
From the SelectedWorks of Jonathan I. Ezor

October 2013

Flawed Transparency: Shared Data Collection and Disclosure Challenges for Google Glass and Similar Technologies

Contact
Author

Start Your Own
SelectedWorks

Notify Me
of New Work



Available at: http://works.bepress.com/jonathan_ezor/11

Flawed Transparency: Shared Data Collection and Disclosure Challenges for Google Glass and Similar Technologies

Jonathan I. Ezor¹

Introduction: Privacy, Its Meanings, and the Role of Technology

Privacy is a term with multiple meanings, arising from culture as well as law. It may connote one's behavior or presence being unmonitored, one's identity being unknown, control over one's bodily integrity and health decisions, or merely being alone. In the business context, "privacy" generally refers to two major contexts: information about personal identity (often called "personally identifiable information" or "PII") and behavior. Control over privacy in these contexts indicates the ability to permit, or limit, the ability of another party to access, use or share data about one's identifying characteristics, and/or observe one's activities. Such control may arise from technical methodologies and tools, legal rights, or some combination of the two. Similarly, limitations of available technologies or laws can reduce the amount of control an individual has over these forms of privacy.

Law and technology have long been interconnected in privacy matters. Innovations as basic and ancient as clothing, the construction of wood and stone buildings, and even glass for windows have enabled their users to begin to control access by others to their identity and behavior, even while laws were established to limit the inquiries and monitoring.² At different points in history, depending on the culture and governing regime, individuals have had more or less legal control over their personal privacy, with technological advances from transportation to financial systems driving both the ability to

¹ Assistant Professor of Law and Director, Touro Law Center for Innovation in Business, Law and Technology.

² In one example, the medieval Jewish scholar Rabbi Shlomo Yitzchaki (known as Rashi), in his commentary on the biblical verse Numbers 24:2, notes that when the Jews wandering in the desert for 40 years established their communal camp, "the openings of their tents did not face each other, so that they should not peer into each other's tents." Numbers - Chapter 24 (Parshah Balak) - Tanakh Online - Torah - Bible, http://www.chabad.org/library/bible_cdo/showrashi/false/aid/9952/jewish/Chapter-24.htm#showrashi=true (last visited Oct 15, 2013).

be anonymous and the need to specifically identify people, especially as opportunities for mobility increased and commerce spread beyond local buyers and sellers.

In the nineteenth century, two broad developments significantly and permanently changed the state of privacy protection: the creation and promulgation of affordable, rapid/instant methods for communicating at a distance such as the telegraph and telephone and recording people's images and activities through photography. The combination of these technologies, along with the improvements in printing and duplication, enabled collection of information on people's identities and activities, and promulgation of that information, to an extent that had literally never been possible, and the law frequently struggled to keep up with the pace of innovation.

It was in this environment that Warren and Brandeis published their trailblazing Harvard Law Review article, "The Right to Privacy."³ Their analysis of how existing legal doctrine did not adequately protect those who were subject to unwanted monitoring and exposure of their activities, and the proposed framework that might add such protection, was explicitly inspired by the tabloid photography and publications made possible by then-new technologies. They write,

*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."*⁴

Indeed, since publication of that article, state legislatures and courts have either enacted or derived a variety of new rights and remedies designed to discourage and punish intrusions on people's solitude and activities.

Communication and imaging are not the only two technological areas impacting on the legal framework defining and protecting privacy. Medical treatments, from surgery to medication to contraception to abortion, have grown in effectiveness, affordability and

³ Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195-96 (1890).

⁴ *Id.* at 195 (notes omitted).

safety, raising new questions about rights of decision-making, autonomy and secrecy. Similarly, the creation and expansion of biometric identification methods, from fingerprints to retinas, voiceprints, and genetic material among others, continue to challenge law enforcement officials, legislators, scientists, ethicists and everyone who may be included within collections of biometric data.⁵

It is the paired development of computers and networking, though, that has had the most revolutionary effect on the ability of people to keep their identities and behavior free from unwanted monitoring, recording or dissemination. As data storage shifted to digital form, and standalone data repositories were networked first locally and then regionally and even internationally, issues of use, misuse and sharing, along with maintenance of integrity, became much more important. Consider a hypothetical collection of 1 million pages of customer transaction records of a major retailer such as Sears in 1950 and in 2013. In the earlier period, prior to Sears' purchase of its first mainframe computer in 1957,⁶ 1 million transaction records would require one or more warehouses to store them, the same number of warehouses to store a single copy of every record, days or weeks to make such a copy, and numerous trucks to move the copy to another location. If the company needed for some reason to review or alter every record, such a process would take even longer than merely copying them. In 2013, by contrast, the digital equivalent of the same million pages could be stored in a single gigabyte of available space on a hard drive or memory card,⁷ a copy of which could be transferred anywhere in the world over the Internet in a matter of minutes, and searching or altering each record could also be done in a few minutes depending on computer and memory read/write speed.

