VII. Surveillance Technologies and Economies

Introduction

Thus far this work has been concerned extensively with the way liberal democracies attempt to balance individual privacy with the need for collective security. Government collection of data on individuals, along with its ethical and legal underpinnings, has been our main concern. In Chapters V and VI, for example, we described surveillance technologies and systems increasingly used by governments for security purposes – passenger name records, data mining to create terrorist profiles and National Identity Cards to name a few. In those sections we touched briefly upon current, widely accepted modern communication and information systems, such as social networks that now result in unprecedented collection of data on individuals by the private sector, often through what is characterized as "participatory surveillance". Here we examine those systems, their use and their impact on individual privacy in more detail. Much of what we describe in this chapter applies more directly to the United States than to the European Union. This is no accident, because we believe that in many important respects the EU offers greater privacy protection than the US.[1] In other liberal democracies we have reviewed (see Appendix) the picture is somewhat mixed; speaking generally, there is a lack of privacy protection in the private sector. India, as noted above, has an implied right to privacy and is motivated to protect privacy and confidentiality in the private sector in part because of its large international IT outsourcing industry. However, in practice, self-regulation is the norm in the private sector. Australia's Privacy Act applies to private sector organizations as well as Australian government agencies. However, the Office of the Privacy Commissioner – the agency responsible for ensuring the Act is complied with – does not have the power to conduct audits of organizations in the private sector. Moreover, the Privacy Act does not cover businesses with less than AU$3 million annual turnover (that is, the majority of businesses in Australia).

During the first decade of the twenty-first century there has been an unprecedented rise in the collection, analysis and dissemination of information on individuals. As we have noted, privacy advocates and civil libertarians have long expressed concern over government-sponsored data acquisition and

1 This is not to idealize the EU. Compliance with EU directives has not been wholehearted, as individual member states have developed and implemented legislation in response to EU directives.

collection activities, which have increased markedly since 2001 as part of efforts to combat terrorism. Concern regarding government use of data is prompted by the fact that government has the ultimate power to limit freedom – it can prosecute. Thus, privacy regulation in the US often focuses on restricting the government's ability to collect and use personal data. Yet, as Garfinkel[2] and others[3,4] have pointed out for some time, in the US the greatest source of data on individuals is collected by the private sector, where it enjoys few constitutional or other statutory protections, often because this personal information is part of the public record or because individuals have been deemed to have consented to the release of their personal information as part of a transaction with another party.[5] Much of the current impetus for collection and analysis comes not from security needs but from commercial needs for information on consumers and consumer behavior in order to offer novel, attractive services, gain new efficiencies or develop new revenue sources. Increasingly, US government agencies, particularly law enforcement agencies such as the FBI, rely on major commercial data brokers such as Acxiom[6] or the Accurint division of LexisNexis[7] for both data collection and analysis.

Continued advances in computer storage and processing, computer networks and information retrieval methods have made possible a range of scalable internet-based services that provide numerous benefits to consumers, but these increasingly require the collection of personal information and its dissemination to numerous parties. The widespread acceptance of and now reliance on internet-based services such as social networking sites, web-based email and search engines, along with the gradual trend to make public and other records containing personal information readily available online, has dramatically increased the types of personal information available on individuals. Most importantly, these trends have significantly lowered the cost of obtaining that information. Moreover, we now live in what was billed in the 1990s as the age of "ubiquitous computing".[8] Networked digital technologies such as cell phones, surveillance cameras and other smart devices make possible constant data collection and surveillance systems that provide location and even detailed behavioral information. In the US, a highly effective industry for aggregating,

2 Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly Media, December 2000).

3 Daniel Solove and Chris J. Hoofnagle, "A Model Regime of Privacy Protection", *University of Illinois Law Review* 2006 (February, 2006): 357–404.

4 Ari Schwartz, written supplement to testimony before the Data Privacy and Integrity Committee, Department of Homeland Security, June 15, 2005. Available at: http://www.netdemocracyguide.net/testimony/20050718schwartz.pdf.

5 By contrast, consent needs to be explicit in the EU context.

6 Available at: http://www.acxiom.com/Pages/Home.aspx.

7 Available at: http://www.accurint.com/.

8 Mark Weiser coined the term "ubiquitous computing" for where computers are embedded in all types of devices and everyone interacts with them for their daily needs. See Mark Weiser, "The Computer for the Twenty-First Century", *Scientific American* (September 1991): 94–10.

analyzing and disseminating information on individuals is in place with the capability to search terabytes of both structured and unstructured data for relevant items.

Most will agree that the ability to share and discover information as well as communicate inexpensively on a worldwide scale offers tremendous opportunities to businesses, consumers and governments.[9] For example, the online availability of personal medical records improves health care by making records readily available for diagnosis, and can lower costs by eliminating unnecessary tests. Knowledge collections are now at our fingertips and not confined to obscure locations. Current internet-based systems provide a two-way communication channel between a service provider and a consumer. Thus, organizations such as retail chains, colleges and libraries can deliver highly personalized content to consumers, students and researchers that addresses their needs or interests.[10] The ability to search vast record collections and retrieve relevant information, a highly active and fruitful area of research in computer science, has allowed both individuals and organizations to utilize knowledge and research.[11] Indeed, many of the systems common today have created opportunities for productive work and socialization that would have been unimaginable fifteen years ago.

This study has been concerned with the significant risks that the release of personal information poses for individual well-being, autonomy and dignity. The systems upon which we now rely for much of our social and economic activity result in the unprecedented release of personal information and raise many questions (albeit somewhat different ones in the EU than in the US). What are the risks associated with just about anyone, including the government, being able to know just about anything about anybody for a nominal cost? As we have noted, many of the legal protections for individual liberties arose in an environment in which physical world restrictions on data limit the flow of information. Such restrictions gave rise to situations of privacy and expectations of privacy. Legal scholars are still unclear how these protections extend to the current era, where there are few practical constraints on the flow of data or what can be known and by whom. In the hope of gaining immediate benefits from internet-based systems, are we revealing too much personal information to too many different parties? Many claim that, in the new information age, information is never lost. What is the impact on individual well-being when possibly outdated information is still available and used to make decisions as to

9 Again, we focus here on the US context. Within the EU, personal data are to be kept and used only for the purposes for which they are originally collected, unless there is explicit consent by the data subject, subject to broad exceptions for government purposes.

