internet identifiers, such as Internet protocol addresses, and geolocation data transmitted by mobile devices are sometimes claimed as personal data. How protected data is defined will have a big impact on new technologies. For example, if geolocation information is viewed as protected data, or as "sensitive" data deserving of enhanced protection, mobile marketing technologies may be stymied. If your location, transmitted by your mobile phone, is "sensitive" information, your cellphone company may not be able to direct you to the nearby restaurants and attractions that its advertisers operate.

Are notices effective? The underlying assumption of U.S. privacy law has long been that users deserve full notice about data collection and use practices, and the ability to make meaningful choices. But increasingly it is becoming clear that users do not pay attention to notices. Lengthy click-through notices on websites and electronic devices are hardly ever read— as some writers of such terms have proven by including absurd terms, such as the user's commitment to give up his or her firstborn child. Even simplified outline disclosures, meant to be easy to understand and act on, are rarely read. At some point, policymakers must push beyond the theoretical benefits of a notice-and-choice regime, and grapple with the practical utility of privacy notices.

How will data be protected? The traditional notice-and-choice model (seeking only to ensure that consumers were told how data would be used, and given choices about limiting uses) generally worked on an opt-out model. Many consumer advocacy groups seek a more restrictive opt-in model, which could significantly limit data collection and use, and thereby correspondingly limit commercial uses of data.

How broadly will the rules apply? Many data-regulation proposals would cover even data already publicly available, or data concerning individuals in their business capacities. Businesses, media, and academic and investigative researchers are likely to object to such coverage as overbroad and likely to limit customary and nonintrusive data usage. Particularly with business-to-business communications, protections drafted with business-to-*consumer* communications in mind may be inappropriate. Attendees at business trade shows, for example, generally desire to have their contact information shared with prospective suppliers and customers.

Who will enforce the rules? Here the choices range widely, from industry self-enforcement procedures (akin to those of the advertising industry's Advertising Self-Regulatory Council) to civil actions and class actions. Many class actions have already been asserted in data privacy cases, typically based on federal and California statutes and on contract claims derived from privacy policy promises. Several of the proposed bills take a middle-ground approach, committing enforcement to state attorneys

general and the Federal Trade Commission. The Obama White House and Commerce Department proposed a system of multi-stakeholder-developed Fair Information Principles tailored to each industry, in which case businesses that do not follow those standards could be prosecuted by the FTC for engaging in unfair trade practices.

How will aggregate and anonymized data be treated? Because of the usefulness of maintaining, analyzing, and using data, many entities collect and maintain data in aggregate or anonymized form, thereby protecting individual privacy while utilizing the data for business purposes. Because of recent studies concerning methods by which such data can be reconnected to individuals, however, even such data may end up falling under restrictive rules.

What kind of disclosures will be mandated? While most websites currently disclose their "privacy policies," current law requires only limited disclosures. Some privacy advocates charge that privacy policies are often too difficult for consumers to read and understand, and as a result have sought to require standardized or "plain English" privacy policies. Standardized policies, however, could prevent flexibility and impede use of new online business techniques.

Conclusion

New technologies intrude, but they also surprise. The dire warnings of privacy prophets in the 1960s could be, and were, long ignored because many of the concerns the authors predicted never materialized, or did so in ways different from what the authors predicted. Government surveillance clearly exists today, but not in the way that George Orwell predicted, and, in our post–9/11 world, it turns out that many U.S. citizens are more accepting of at least some government surveillance than one would have earlier expected. The intruding devices of earlier decades—tiny tape recorders, wiretapping, telephoto and night-vision lenses, parabolic microphones—are not the huge threat today many expected. Rather, today's unexpected privacy threats stem from the collection and use of data that people freely and knowingly create and post themselves, using the Internet, social media, and electro nic communications. Today's new electronic technologies—the Internet, mobile devices, electronic shopping and business transactions, the inter-connectedness of the world—have created so many efficiencies and benefits that those technologies have readily become well established in people's lives. Combatting the privacy risks in those new technologies, while maintaining their many benefits, will require sophistication and sensitivity.