Just as the technology of the nineteenth century (as described by Warren and Brandeis) created the need for legal protection for privacy, so too did the move to digital information and transmission prompt attention from legislatures and regulators. In the

⁵ See, e.g., Whitehead Institute - News - 2013 - Scientists expose new vulnerabilities in the security of personal genetic information, <http://wi.mit.edu/news/archive/2013/scientists-expose-new-vulnerabilities-security-personal-genetic-information> (last visited Jul 25, 2013).

⁶ Sears Digital Archive - Timeline - Sears Chronology, <http://www.searsarchives.com/history/chronologies/detailed/1950s.htm> (last visited Oct 15, 2013).

⁷ Applied Discovery, HOW MANY PAGES IN A GIGABYTE (2007), http://cdn.ca9.uscourts.gov/datastore/library/2013/03/28/Cotterman_gigabyte.pdf.

United States, the initial efforts regarding digital privacy focused primarily on governmental data practices, including the U.S. Department of Health, Education and Welfare's (now Health & Human Services) very influential 1973 report on consumer privacy, *Records, Computers and the Rights of Citizens*,⁸ the Privacy Act of 1974⁹ (which addressed the permissible use by governmental bodies of collected personal data), and subsequent reports and regulations arising from the Privacy Act.¹⁰ The next major federal data privacy statute, the Electronic Communications Privacy Act of 1986 ("ECPA"), discusses both permissible and restricted use and sharing of personal data by governmental entities and private individuals and companies. ECPA actually includes three separate sections, each with its own subject matter and provisions: the Wiretap Act,¹¹ the Pen Register Statute,¹² and the Stored Communications Act.¹³ Together, the three portions of ECPA cover when and how electronic communications may be accessed by and shared with third parties both during and following transmission, and address both content and non-content elements within those communications. (Various states have adopted their own versions of ECPA, although the federal statute applies whenever communications involve "interstate commerce," and courts have read that requirement to be met whenever messages travel via the Internet even where both sender and recipient are in the same state.) The key word here is "communications:" ECPA does not apply to data that have not been transmitted through electronic wired or wireless networks.

Self-Regulation Best Practices: The Fair Information Practice Principles

It is crucial to note, however, that the United States has explicitly not adopted a general federal law protecting the overall privacy of personal information, although other

⁸ EPIC - Records, Computers and the Rights of Citizens, <https://epic.org/privacy/hew1973report/> (last visited Oct 16, 2013).

⁹ 5 U.S.C. § 552a, as amended.

¹⁰ See, e.g., ASPE, <http://aspe.hhs.gov/datacncl/privacy/#act> (last visited Oct 16, 2013).

¹¹ 18 U.S.C. §§2510-22.

¹² 18 U.S.C. §2701-11.

¹³ 18 U.S.C. §§3121-27.

jurisdictions throughout the world have done so.¹⁴ Instead, the primary method through which U.S. businesses are asked to respect and protect the privacy of customers' PII is self-regulation; that is, through their own voluntary efforts. It is generally only where the type of information is deemed sufficiently sensitive, or the population from which the information is obtained is particularly vulnerable, that Congress has enacted specific legislation mandating data privacy practices and agencies have promulgated regulations supporting the legislation.¹⁵

Self-regulation is not without standards and enforcement, even if it lacks formal legislative or regulatory requirements. Almost all self-regulatory structures for data privacy, whether adopted by individual organizations or through trade associations or other groups, follow similar guidelines for best practices, often called fair information practice principles or FIPPs. The Federal Trade Commission, the chief consumer protection agency for the federal government, included a concise discussion of FIPP in its 1998 report to Congress regarding online privacy:

Fair Information Practice Principles Generally

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. Notice/Awareness

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information. Moreover, three of the other principles discussed

¹⁴ For a discussion of the EU Data Protection Directive, the Canadian PIPEDA privacy laws, and others, see Chapter 9 of JONATHAN I. EZOR, *PRIVACY AND DATA PROTECTION IN BUSINESS: LAWS AND PRACTICES* (2012).

¹⁵ See at note 23 regarding specific privacy laws and regulations.

below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- *identification of the entity collecting the data;*
- *identification of the uses to which the data will be put;*
- *identification of any potential recipients of the data;*
- *the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);*
- *whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and*
- *the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.*

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data; whether the consumer has been given a right of access to the data; the ability of the consumer to contest inaccuracies; the availability of redress for violations of the practice code; and how such rights can be exercised.