10 There has, nevertheless, been concern about the way in which Google's personalizing of responses to research requests tends to confirm "detected" biases.

11 W. Fan, L. Wallace, S. Rich, and Z. Zhang, "Tapping the Power of Text Mining", *Communications of the ACM* 49, no. 9 (September 2006): 77–82.

a person's work ethic and employability? Moreover, how do individuals correct information that is incorrect if it is held in unknown data repositories and not tethered to any authoritative data source? A key feature of Web 2.0 systems is the ability for just about anyone to post information that then can be made available to anyone. How do systems in which anyone can publish information about anyone else and make it widely available impact human dignity?

Within the US, the focus has primarily been on the risks that government data collection pose for liberal democracies. However, as has been realized in the EU, aggressive collection of personal data in the private sector, along with advancing capabilities for data synthesis and analysis, now offer not only governments but unwanted others the opportunity to obtain information on individuals that was heretofore unavailable. In Chapter IV, we examined the Supreme Court decision in *United States v. White* that (in the US) severely limits Fourth Amendment protections for data provided to third parties.[12] In current, widely used internet-based systems such as social networks and search engines, third party data controllers typically obtain personal information through consent and terms-of-use agreements. The information is often no longer subject to the usual Fourth Amendment restrictions if sought by government as part of a criminal investigation. Often, law enforcement authorities can quickly obtain information on individuals from data controllers with a subpoena instead of a warrant, which requires authorities to demonstrate probable cause. In addition, restrictions on government collection of information do not apply to information that has been made publicly available – for example, information posted on a blog or personal website.

In the remainder of this chapter we examine recent technologies and organizational practices enabled by those technologies that make it very difficult – particularly in the US – for both individuals and organizations to control the exposure of sensitive personal information. Trends we examine include the following:

- Widespread acceptance and reliance on network-enabled digital devices and services to which users continually provide personal and often highly sensitive information.
- Organizational models and practices employed by service providers such as social networking sites, web-based email hosts, and other application service providers that require users to allow personal information to be made available to third parties.[13]
- Emergence in the US (but outlawed in the EU) of an efficient data aggregation and brokerage industry, with exceptional capabilities to gather, store,

12 The EU, as noted earlier, places much more stringent restrictions on third-party transmissions of data.

13 Broadly speaking, whereas the US has tended to favor opt-out models, the EU has mandated opt-in ones.

synthesize and make information on individuals, available for a range of specific purposes, e.g. targeted marketing, employment screening or law enforcement investigation.

- The inability of parties holding personal information to secure it properly (though increased legal liability would incentivize increased security).

We also comment on the impact that these trends are having on commonly accepted notions of privacy (focusing in this chapter largely on the US situation).

Technologies, organizational practices and information exposure

Today, an array of technologies – as well as business practices enabled by those technologies – allow aggregators to build a detailed personal profile of just about anyone. Recent advances in the knowledge-discovery technologies, data-clustering and link analyses now make it possible to group together related records in a transactional database of billions of records and establish connections among the groups. Thus it is often possible to find information on associations, relatives, past addresses and related items with little difficulty from large-scale transactional databases.[14] Furthermore, the continued development of information storage and retrieval systems, increasing levels of surveillance made possible by rapidly improving camera technologies, and the constant collection of personal information by third parties provide the information needed to establish a detailed picture of an individual that includes current interests, recent purchase history, recent whereabouts and health and financial information.

Peter Fleischer, global privacy counsel for Google, in an address to Google's employees characterized what Google considers to be the new reality concerning concepts of personal privacy.[15] Mr. Fleischer stated that historical concepts of privacy depended on forgetfulness, incompetence or laziness. Information was simply lost, or nobody bothered to find it. Mr. Fleischer claimed that those conditions have protected individual privacy for millennia. He further stated that we now live in a world in which we can remember everything and find everything. He conjectured that such an environment considerably changes expectations of privacy, especially those derived from a physical world in which information can become obscure. He further pointed out that the internet readily

14 The credit industry maintains a large-scale transactional database of credit applications that is mined using these techniques to detect fraudulent credit applications. See the report, "US Identity Fraud Rates by Geography", San Diego, CA: I.D. Analytics Inc. (February 2007).

15 Peter Fleischer, "Protecting Privacy on the Internet", December 19, 2007, available at http://www.youtube.com/watch?v=2IKBke1puFw.

allows data to cross national boundaries and that systems such as Google's cannot be architected to stop at an international border. He concluded, therefore, that having different privacy regimes in different countries is out of touch with the modern reality. He noted that, historically, in phone conversations there was a "sense of evanescence" to the conversation. However, with email and chat, data are stored by third parties and the data remain. He thus concluded that expectations of privacy must change.

(i) Social networking

In the past decade, social networking websites, which began as a niche phenomenon to support hobbies and other specific interests, have become for many the *de facto* mode of communication, especially among young adults and teens. Facebook, the current leading social networking site, reports that it now has 500 million active users worldwide, and that over 50% of active users log on to their Facebook account daily.[16] According to a recent Pew Internet study, internet usage among Americans is currently 93% for teens and young adults (ages 12–29), over 70% for adults (ages 30–64) and just under 40% for adults over sixty-five.[17] The study also reports that 73% of online teens and 47% of online adults now use social networking sites, a 50% increase during the last five years. Of those who have profiles, 73% have a profile on Facebook,[18] 48% have one on MySpace[19] and 14% have a LinkedIn[20] profile. Thus a significant portion of the American population uses social networking sites and most of their profiles are posted on one or more of the three top websites.