Further Reading

Hemnes, Thomas. "The Ownership and Exploitation of Personal Identity in the New Media Age." John Marshall Review of Intellectual Property Law 12 (2012): 1.

Humbach, John A. "Privacy and the Right of Free Expression." First Amendment Law Review 11 (2012): 16.

Lenard, Thomas N., and Paul N.Rubin. "In Defense of Data: Information and the Costs of Privacy." Policy and Internet 2, no. 1 (2010).

Miller, Arthur. The Assault on Privacy. Ann Arbor: University of Michigan Press, 1971.

Narayanan, Arvind, and VitalyShmatikov. "Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)." IEEE Symposium on Security and Privacy , November 22, 2007. http://arxiv.org/PS_cache/cs/ pdf/0610/0610105v2.pdf.

Prosser, William L. "Privacy." California Law Review 48 (1960): 383.

Richards, Neil M. "Intellectual Privacy." Texas Law Review 87 (2008): 387.

Richards, Neil M. "Reconciling Data Privacy and the First Amendment." UCLA Law Review 52 (2004–2005): 1149.

Sableman, Mark. "'We Know What You Like': Online Behavioral Advertising and the New Focus on Data Privacy." St. Louis Bar Journal (Summer 2011).

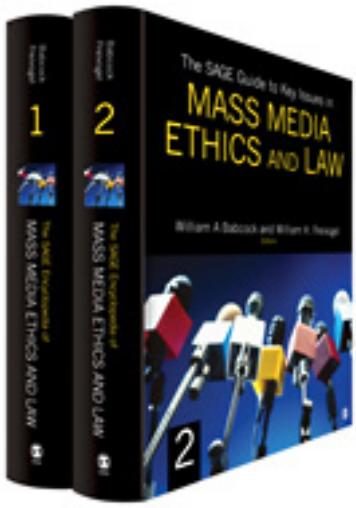
Sableman, Mark, Heather Shoenberger, and Esther Thorson. "Consumer Attitudes toward Relevant Online Behavioral Advertising: Crucial Evidence in the Data Privacy Debates." Media Law Resources Center Bulletin, International Media Law Developments: Reform, Regulations and Rebalancing (2013).

U.S. Department of Commerce Internet Task Force. Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (December 2010). http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internetecon-omy-dynamic-policy-framework.

U.S. Federal Trade Commission. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (December 1, 2010). http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

Westin, Alan. Databanks in a Free Society. Washington, DC: National Academy of Sciences, 1972.

Westin, Alan. Privacy and Freedom. New York: Bodley Head, 1967. http://dx.doi.org/10.4135/9781483346540.n30



Reprinted from

The SAGE Guide to Key Issues in Mass Media Ethics and Law

Edited by William A. Babcock and William H. Freivogel
Published May 2015.

Mark Sableman

Mark Sableman is a partner with Thompson Coburn LLP. He practices in intellectual property, media, and information technology law. He helps clients gather and publish news, build brands, fight infringement and false advertising, protect and use information technology, and conduct business in the online world. He has been listed in *The Best Lawyers in America*® since 1996 and is currently listed for Advertising, Copyright, Trademark and Media Law, and for First Amendment and Intellectual Property Litigation.

Chicago
55 East Monroe Street
37th Floor
Chicago, IL 60603
312.346.7500

Los Angeles
2029 Century Park East
19th Floor
Los Angeles, CA 90067
310.282.2500

St. Louis
One US Bank Plaza
St. Louis, MO 63101
314.552.6000

Southern Illinois
525 West Main Street
Belleville, IL 62220
618.277.4700

Washington, D.C.
1909 K Street, N.W.
Suite 600
Washington, D.C. 20006
202.585.6900

THOMPSON COBURN LLP

www.thompsoncoburn.com