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent. At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the

consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer. Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put. Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself -- i.e., to view the data in an entity's files -- and to contest that data's accuracy and completeness. Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data. Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them. Absent

an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.

a. Self-Regulation

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress). Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association; external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue. A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed. Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (e.g., correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer. Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation. The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, e.g., the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages; and the elements of any such cause of action.

c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers. Whether

*enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.*¹⁶

Other examples of FIPPs include the one included in the Obama administration's white paper on consumer privacy,¹⁷ those created by the Organisation [sic] for Economic Co-operation and Development ("OECD"),¹⁸ and the Code of Fair Information Practice published by the Government of South Australia in 2004.¹⁹

The key concept shared by all FIPPs, and in fact underlying the efficacy of the other elements of a FIPP, is informed consent. A user must not only be empowered to decide whether and how her personal information is used, but must do so with full knowledge of the proposed use. Without knowledge, consent is meaningless, access and participation are incomplete at best, and a user is unlikely to avail herself of redress without knowing how her data are being utilized in the first place. Best practices and enforcement bodies alike require that users be given clear and complete notice of planned personal information collection.

Self-Regulation in Action: The Privacy Policy

In a self-regulatory environment such as that of the United States, the process of notice most often takes the form of a disclosure statement known as a "privacy policy." The term "privacy policy" itself is somewhat misleading; while "policy" implies either aspirational goals or internal organizational matters, a "privacy policy" is more accurately defined as a statement of privacy-related *practices*. There is no single federal mandate for general consumer privacy disclosures, whether online or offline; instead, one may look to

¹⁶ FTC, PRIVACY ONLINE—A REPORT TO CONGRESS (1998), <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> at 7-11 (notes omitted).

¹⁷ Internet Privacy: Protecting Consumers, Building Trust, Creating Jobs | The White House, <http://www.whitehouse.gov/blog/2012/02/24/internet-privacy-protecting-consumers-building-trust-creating-jobs> (last visited Oct 16, 2013).

¹⁸ OECD Privacy Principles, <http://oecdprivacy.org/> (last visited Oct 16, 2013). As the OECD states in its introduction to its list of principles, "The OECD Privacy Principles tie closely to European Union (EU) member nations' data protection legislation (and cultural expectations), which implement the European Commission (EC) Data Protection Directive (Directive 95/46/EC), and other "EU-style" national privacy legislation. . . ." Accordingly, the categories and arrangement of the OECD principles are somewhat different from their U.S. counterparts, but the underlying ideas are essentially similar.

¹⁹ Government of South Australia, CODE OF FAIR INFORMATION PRACTICE (2004), <http://www.health.sa.gov.au/Portals/0/Health-Code-July04.pdf> (last visited Oct 16, 2013).

states such as California for a formal requirement to include a privacy-related disclosure in an online resource, and Pennsylvania for a prohibition on knowingly false statements in a privacy policy. The federal government, however, plays a significant role in the regulation of privacy policies even without formally requiring them in all circumstances by law, through its consumer protection power exercised primarily through the Federal Trade Commission (“FTC”).

The FTC obtains its authority and broad jurisdiction through its formational statute, the FTC Act.²⁰ More specifically, Section 5 of the FTC Act²¹ prohibits deceptive or misleading practices against consumers, and authorizes the FTC to take action against those who violate this prohibition. In the Internet age, the FTC has long seen this authorization to include oversight over personal data collection and use practices, and to both advocate for privacy best practices (i.e. those consistent with FIPP) and bring action against organizations whose disclosures were deemed deceptive or misleading or whose practices were otherwise harmful to consumers. The FTC’s advocacy includes reports to Congress, recommendations for specific legislative mandates where self-regulation was insufficient, and a broad range of business and consumer educational efforts. On the enforcement side, the FTC has brought numerous actions against both online and offline businesses over incomplete or inaccurate disclosures or even where information security was felt to be insufficient to protect consumers. That is, even when what the organization did not violate any specific provisions of a privacy or data security law or regulation, the FTC has nonetheless successfully exercised its broad Section 5 jurisdiction.²² In those contexts where there is specific legislation, the FTC, along with its sister agencies (both state and federal) with related jurisdiction, actively enforce violations of the law, in some instances gaining judgments or settlements of hundreds of thousands of dollars or more.²³

²⁰ 15 U.S.C. §41 et seq.

²¹ 15 U.S.C. §45.

²² For examples of the FTC’s general privacy enforcement, see Legal Resources | BCP Business Center, <http://business.ftc.gov/legal-resources/48/35> (last visited Oct 22, 2013).