Given the growing reliance on social networks, there has been considerable research into the impact on privacy. Most information posted on the three major social network websites is associated with the user's real identity. In social networks such as Facebook, pseudonymity is discouraged through site usage norms and the need to provide a valid email address to register. Following usage norms, most users do provide a real identity, but as many have noted it is very easy to set up an account using a pseudonym.[21] When social networking first became popular, Facebook was considered a more secure environment than MySpace because a Facebook user was associated with a physical world

16 Facebook: pressroom statistics. Available at http://www.facebook.com/press/info.php?statistics.

17 Pew Internet and American Life Project, "Social Media & Mobile Internet Use Among Teens and Young Adults, Pew Research Center", Feb 3, 2010, available at: http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx. For country-by-country Facebook usage (including the EU), see: http://www.nickburcher.com/2009/07/latest-facebook-usage-statistics-by.html.

18 http://www.facebook.com.

19 http://www.myspace.com.

20 http://www.linkedin.com.

21 For this reason Japanese social network users patronize Gree or Mixi rather than Facebook. See Hiroko Tabuchi, "Facebook Wins Relatively Few Friends in Japan", *The New York Times*, January 9, 2011.

institution such as the user's high school or university. There was some expectation that information revealed would be limited to members whom the users knew from the offline world. Social networking sites allow users to define a group of friends who can view the user's profile information. Default settings will often expose the information posted to anyone associated with the user's institution, but users can opt to limit exposure to a group of friends and user-adjustable controls enable even finer-grained control of the information exposed. In many ways, Facebook and other social network sites give the impression that they offer an intimate setting in which friends can communicate and the privacy of the group is protected.

Gross and Acquisti have examined the potential for information revelation in social networks in which the use of a real account name is typically connected to an account profile.[22] They point out that the term "friends" used on a social networking website is quite different from the idea of a friend in the physical world. On a social networking site, a friend is determined by a binary setting, yes or no, while in the real world friends are associated with various degrees of trust. On a social networking site people are often included as friends even if the user does not know the person and has no established trust relationship. The number of a user's friends is much higher on a social networking site. Although physical world friendships typically number between fifteen and twenty, Gross and Acquisiti found that on a college campus in 2004 the average number of social networking friends was over sixty, all of whom enjoyed the same level of trust. Currently, the average US Facebook user has 130 friends.[23] The ease of joining and extending a friend network on most sites means that users must exert considerable effort to control the membership of the group. Research indicates that most users are apt to accept friends they do not know well as long as they do not have a previous dislike for the person.[24] Another difficulty is that the composition of the friends group changes over time. When friend groups start, they are often small groups in which the members are intimately acquainted. As the groups grow the relationships frequently become looser. Thus information intended for the smaller, original group can find its way to members of the larger group. In addition, users may find it difficult to limit the group by denying access to someone who requests membership. Social networking sites provide numerous incentives for prospective users to join the site and become a current member's friend.[25]

---

22 Ralph Gross and Alessandro Acquisti, "Information Revelation and Privacy in On-line Social Networks (The Facebook Case)", *Proceedings of the ACM Workshop on Privacy in Electronic Society (WPES)*, November 2005, available at: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

23 Facebook, Press Room, Statistics. Available at http://www.facebook.com/press/info.php?statistics.

24 Danah Boyd, "Friendster and Publicly Articulated Social Networking", Conference on Human Factors and Computing Systems, April 24–29, Vienna, Austria, 2004, available at: http://www.danah.org/papers/CHI2004Friendster.pdf.

25 Facebook's homepage presents a "find friends" option. Nonmembers can look for a member's name and are then offered an opportunity to register and join the current member's group of friends.

Leading privacy organizations and the Federal Trade Commission are increasingly scrutinizing Facebook's approach to privacy protection. The Electronic Frontier Foundation (EFF) has praised Facebook's recent decision to introduce privacy controls that allow users to restrict access to content on a per-post basis.[26] Users can limit access to a post to a particular subset of friends selected from a drop down menu. At the same time the EFF and other privacy organizations were highly critical of Facebook's default settings in a new privacy tool released in December 2009. In a complaint filed with the Federal Trade Commission[27] the EEF noted that the new settings give all Facebook users and possibly anyone on the internet access to a user's friend list, profile, photos, gender, geographic region and pages they favor. Previously only a user's name and network were available. The new settings were applied to all Facebook users, unless the user took the trouble to make the settings more restrictive.

Besides friends making personal information available, there are many other ways in which information propagates in a social networking site. In the US, the basic business model of a social networking site requires that information on users be made available to third parties for targeted marketing and other commercial purposes.[28] The importance of having unfettered access to user data is evidenced in the Facebook terms of use agreement:

> By posting User Content to any part of the Site, you automatically grant, and you represent and warrant that you have the right to grant, to the Company an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, publicly perform, publicly display, reformat, translate, excerpt (in whole or in part) and distribute such User Content for any purpose on or in connection with the Site or the promotion thereof, to prepare derivative works of, or incorporate into other works, such User Content, and to grant and authorize sublicenses of the foregoing. You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content.[29]

---

26 Electronic Frontier Foundation, ''Facebook's New Privacy Changes: The Good, the Bad and the Ugly'', December 9, 2009. Available at: http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.

27 In the Matter of Facebook, Complaint and Request for Injunction, Request for Investigation and Other Relief, before the Federal Trade Commission (December 17, 2010). Available at: http://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf. For the fallout from this, see: http://epic.org/privacy/inrefacebook/.

28 On November 9, 2009, an addition to the EU's e-privacy Directive, Directive on Privacy and Electronic Communications, 2002/58/EC, mandated an opt-in rather than opt-out requirement that included Facebook and other US-based social networking sites. Implementation has been lax, however. See: http://www.pcworld.com/businesscenter/article/235985/eu_orders_member_states_to_implement_cookie_law_or_else.html.

29 Taken from the term-of-user agreement available at: http://facebook.com/policy.php, February 7, 2007. This would almost certainly violate EU law.

Facebook also informs users that it collects information not only from what they post but also from newspapers, blogs, instant messaging services and other users of Facebook in order to provide a more personalized experience. Privacy settings on social network sites usually default to allow for as much information sharing among users and third parties in order to maximize the utility of user data. Chris Kelly, Facebook's privacy officer, noted that about 20% of Facebook's users reset privacy controls from their default values. Thus the vast majority of users do not.

Facebook allows third-party developers to write software programs that users can install on their Facebook sites to give the site various capabilities similar to those provided by java scripts used on websites. The top twenty-five Facebook applications (referred to as Apps) have about 5.5 million active users per month.[30] Most applications do not have a privacy policy and the Facebook terms-of-service agreement provides the following warning:

> ALL PLATFORM APPLICATIONS ARE PROVIDED AS IS [and that] YOU UNDERSTAND AND AGREE THAT YOU DOWNLOAD, INSTALL AND/OR USE ANY PLATFORM APPLICATIONS AT YOUR OWN DISCRETION AND RISK.

The *Washington Post* reports that the applications have become so popular that there are now venture capital firms devoted entirely to funding Facebook App development.[31] Felt and Evans[32] report that when a user installs a Facebook App under the default privacy settings, the App has access to all of the user's information even if it does not need it. The App can collect information and copy it to a third-party server, which may then use it for a targeted marketing campaign or other purposes. Once the information has been harvested, neither Facebook nor the user has any control over its use.

Rosenbloom examined why social networking site users are apt to post such intimate details of their personal lives in an environment in which they have so little control.[33] He states that the ''porous nature of the Net has radically redefined the arena in which individuals are willing to disclose personal information . . . the comfort zone is much larger and the circle of friends more broadly defined.'' At the time Rosenbloom was referring primarily to college students and those who grew up using the internet. However, this general

---

30 ReadWriteWeb, ''Does That Facebook App Have a Privacy Policy? Probably Not'', July 29, 2009. Available at: http://www.readwriteweb.com.

31 *The Washington Post*, ''A Flashy Facebook Page at a Cost to Privacy'', June 12, 2008.

32 A. Felt and D. Evans, ''Privacy Protection for Social Networking APIs'', presented at Web 2.0 Security and Privacy 2008, Oakland, Ca, May 22, 2008. Available at: http://www.eecs.berkeley.edu/~afelt/privacybyproxy.pdf. New EU laws have limited access, though not yet with full effect.

33 David Rosenblum, ''What Anyone Can Know: The Privacy Risks of Social Networking Sites'', *IEEE Security and Privacy* 5, no. 3 (May/June 2007): 40–49.

tendency appears in all groups who use the sites. Acquisti has noted that in using online systems users can seldom strike an adequate balance between the immediate benefit of providing information and the long-term risks of revealing it.[34] In addition, with the social network phenomenon there is the tremendous force of peer pressure to participate, as well as the confidence inspired by using a well-known website.

The impact of social networks on individual well-being is an open question. Given the inability to control who has access to information posted on a social networking website, it is important not to assume that privacy expectations in the physical world carry over to the world of social networking. James Rachels observed that privacy is valuable because it enables us to form varied and intimate relationships with other people.[35] This is precisely how social networking sites are used. However, the intimacy needed to protect communications within small groups is an illusion.

(ii) Highly dynamic systems

US businesses have long collected data on customers, but information on the activities of specific individuals was not the primary interest. When scanning devices were introduced into supermarkets and other stores in the early 1970s it became possible to collect detailed data on items being purchased, monitor inventory more effectively and reduce the costs of marking each item.[36] By 2006, the retailer Wal-mart had amassed a 586-terabyte data warehouse that included sales and inventory data.[37] Wal-mart records every item sold to every customer in every store on a daily basis. For most consumer goods purchased in retail outlets like Wal-mart, the retailer does not care exactly who bought what. Mass-market retailers are more concerned with questions such as how many tubes of a certain toothpaste were sold and what item was most often purchased with the toothpaste. Data analysis is often done to determine why certain goods may or may not be selling and how item placement can improve sales. Wal-mart claims to keep the data for only two years and also claims not to track the purchases of individual customers.

For over ten years companies like comScore Networks[38] have monitored the behavior of millions of internet users to gain insights into consumer behavior. Data are collected to try to spot trends in consumer purchases and interests.

---

34 Alessandro Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification", *Proceedings of the ACM Conference on Electronic Commerce*, 2004, 21–29.

35 James Rachels, "Why is Privacy Important", *Philosophy and Public Affairs* 4 (Summer, 1975): 323–33.

36 James Sinkula, "Status of Company Usage of Scanner Based Research", *Journal of the Academy of Marketing Science* 14 (1986): 63–71.

37 C. Babcock, "Data Data Everywhere", *Information Week Global CIO*, January 9, 2006.

38 comScore, Inc., http://www.comscore.com.

The company enlists about two million internet users (who are compensated) and claims that user privacy is protected. For most of the company's activities, individuals are not the main concern; general trends are. The company monitors users in order to assess the effectiveness of ad campaigns, the use of web sites and to develop detailed profiles of users who might be purchasing certain kinds of goods or visiting particular websites. comScore clients rely on the company's research to build customer profiles and target consumers based on those profiles. In this type of targeted advertising the user's recent behavior or contextual information is used to present targeted ads. Although this type of marketing has raised privacy concerns, an identity is not required and is typically not associated with a behavioral pattern.

What is dramatically changing the picture is a collection of technologies often referred to as highly dynamic systems (HDS) that allow personalized services and products to be delivered to a particular consumer.[39] Like the client server computing paradigm upon which e-commerce is based, HDS provide a one-to-one communication channel with a customer. Such systems are built with wireless technologies, sensor networks, RFID tags, smart cards, cell phones, surveillance systems, easy pass cards, surveillance cameras and internet-connected televisions. All these technologies are used to establish a one-to-one communication channel between customer and provider which enables the provider to deliver content appealing to the customer. Of course, the provider is constantly changing; many different entities have the opportunity to provide content and many different entities need access to personalized data. Often the user simply makes a selection and obtains a desired product or service. However, the more the provider knows about the individual on the other end of the channel, the more likely something appealing can be presented, for example, an ad the customer might click on, a movie the customer might download or a restaurant the consumer might visit if a location-enabled cell phone indicates that he or she is in a particular area.