²³ Examples of these include the Children’s Online Privacy Protection Act of 1998 (“COPPA”) (see Children’s Privacy | BCP Business Center, <http://www.business.ftc.gov/privacy-and-security/childrens-privacy> (last visited Oct 22, 2013)); the privacy and security rules enacted under the Health Insurance Portability and Accessibility Act of 1996 (“HIPAA”) (see Understanding Health Information Privacy, <http://www.hhs.gov/ocr/privacy/hipaa/understanding/> (last visited Oct 22, 2013)); and the financial privacy

New Capabilities and New Challenges

A common assumption underlying all of these areas of privacy enforcement, whether from laws and regulations focusing on specific subject matter or populations or general consumer protection, is that disclosure is both necessary and *possible*. A Web site includes a page with its privacy policy (and provides a readily viewed link to the policy), a bank sends an annual privacy notice by mail or e-mail, or a doctor or pharmacy hands its health privacy notice to new patients and customers. What about circumstances where the technology does not lend itself to clear, prominent disclosures? In recent years, the shifting of user interaction from larger-screen computers to smaller mobile devices (smartphones and tablets), and from standalone software (which can be accompanied by license agreements and privacy disclosure) to applications (or “apps”) instantly downloaded and installed via online marketplaces, have substantially reduced the screen space and interaction time to provide privacy disclosures, even while the devices and applications themselves offer more channels for collecting and using personal information. Regulators from the FTC to state attorneys general have held workshops and issued reports²⁴ on the privacy challenges of mobile devices and apps, and have also begun seeking agreements²⁵ and bringing enforcement actions,²⁶ especially where mobile privacy crosses over into areas such as children’s privacy.²⁷

Even in these areas, however, the underlying assumption is that the party collecting personal information has a direct relationship with, and can therefore communicate its

rules enacted under the Gramm-Leach-Bliley Act (Gramm-Leach-Bliley Act | BCP Business Center, <http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act> (last visited Oct 22, 2013).

²⁴ See, e.g., FTC Staff, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), <http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf> (last visited Oct 21, 2013); Kamala D. Harris, Attorney General, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (2013), http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (last visited Oct 21, 2013).

²⁵ Attorney General Kamala D. Harris Announces Expansion of California’s Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement | State of California - Department of Justice - Kamala D. Harris Attorney General, <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer> (last visited Oct 21, 2013).

²⁶ California AG sues Delta over mobile app privacy | Internet & Media - CNET News, http://news.cnet.com/8301-1023_3-57557701-93/california-ag-sues-delta-over-mobile-app-privacy/ (last visited Oct 21, 2013). Note that Delta ultimately won a dismissal of this case: Delta Wins Dismissal of California Mobile App Privacy Suit (1) - Businessweek, <http://www.businessweek.com/news/2013-05-09/delta-wins-dismissal-of-california-mobile-app-privacy-suit-1> (last visited Oct 21, 2013).

²⁷ Mobile Apps Developer Settles FTC Charges It Violated Children’s Privacy Rule, <http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm> (last visited Oct 21, 2013).

practices in some way to, the person from whom the information is collected. When that is not the case, though, the disclosure-driven model may fall short of the FIPP ideal, and new practices or legal obligations may need to be enacted to aid in privacy protection. One example of this is the collection by a company of personal and behavioral information from users across multiple Web sites and platforms the company does not own or control, through various technologies. Among the earliest method of cross-site data collection by non-site owners arose through the embedding of so-called cookie files, small text files automatically placed on a user's computer by a Web site the user accessed, and subsequently readable only by the party that placed the text file (and the user herself). Cookies were designed to enable easy recognition of repeat access by the same computer²⁸ to a given site without requiring the computer user to enter credentials each time, providing "state" information that the general architecture of the World Wide Web otherwise lacked.²⁹

As a technical matter, cookie files may be placed not only by the main Web page viewed by a user, but by other elements that may make up that Web page, including advertisements and other content delivered from third-party sources through links embedded in the main page's HTML code. Accordingly, companies that serve advertising across multiple sites could place and retrieve their cookies through their advertisements, allowing the advertising firms to develop a record of the Web browsing behavior of a particular computer:

The most important use of cookies however, and the most controversial, is to use cookies for tracking where you go and what you do there. These are typically used by advertising sites but you do not visit any of the advertising websites, so how can they get their cookies into your local storage? If you look at the cookies stored on your machine you will probably find cookies from DoubleClick, a site that tracks what ads you

²⁸ Cookie files are directly associated with devices connected to the Internet rather than the humans utilizing those devices, similar to the way traditional telephone numbers are associated with the equipment and will enable a call to be placed to whomever happens to be holding the telephone at the time. Even when additional data are combined with these device-matched identifiers to associate them to individual accounts, they still cannot serve as proof that the individual account holder was utilizing the device. A stolen laptop will maintain and offer up its owner's cookie files even when used by the thief, just as a lost cellphone will ring in the finder's hand when its number is dialed.