HDS provide a host of opportunities to collect data. They frequently need both personal and contextual information (e.g. a person's current location or recent purchase history) to provide personalized services. Extensive and unobservable data collection is inherent in these systems and loss of control of the data collected is inevitable. An analysis of HDS summarizes the privacy issues for the US:

- data are collected without any indication;
- data collection takes place without a predefined purpose;
- data, once collected, persist in a variety of locations; and

39 K. Srikumar and B. Bashker, "Personalized Recommendations in E-commerce", *International Journal of Electronic Business* 3, no. 1 (2005): 4–27.

- different devices record multiple events simultaneously, leading to various possible interpretations of logged raw data and making the assignment of a valid privacy policy impossible.[40]

These systems certainly allow much finer levels of data collection. For example, an RFID tag in clothing and a surveillance camera in a store could be used to indicate your presence in a store, how much time you spent there and even (in the US) what aisles you visited.

Research suggests that most current privacy-enhancing technologies, which are based on concealing data, are not compatible with HDS. These systems typically involve continuous collection of data from multiple sources, usually for a variety of purposes. It is difficult, if not impossible, to build systems that would limit data collection at the source. Anonymity would prevent personalized services from being delivered. Pseudonymity would allow personalized services but would require the controlled release of personal data, which might impede personalization or limit the types of services that could be offered. Finally, data are frequently collected from so many different sources that it would be difficult, if not impossible, to guarantee that a real identity could not be discovered. Nonetheless, researchers are currently exploring techniques for developing privacy-policy-aware HDS collection devices in an effort to make "upfront notices of data collection" available to consumers.[41] Consumer privacy preferences would determine data collection parameters and consumers would be able to inspect their privacy state in a connected world.

(iii) Cell phones and targeted advertising

Cell phones provide unique opportunities to present customized content to consumers, but raise many privacy questions. A popular idea is to make banner ads appear when a user is close to a particular store or restaurant. Of course, now the user location must be tracked and revealed to a third party. In the US, companies are already developing browsers for cell phones that are location aware.[42]

The business model for most websites is click-through advertising. In other words, the website gains revenue when a visitor clicks on an ad displayed on the site. Google, for example, uses your search term to decide what ads to display in

40 S. Sackmann, J. Struker and R. Accorsi, "Personalization in Privacy-aware Highly Dynamic Systems", *Communications of the ACM* 49, no. 9 (September 2006): 32–38. Some of these issues are covered by the EU e-Privacy Directive.

41 Marc Langheinrich, "Personal Privacy in Ubiquitous Computing – Tools and System Support", PhD dissertation, ETH Zurich, Switzerland, May 2005. Available at: http://www.vs.inf.ethz.ch/res/papers/langheinrich-phd-2005.pdf.

42 Marin Perez, "Opera Add Locations Awareness", *Information Week*, March 9, 2009.

the hope of presenting something interesting and relevant that will elicit a click on the ad and perhaps a purchase. Thus there is tremendous incentive to know as much as possible in order to present highly relevant ads.

Cell phones and communications devices are ideal for targeted advertising because the content of the conversation or text message and the user's location can be used to determine relevant content. For example, a company called Pudding Media plans to offer extremely low-cost internet phone service.[43] Users have only to agree to have the content of their calls monitored. Essentially this is the same model that Google uses to provide targeted advertising to its Gmail users. Both companies claim that their systems target ads only contextually and do not employ any demographic or identity information in the process. Both claim that the content of the communications is not saved. In tests of the Pudding Media service, the company reports that the targeted ads presented often influence the content of the conversation, causing the participants to focus on the ads.

Both services exemplify a basic business model that pervades the modern internet – free or low-cost services are provided in exchange for access to personal information. Jonathan Sackett, chief digital officer for Arnold Worldwide, a unit of the advertising company Havas, summed up the current concerns of internet marketers: "Still, it makes me caution myself and caution all of us as marketers. We really have to look at the situation, because we're getting more intrusive with each passing technology."[44]

(iv) A sample of Web 2.0 technologies

Unlike the static pages of the early web, the Web 2.0 environment provides various mechanisms for uploading content to websites and making it available to a wide audience. One of the most successful websites to emerge in the Web 2.0 era (the past five years) is YouTube.[45] Originally started to foster the communication and sharing of musical ideas and techniques among musicians, the site rapidly expanded to include all types of video and is now the world's preeminent video sharing site. According to the internet research company Alexa,[46] YouTube is the world's third most popular website behind Google and Facebook. Google purchased YouTube, a company with only sixty-five employees, for 1.65 billion in Google stock in 2006.

YouTube videos can be uploaded by anyone who has a YouTube account, which requires only a valid email address. Videos can be made available to all on the

43 Louise Story, "Company Will Monitor Phone Calls to Tailor Ads", *The New York Times*, Sept. 24, 2007.
44 *Ibid*.
45 http://www.youtube.com.
46 Alexa, Top 500 Sites on the Web, http://www.alexa.com/topsites/global.

site or restricted to friends and family. Videos are usually followed by posts of texts from users who are either anonymous or frequently use pseudonyms. The uploader of a video can control whether posts are permitted or not and only the person who uploaded the video can remove it; others must appeal to YouTube.

Numerous privacy issues arise in relation to YouTube. The company does little monitoring of uploaded video; so almost anyone can upload just about any video. Copyright infringement has resulted in a major federal lawsuit against the company by Sony Viacom.[47] YouTube now has a department that routinely removes videos of copyrighted materials upon complaints from copyright holders. For others, the process of having an objectionable or harmful video removed can require considerable time, and there are frequent complaints that the company is unresponsive. Web 2.0 technologies scale only when any work to be done is spread over the user base not relegated to the site operator. In addition, YouTube collects the following information: each occasion on which a video is watched; the unique "login ID" of the user who watched it; the time at which the user started to watch the video; the Internet Protocol (IP) address and other information needed to identify the user's computer; and the identifier for the video. As with Google, this information is used to present targeted advertising each time the user logs into the site. In the *Viacom vs. YouTube* judgment, YouTube was ordered to release the logged information to Viacom for each Viacom video viewed.[48]

Privacy issues with YouTube also center on users uploading videos intended for only a small group of individuals but made available to anyone on the internet. Business organizations can suffer when the intimacy they require in conversations with clients or employees is compromised. A recent video involving the law firm of Cohen and Grigsby offers an example.

An extremely contentious practice, especially in the information technology industry, is the hiring of foreign workers on H1 visas. The Department of Labor (DOL) issues a permanent labor certification (PERM) to an employer that allows the employer to hire a foreign worker to work permanently in the US.[49] Among other requirements, the employer must demonstrate that there are no US workers with the appropriate skills available for the job at the prevailing wage. Cohen and Grigsby is a law firm that advises corporate clients on how to meet

---

47 Viacom Intern. Inc. v. YouTube Inc., 253 F.R.D. 256 (SDNY 2008*J*. However, the Southern District Court of New York (trial level court) granted summary judgment against Viacom and the case is currently on appeal before the Second Circuit, with the parties expecting that the fate of the appeal will turn on the Supreme Court's decision in Global-Tech Appliances v. SEB. See e.g. http://www.hollywoodreporter.com/thr-esq/how-an-obscure-supreme-court-207972.

48 However, YouTube's compliance was connected with its victory in a copyright suit by Viacom. See: http://www.zdnet.com/blog/btl/google-prevails-in-viacom-youtube-copyright-lawsuit-appeals-on-deck/36229.

49 United States Department of Labor, Permenant Labor Certification, available at http://www.foreignlaborcert.doleta.gov/perm.cfm.

the PERM requirements of DOL. In a frank presentation, firm representatives describe ways of placing want ads in newspapers in a manner that meet DOL requirements but which make the ads unlikely to attract qualified US applicants for the position. The firm obviously intended the presentation for current and prospective clients and certainly did not want the recorded sessions to be open to public viewing, where they would engender a wave of negative publicity and unwanted attention. Someone posted the recorded presentation on YouTube, where it was viewed over 155,000 times during the first week of posting. It attracted so much attention it eventually found its way onto CNN where it reached an even wider audience.

Data aggregators and processors[50]

During the past fifteen years a highly developed data brokerage industry has arisen that not only makes information on individuals available at relatively low cost but also can perform custom analyses of individuals or groups for various purposes, including law enforcement, employment background checks and targeted marketing campaigns. Companies such as ChoicePoint,[51] Acxiom and LexisNexis employ the latest algorithmic tools, along with computing power once reserved for large-scale scientific computation, to synthesize personal information from numerous sources and make a detailed profile of an individual available to either businesses or government. Due to the sensitivity of making personally identifiable information available to end consumers, these larger brokers today prefer to offer services only to larger, established businesses. Government agencies, particularly law enforcement agencies such as the FBI, are increasingly turning to these major data brokers for both data and analysis.

By 2005, largely through acquisitions of smaller data management companies, Acxiom, ChoicePoint and LexisNexis had grown to be the world's three largest aggregators and providers of data on individuals, each with annual revenues of over $1 billion. These organizations leveraged their significant analysis and processing capabilities, gleaned over many years of managing data for large corporate clients, to provide detailed information on and profiles of individuals to insurers, collection agencies, direct marketers, employment screeners and government agencies, including state and local law enforcement agencies. The website of Accurint,[52] the information subsidiary of LexisNexis, indicates the detailed information held and made available. For example, one product provided

50 It should be emphasized again that EU law prevents the existence of an industry as outlined in this section.

51 In 2008, Reed Elsevier, the parent company of LexisNexis, purchased ChoicePoint for $3.6 billion and merged it with LexisNexis.

52 Accurint, http://www.accurint.com/, last visited May 5, 2009.

by the company, People at Work, holds information on 132 million individuals including addresses, phone numbers and possible dates of employment. The site advertises the ability to find people, their relatives, associates and assets. In the next section we discuss some of the capabilities that data aggregators have for establishing detailed individual profiles.

Securing data repositories

To owners of large central repositories of valuable personal data, security is of paramount concern. However, given the large number of business partners and clients who require access to the data, protecting the sensitive information in these repositories is not an easy task. Large-scale breaches at both ChoicePoint and Acxiom earlier this decade generated a great deal of attention from privacy advocates and prompted calls for regulation of the activities of the data aggregation industry.[53] In May 2009, LexisNexis disclosed a breach that exposed the personal information of 40,000 individuals and compromised names, birthdates and social security numbers.[54] The breach appears to have taken place from June 2004 to October 2007. The company breach letter said the thieves, who were once legitimate LexisNexis customers, used mailboxes at commercial mail services and information taken from LexisNexis to set up about 300 fraudulent credit cards.[55] The breach letter indicated that LexisNexis learned of the breach from the United States Postal Inspection Service, which was investigating the fraudulent credit cards.

Other industries that maintain large central repositories of sensitive personal information are the retail and card payment processing industries. Each has suffered notable large-scale breaches during the past five years.[56] Unlike the data aggregation industry, breaches in these industries appear to have involved malware on servers that collected data and transmitted it outside the company. These breaches, however, also involved individuals with detailed insider knowledge of the systems that were compromised. Although the credit card industry and retail industries have not reported significant rises in the rates of credit card fraud,[57] the scope of recent payment card breaches, the rapidity with which stolen credit information has been used and the geographical

53 Solove and Hoofnagle, "A Model Regime of Privacy Protection".

54 Amy Westfeldt, "LexisNexis Warns 32,000 People about Data Breach", *San Francisco Chronicle*, May 1, 2009, 22.

55 LexisNexis Breach Notification Letter. Available at: http://privacy.wi.gov/databreaches/pdf/LexisNexisLetter050509.pdf, visited May 1, 2009.

56 Douglas Salane, "Are Large Scale Data Breaches Inevitable?", *Cyber Infrastructure Protection '09*, City University of New York, June 2009.