²⁹ Client-Side Storage, WORLD WIDE WEB CONSORTIUM, <http://www.w3.org/2001/tag/2010/09/ClientSideStorage.html> (last visited Oct 22, 2013).

*look at. This happens because a search engine you used has a relationship with DoubleClick and allows it to set cookies in your local storage. These are called third-party cookies. Another way that you can get third-party cookies on your client is from websites that show content gleaned from other sites. In such situations, the websites that provide the content may be able to set cookies on your machine.*³⁰

The power of third-party cookies to create cross-site profiles has drawn both legislative and enforcement attention, particularly when additional data sources could be used to add real names and addresses to otherwise anonymous cookie profiles. When advertising network DoubleClick (which had developed large repositories of cookie-driven anonymous user browsing profiles) sought to acquire offline marketing database company Abacus Direct, the acquisition was initially challenged out of concern DoubleClick would combine Abacus' existing databases and de-anonymize the DoubleClick tracked users; after the acquisition was approved and completed, the FTC investigated DoubleClick to ensure it was not doing so in violation of its public statements.³¹ User tracking remains of significant concern, especially as mobile devices proliferate, since they allow companies to track users not only across multiple devices, but to gather information including the user's location and travel history and even vehicle speed depending on the device used and its capabilities.³² As with other areas of technological capabilities impacting on consumer privacy, the FTC has taken an active role in making recommendations and proposing best practices for user tracking,³³ and has modified its COPPA regulations to incorporate the modern reality of third-party ad networks and tracking even on children-focused Web sites.³⁴ Additionally, members of the U.S. Congress are seriously considering enacting Do Not Track legislation.³⁵

³⁰ Id.

³¹ Federal Trade Commission, LETTER TO CHRISTINE VARNEY OF HOGAN & HARTSON RE: DOUBLECLICK INC. (2001), <http://www.ftc.gov/os/closings/staff/doubleclick.pdf> (last visited Oct 21, 2013). See also *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

³² See, e.g., Cellphones Track Your Every Move, and You May Not Even Know - NYTimes.com, , <http://www.nytimes.com/2011/03/26/business/media/26privacy.html> (last visited Oct 22, 2013).

³³ FTC Resources for Reporters: The Do Not Track Option: Giving Consumers a Choice, <http://www.ftc.gov/opa/reporter/privacy/donottrack.shtml> (last visited Oct 22, 2013).

³⁴ In its updated frequently-asked questions document for COPPA, the FTC writes:

Persistent identifiers were covered by the original Rule only where they were combined with individually identifiable information. Under the amended Rule, a persistent identifier is covered

Remote Information Collection and the Failure of the Disclosure Model

The limitations of relying on the informed consent model for privacy protection can best be seen in the growing number of contexts where there is no opportunity for consent between collector and information owner, because there is no real contact between them prior to the collection. Google, whose diverse business model centers upon the monetization of collected data (including user personal information and behavior data),³⁶ has developed or expanded a number of different offerings whose operation relies upon

where it can be used to recognize a user over time and across different websites or online services. Consistent with the above, operators need not seek parental consent for these newly-covered persistent identifiers if they were collected prior to the effective date of the Rule. However, if after the effective date of the amended Rule an operator continues to collect, or associates new information with, such a persistent identifier, such as information about a child's activities on its website or online service, this collection of information about the child's activities triggers COPPA. In this situation, the operator is required to obtain prior parental consent unless such collection falls under an exception, such as for support for the internal operations of the website or online service.

Complying with COPPA: Frequently Asked Questions | BCP Business Center, <http://business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions> (last visited Oct 22, 2013). The COPPA regulations may be found at 16 CFR Part 312.

³⁵ "Do not track" law needed for consumers, says Sen. Rockefeller - The Hill's Hillicon Valley, <http://thehill.com/blogs/hillicon-valley/technology/322779-do-not-track-legislation-needed-rockefeller-says> (last visited Oct 22, 2013).

³⁶ Google's self-described philosophy includes the following statements:

...Google is a business. The revenue we generate is derived from offering search technology to companies and from the sale of advertising displayed on our site and on other sites across the web. Hundreds of thousands of advertisers worldwide use AdWords to promote their products; hundreds of thousands of publishers take advantage of our AdSense program to deliver ads relevant to their site content....

Once we'd indexed more of the HTML pages on the Internet than any other search service, our engineers turned their attention to information that was not as readily accessible. Sometimes it was just a matter of integrating new databases into search, such as adding a phone number and address lookup and a business directory. Other efforts required a bit more creativity, like adding the ability to search news archives, patents, academic journals, billions of images and millions of books. And our researchers continue looking into ways to bring all the world's information to people seeking answers....

Even if you don't know exactly what you're looking for, finding an answer on the web is our problem, not yours. We try to anticipate needs not yet articulated by our global audience, and meet them with products and services that set new standards....

Ten things we know to be true – Company – Google, <https://www.google.com/about/company/philosophy/> (last visited Oct 22, 2013).

remote information collection without obtaining prior consent. Such activities have generated not only user concern, but legal exposure as well.

One area where Google has faced, and continues to face, legal challenges is in connection with its Google Street View technology, which embeds street-level photographs of locations throughout the world in Google's map and navigation products. Unlike Google Earth's satellite imagery, which Google licenses from third party vendors,³⁷ Google Street photos are taken by Google's own fleet of cars with mounted 360° panoramic cameras, which have been driven on "all seven continents."³⁸ Although Google promises "privacy" within Street View, including blurring license plates and faces,³⁹ Google cannot, and does not, obtain permission from any of the individuals whose images are captured by Street View cameras, sometimes resulting in awkward or embarrassing behavior memorialized for the world to see.⁴⁰ More troubling, however, was the revelation that, along with photographs, Google Street View cars were detecting and recording WiFi transmissions from wireless routers along their routes. Google claimed to be utilizing this information to support its enhanced location services (which enable mobile devices to approximately determine their location based upon a database of nearby known WiFi networks whose locations were previously recorded),⁴¹ but in lawsuits and investigations in the United States⁴² along with the U.K., Switzerland and elsewhere in the world,⁴³ there are allegations that Google also captured actual data traffic from the networks it detected, in potential violation of wiretapping and privacy laws.

³⁷ Understanding Google Earth imagery - Earth Help, <https://support.google.com/earth/answer/176147> (last visited Oct 22, 2013).

³⁸ About Street View – About – Google Maps, <http://www.google.com/maps/about/behind-the-scenes/streetview/> (last visited Oct 22, 2013).

³⁹ Privacy and Security – About – Google Maps, <http://www.google.com/maps/about/behind-the-scenes/streetview/privacy/> (last visited Oct 22, 2013).

⁴⁰ See, e.g., 36 Embarrassing Google Street View Sightings, <http://mashable.com/2013/06/10/google-street-view-embarrassing/> (last visited Oct 22, 2013).

⁴¹ Configure access points with Google Location Service - Google Maps Help, <https://support.google.com/maps/answer/1725632?hl=en> (last visited Oct 22, 2013).

⁴² See, e.g., *Joffe v. Google Inc.*, No. 11-17483 (9th Cir.) (Sept. 10, 2013), <http://cdn.ca9.uscourts.gov/datastore/opinions/2013/09/10/11-17483.pdf> (last visited Oct 22, 2013).

⁴³ EPIC - Investigations of Google Street View, <https://epic.org/privacy/streetview/> (last visited Oct 22, 2013).

Google has made no attempt to disguise or hide its Street View vehicles, which are prominently branded with the Google logo,⁴⁴ nor did it hide that it was directly collecting data using these vehicles; although Google did not seek prior consent, at least it was providing visual notice of its activities. By contrast, Google's recent foray into wearable computing, the Google Glass device, provides neither notice nor an opportunity to consent before it captures information about its surroundings. Instead, Glass has been specifically designed to be discreet, worn by its users as a futuristic-looking frame worn like eyeglasses, with a reflected display visible only to the wearer in the single lens-like screen. Users control Glass primarily through voice commands, and can capture still images or video, send messages, obtain translations, get information and directions and otherwise run specialized Glass apps, connected to the Internet via a wireless data connection.⁴⁵ The primary focus of privacy discussions around Glass has been its users' always-on cameras and other sensors, which could be recording inappropriate locations such as restrooms and private meetings, although other commentators have responded that Glass' capabilities mirror and in some cases lag behind those of modern smartphones (albeit with a greater ability to hide from casual notice). Those who interact with Glass-wearing users at least have the ability to ask what the Glass devices are recording, and express or deny consent for continued monitoring, and Glass users may refer to Google's terms of sale for Glass to learn what information Google is collecting from them.⁴⁶ In these details, the privacy issues for Glass' users and those around them are similar not only to smartphones, but other wearable recorders and vehicle-mounted cameras.

What remains uncertain, both practically and legally, is what information Google itself is collecting from its deployed Glass devices regarding the people and environments surrounding Glass wearers. As with Google Street View cars, Glass devices can detect and use WiFi networks,⁴⁷ and while Glass itself lacks GPS circuitry, it pairs with Android

⁴⁴ Google Street View car - CNET News, http://news.cnet.com/2300-1023_3-10016855.html (last visited Oct 22, 2013).