57 CyberSource Corporation, "Online Fraud Report: Online Payment Fraud Trends, Merchant Practices and Benchmarks", available at http://www.cybersource.com, visited May 1, 2009.

scope of the fraud raise concerns that data thieves are now taking advantage of the capabilities afforded by worldwide crime organizations to monetize vast collections of breached financial information. Loss by aggregators and data processors of sensitive personal data, especially financial data, poses significant risks to individual security.

Breaches in the data aggregation industry involved insiders such as contractors who extended their authorized access. Breaches in the payment processing industry made use of malware that relayed sensitive personal financial information to data thieves. However, regardless of the industry, basic privacy policies that (1) limit the amount of data collected, (2) limit where data are stored and the time for which they are stored and (3) restrict the use of data to the task for which they are collected play a critical role in preventing and mitigating breaches. Large-scale breaches are expensive, especially if the information lost involves sensitive personal financial data. Breaches in the payment industry can exact extremely high costs, particularly to organizations such as card processors, whose businesses depend on the trust of partners and customers. Breached notification laws, which keep both consumers and business partners aware of what is happening with their data, are changing the way all industries and organizations view information security.

Impact on basic notions of privacy

Modern information and communications systems are having a tremendous impact on basic, long-held notions of privacy. Although we offer an extended account of privacy in the next chapter, it is useful to relate some of the foregoing discussion to Alan Westin's differentiation of the four states of privacy: solitude, intimacy, anonymity and reserve.[58] In Chapter VI we examined the impact of recent securitization technologies on both intimacy and anonymity. Here is how modern information and communications systems can impact each of these states. Solitude is a state in which an individual is isolated and does not expect to be observed by others in any manner. Intimacy is the state in which an individual interacts with a small group and expects that his actions will be observed and limited to members of that group, for example, the interaction between spouses, among family members or among partners in a firm. Anonymity occurs when a person enters the public arena but surveillance does not result in identification. Thus the person has the freedom of action and expression that he or she might not have in other venues. The fourth state of privacy – reserve – may be the most important. Reserve is simply the ability to withhold information. We show reserve when we exercise discretion in the release of information, or in the

58 Alan Westin, *Privacy and Freedom* (New York Atheneum, 1967).

thoughts we convey, because these may be deemed either inappropriate for the occasion, offensive to another's sensibilities, to give an adversary an advantage or to have unknown, possibly negative, consequences. Yet Herman Tavani and James Moor think that privacy should not be defined in terms of what information individuals can control because they can control so little.[59] Instead, they stress that in order for individuals to have the freedom to function and prosper they must have the opportunity to limit access to personal information even if they do not have control of that information. Yet such privacy is an essential requirement for realizing the core values.[60]

The systems upon which we now rely for both business and social interactions can compromise each state of privacy. Analysis of a search history can reveal a person's innermost thoughts, fears, fantasies, aspirations or health concerns and thus undermine reserve. Online sites have replaced the usual meeting places for small groups, for example, the local tavern, club, mall or street corner. There is frequently a presumption that data posted or communications will be limited to a small circle of friends. Yet social networking site users cannot predict who will have access to their communications or how they will be used. For example, Pre-employ.com, an employment screening service, reports that in 2009 over 40% of employers obtained information on job candidates from social networking sites.[61] Although people have communicated online for years, prior to the social networking era they usually did so with a pseudonym, and data were held for only short periods. With current widely used systems a real identity is associated with a profile, and anything posted on major social networking sites may be archived indefinitely. As we have noted, most site owners state clearly in their terms-of-service agreements that the data may be used in any way the site deems reasonable. The situation is complicated by online privacy policies that are difficult to read, indicate little protection for personal data and are often considered to be simply legal disclaimers for protecting the site owner.[62] Furthermore, most terms-of-service agreements examined in this review indicate that information posted becomes part of the company's assets and, if the company is sold, those assets may be subject to a different privacy policy.

59 Herman T. Tavani and James H. Moor, "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies", *Computers and Society* 31, no. 1 (March 2001): 6–11.

60 James H. Moor, "Towards a Theory of Privacy in the Information Age", *Computers and Society* (September 1997): 27–32.

61 Pre-employ.com, "Background Checks and Social Networking Sites", February 24, 2009.

62 Irene Pollach, "What's Wrong with On-line Privacy Policies?", *Communications of the ACM* 50, no. 9 (September 2007): 103–108.

Protecting consumer privacy

In Chapter IX we examine the complexity of oversight and accountability, largely with regard to government sector surveillance. That section makes the point that, "as liberal writers from as far back as John Locke realized, good social order requires more than reliance on individual good will and good judgment. Structural supports and incentives are needed." Yet in determining how information is protected by those who control data in the modern internet, particularly social networks, search engines and sites that share information with third-party advertisers, there is exceptional reliance on the individual good will and judgment of the data controllers. Most users count on the data controllers to protect their information and not use it in a way that would cause them harm. A recent letter[63] to the US Committee on Commerce, Science and Transportation by a coalition of fifteen major American privacy and consumer groups representing millions of Americans notes that internet users face the following choice – "either stay off-line and ignore the benefits of new technology, or plug in and run extraordinary risks to privacy and security." The letter states that current privacy laws are inadequate and that self regulation has failed. The letter further states there is nothing in US law similar to the National Do Not Call Registry[64] to protect consumers from unwanted advertising and profiling by internet firms.

In the US, the Federal Trade Commission (FTC) is the primary government agency responsible for protecting consumers from harm that results from the collection and sharing of their personal information.[65] This role grew out of the FTC's longstanding mission as the enforcer of the Fair Credit Reporting Act, which mainly protects consumer credit information. Since the 1990s the FTC has increasingly concerned itself with privacy issues beyond the scope of consumer credit, with authorization derived primarily from specific sector statutes enacted during the past fifteen years and Section 5 of the FTC Act, which gives the commission authority to take action against deceptive or unfair trade practices.[66] For protecting consumer privacy outside of specific sector legislation the FTC relies heavily on Section 5 of the FTC Act, which allows it to bring actions against organizations that misrepresent the way in which they collect and use consumer information.