⁴⁵ Google Glass - What It Does, <http://www.google.com/glass/start/what-it-does/> (last visited Oct 22, 2013).

⁴⁶ Terms of Sale – Google Glass, <http://www.google.com/glass/terms/> (last visited Oct 22, 2013).

⁴⁷ Setting up Wifi - Google Glass Help, <https://support.google.com/glass/answer/2725950?hl=en> (last visited Oct 22, 2013).

phones to obtain location information.⁴⁸ Moreover, Google Glass' cameras can record and transmit images not only to the user's personal account but to Google overall; the company already offers sophisticated image recognition technologies⁴⁹ which could enable it to analyze and aggregate the visual record from Glass users throughout the world; the same could be true for audio, including speech recognition, which Glass already offers for its users.⁵⁰ Google is in the early stages of potentially seeding the world with cameras and microphones that can literally feed it information from anywhere Glass users can go, a scenario reflected in fiction in Dave Eggers' recently released book *The Circle*.⁵¹

⁴⁸ Setting up Glass - Google Glass Help, <https://support.google.com/glass/answer/3064121?hl=en> (last visited Oct 22, 2013).

⁴⁹ How Google's Image Recognition Works, <http://googlesystem.blogspot.com/2013/06/how-googles-image-recognition-works.html> (last visited Oct 22, 2013).

⁵⁰ Google Glass - What It Does, *supra* note 45.

⁵¹ DAVE EGGERS, *THE CIRCLE* (2013). The novel was excerpted by The New York Times Magazine, including this passage where Eamon Bailey, one of the senior executives in The Circle, a Google-like search and technology company, introduces a new product to his employees:

"Hello, everyone. My name is Eamon Bailey," he said, to another round of applause that he quickly discouraged. "Thank you. I'm so glad to see you all here. I know you're used to hearing from one of our engineers or developers, but today, for better or for worse, it's just me. For that I apologize in advance. But what I have to show you today, something we're calling SeeChange, I think it'll knock your socks off."

A screen descended behind him, and on it appeared a rugged coastline in perfect resolution. "O.K., this is live video of Stinson Beach. This is the surf right at this moment. Looks pretty good, right?"

...Now, many of you still aren't so impressed. As we all know, many machines can deliver high-res streaming video, and many of your tablets and phones can already support them. But there are a couple new aspects to all this. The first part is how we're getting this image. Would it surprise you to know that this crystal-clear image isn't coming from a big camera, but actually just one of these?"

He was holding a small device in his hand, the shape and size of a lollipop.

"This is a video camera, and this is the precise model that's getting this incredible image quality. Image quality that holds up to this kind of magnification. So that's the first great thing. We can now get high-def-quality resolution in a camera the size of a thumb. Well, a very big thumb. The second great thing is that, as you can see, this camera needs no wires. It's transmitting this image via satellite."

A round of applause shook the room.

"Wait. Did I say it runs on a lithium battery that lasts two years? No? Well it does. And we're a year away from an entirely solar-powered model, too. And it's waterproof, sandproof, windproof, animalproof, insectproof, everything-proof."

While other manufacturers are either working on or already releasing wearable devices to compete with Glass, Google's offering raises particularly challenging concerns given the multitude of other information channels through which Google collects user information, and the technological leadership Google has shown in analyzing and aggregating those data sources. At the same time, Google has disclosed little if any information about what data it may be collecting via Glass devices or how it might use those data; instead, Google links Glass privacy queries to its overall Google privacy policies, which do not provide any specifics about Google's own use of Glass-collected information. Additionally, whatever Google may disclose on its Web site, it is not doing so in the presence of those from and about whom it might be collecting information, and Glass' tiny, subtle form factor means that people are not necessarily otherwise on notice that Google data collection is taking place around them. It is also uncertain whether any direct collection of personal information by Google from children under the age of 13 could be a violation of COPPA unless it was preceded by verifiable parental consent.

A Proposed Solution: Privacy Certification for Wireless Devices

Given both the technological and practical realities of wearable, wirelessly connected devices, from Google or others, what might be the best approach to encourage and enable innovation while endeavoring to preserve the privacy of those into whose lives a wearable device user may come? In jurisdictions such as the United States where privacy is protected by a combination of self-regulation and specific laws, wearable devices may fall between the notice-driven assumptions of the former and the specific definitions and procedures of the latter. Even in those regions with more affirmative, formal requirements for all data collection and use, the existing laws may fail to properly

More applause overtook the hall.

“O.K., so, many of you are thinking, Well, this is just like closed-circuit TV crossed with streaming technology, satellites, all that. Fine. But as you know, to do this with extant technology would have been prohibitively expensive for the average person. But what if all this was accessible and affordable to anyone? My friends, we're looking at retailing these — in just a few months, mind you — at \$59 each.”

We Like You So Much and Want to Know You Better - NYTimes.com, ,
<http://www.nytimes.com/2013/09/29/magazine/dave-eggers-fiction.html> (last visited Oct 22, 2013).

account for the roles of the device manufacturer/seller and its wearer in the data collection process, and how to separate the collection by one from that by the other. Nor would prohibition of wearable device use be effective; given the ever-decreasing size of cameras and other sensors, the ubiquity of wireless connections and the multitude of available interfaces, users seeking a wearable experience can likely build their own, or purchase one whose use is easily hidden, just as drivers who wish to hide car-mounted radar detectors from police and thieves may use remote displays or even smartphone apps to interact with otherwise concealed detectors.

The best approach would be to provide both a platform and a mandate for companies like Google to more fully and publicly disclose their privacy practices with regard to wearable devices, with redress available for failure to do so (or to update the disclosure when practices change). Rather than create an entirely new legal regime, or to further seek to stretch the FTC's Article 5 or general similar consumer protection authority to impose such a mandate, the solution may lie in adapting an existing structure to which wearable wireless devices are already subject: the licensing and approval process for governmental bodies responsible for radio spectrum management, such as the U.S.' Federal Communications Commission ("FCC").

The FCC describes itself as follows:

The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. It was established by the Communications Act of 1934 and operates as an independent U.S. government agency overseen by Congress. The commission is committed to being a responsive, efficient and effective agency capable of facing the technological and economic opportunities of the new millennium. In its work, the agency seeks to capitalize on its competencies in:

- *Promoting competition, innovation, and investment in broadband services and facilities;*
- *Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution;*
- *Encouraging the highest and best use of spectrum domestically and internationally;*

- *Revising media regulations so that new technologies flourish alongside diversity and localism;*
- *Providing leadership in strengthening the defense of the nation's communications infrastructure.*⁵²

As part of its function, the FCC requires manufacturers of wireless devices to submit their devices for testing to ensure that they do not emit harmful electromagnetic radiation and that they comply with frequency allocation and other spectrum requirements. All smartphones, tablets and other computing devices with wireless radios of any kind must go through the FCC process, in parallel with similar processes in other countries, and Google Glass is no exception: the Google Glass Explorer Edition was submitted to the FCC in January 2013.⁵³ Separately, the FCC exercises jurisdiction over wireless carriers, including issues related to consumer information and privacy.⁵⁴ Google is not, however, a wireless carrier in general subject to FCC rules, and even if it is, the privacy jurisdiction does not crossover into data collected via other carriers.

The FCC could, however, potentially modify its wireless device certification procedures to require that device manufacturers seeking approval also provide privacy-related information, not just technical specifications, as a prerequisite for certification.

Companies like Google, that are both manufacturers and service providers, would be obligated to formally provide detailed information about their collection and use of personal information themselves or for their business partners through the devices they sought to bring to market, and to make that information available for public viewing. Any failure to fully disclose information practices, or to maintain an updated disclosure reflecting relevant changes, could subject the manufacturer to penalties or perhaps even cause loss of the right to sell the device, and could also serve as evidence in any other governmental or private legal action brought against the company for privacy violations. Those device manufacturers that were not also in the business of collecting personal

⁵² What We Do | FCC.gov, <https://www.fcc.gov/what-we-do> (last visited Oct 22, 2013).

⁵³ OET List Exhibits Report, https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=287362&typ=8374&fcc_id=A4R-X1 (last visited Oct 22, 2013), available via <http://ezor.org/fccglass>.

⁵⁴ FCC Votes to Apply Privacy Rules To Data Collected on Wireless Devices | Bloomberg BNA, <http://www.bna.com/fcc-votes-apply-n17179874845/> (last visited Oct 22, 2013).

information would avoid any disclosure burden or enforcement risk, and guidelines and enforcement could be modeled on the existing FCC privacy oversight or on FTC, SEC or other federal agency procedures.

Making this change to FCC processes, and adding privacy-related disclosures, could be done relatively quickly, through a notice and comment period during which consumers and manufacturers alike would have the opportunity to offer their views and make suggestions. If ultimately adopted, such an approach would significantly improve the ability of consumers other than those purchasing and using wearable devices to discover what information was being collected about them and by whom. It would also better empower advocacy groups and oversight bodies to verify whether companies were abusing the access their market power and technological expertise might provide to them. This approach would certainly not solve all the privacy issues, but it represents a practical method of addressing the gap between self-regulation and legislation into which wearable, networked devices like Google Glass currently falls.