---

63 "Congress needs to act on privacy", Coalition Letter of Consumer and Privacy Orangizations, July 1, 2011. Available at http://epic.org/privacy/consumer/Privacy_Groups_to_US_Congress_final.pdf.

64 National Do Not Call Registry, https://www.donotcall.gov/default.aspx.

65 However, it should be noted that even if the FTC could enact and enforce a more rigorous privacy program (as suggested below) it would do nothing to regulate government intrusions. This is markedly different from what is happening in the EU, in which both the Commission and the European Data Supervisor are calling for an extension of data protection laws to policing and criminal justice as well as the private sector.

66 15. U.S.C. § 1681.

The FTC is in the process of conducting a thorough examination of its enforcement practices in the area of privacy protection.[67] Up to now the FTC has employed two approaches as guides to protecting consumer information: (1) the notice and choice approach; and (2) the harm-based approach. As part of the notice and choice approach the FTC has brought actions against organizations that engage in unfair and deceptive practices by using or collecting information in ways which violate stated privacy policies and terms-of-use agreements. Under the harm-based approach the FTC has taken action when organizations handle data in ways likely to cause physical or economic harm, or result in unwanted intrusions. The harm-based approach triggers FTC action when organizations fail to protect consumer information adequately, for example, by exposing consumer information that might result in economic loss through identity theft. Aside from the approaches being used as guides for enforcement actions, the FTC uses them to promote industry self-regulatory practices. The agency encourages organizations to put in place systems that inform consumers about privacy issues and give them the choice as to whether or not to release their personal information. The FTC also promotes industry practices that protect consumer data.

In its current review, the FTC has cited limitations with both approaches. It claims that the notice and choice approach is unworkable because typical privacy policies have now become long, complex documents that consumers cannot possibly read. The agency also notes that an increasing number of privacy policies are simply legal disclaimers. According to the FTC, the harm-based approach is too narrow as it limits harm to specific areas, often indicated by sector specific legislation. The approach does not address the wide array of harms that result from making sensitive personal information available to many different parties. The agency notes that it has little authority to address situations that lead to reputational harm, a common occurrence when, for example, social networks fail to regulate what users post regarding other users.[68] The agency can also do little when consumers agree to surveillance without being aware of the consequences. Overall, the FTC has relied extensively on promoting industry best practices as part of a self-regulatory approach to privacy. The FTC chairman, Jon Leibowitz, recently remarked, "Despite some good actors, self-regulation of privacy has not worked adequately and is not working adequately for American consumers."[69]

---

67 FTC Preliminary Staff Report, "Protecting Consumers in an Era of Rapid Change: Proposed Framework for Business and Policy Makers", December 2010, available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

68 Daniel J. Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007).

69 Edward Wyatt and Tanzina Vega, "FTC Honors Plan to Honor Privacy of Online Users", *The New York Times*, December 1, 2010.

In its attempt to protect consumers in the modern internet environment the FTC is largely trying to promote industry-wide practices that follow the Fair Information Practice Principles that it presented in 2000.[70] The FTC 2000 framework arose from classic work done at HEW in the early seventies to derive a general privacy framework.[71] The proposed new FTC framework emphasizes privacy by design, simplified choice and greater transparency, and embodies its Fair Information Practices Principles. In order to implement the framework in view of specific technologies and current business practices the FTC has sought input from consumer and industry groups through a series of roundtable meetings.[72] Although the FTC does not seek a legislative mandate for its new proposed framework, as part of its privacy by design initiative the agency has called for an effective and enforceable Do Not Track Tool that would give consumers the technical means to protect their online behavior from unwanted intrusion.[73]

In Chapter IV we discussed the dramatically different approaches to privacy protection in the US and EU and examined some of the cultural and historical factors that account for these differences. We noted that privacy protection in the US, unlike in the EU, is highly fragmentary and sector based. Often privacy legislation arises in response to a specific harm caused to consumers by existing data use practices. As we have noted, lack of an enforceable uniform privacy framework creates numerous gaps and results in a complex array of legislation to close the gaps. Although the public increasingly looks to the FTC to force organizations to protect consumer data, the agency does not have a broad legislative mandate for privacy protection. Given the rising consumer alarm over online privacy issues and the threat of increased legislative remedies, many organizations that provide internet-based services are now increasingly open to an overarching privacy framework. The FTC approach, however, still relies heavily on self-regulation to protect consumer data. Without a mandated framework to protect consumer privacy it appears that the FTC and Congress are in a never-ending game of plugging holes in a dyke as new harms surface that cannot be predicted in advance.

The FTC's recent reexamination of its consumer privacy protection policies provides additional impetus for a national data protection authority with a

---

70 FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace (2000)*, available at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

71 US Dept. of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973*), available at: http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

72 FTC Press Release, FTC to Host Public Roundtables to Address Evolving Privacy Issues (Sept. 15, 2009), available at: http://www.ftc.gov/opa/2009/09/privacyrt.shtm.

73 Testimony of David Vladeck, Director of the Bureau of Consumer Protection, Federal Trade Commission, before the Subcommittee on Commerce, Trade and Consumer Protection, US House of Representatives, Dec. 2, 2010, available at: http://www.ftc.gov/os/testimony/101202donottrack.pdf.

mandate to oversee privacy protection. Given the FTC's extensive history of privacy protection and current mandates through a range of legislation, the agency would certainly play a critical role in such an authority. We spoke earlier of a grassroots movement that could be a motivating force for a national data authority. Indeed, in response to widespread consumer outrage over the handling of sensitive personal data and the inability of organizations to secure it, a strong group of highly effective privacy advocacy organizations has arisen to represent consumer privacy interests. In addition, a number of industries now have an interest in a uniform privacy framework that would eliminate high compliance costs of a severely fragmented legislative regime of privacy protection. Without a uniform framework in place the nation faces continued proliferation of legislation and regulation, which makes oversight, enforcement and compliance extremely difficult and costly. The challenge is not only to put in place an adequate privacy protection framework but also to implement it in a way that provides adequate consumer protections and at the same time promotes innovation and development.