ACLU
AMERICAN CIVIL LIBERTIES UNION of OREGON
FOUNDATION

Do we still want privacy in the information age?

Marvin Gordon-Lickey

PROLOGUE

All those who can remember how we lived before 1970 can readily appreciate the many benefits we now enjoy that spring from the invention of digital computing. The computer and its offspring, the internet, have profoundly changed our lives. For the most part the changes have been for the better, and they have enhanced democracy. But we know from history that such large scale transformations in the way we live are bound to cause some collateral damage. And the computer revolution has been no exception. One particular casualty stands out starkly above the sea of benefits: we are in danger of losing our privacy. In the near future it will become technically possible for businesses, governments and other institutions to observe and record *all* the important details of our personal lives, our whereabouts, our buying habits, our income, our social and religious activities and our family life. It will be possible to track everyone, not just suspected criminals or terrorists. Even now, information about us is being detected, stored, sorted and analyzed by machine and on a vast scale at low cost. Information flows freely at light speed around the world. Spying is being automated. High tech scanners can see through our clothes, and we have to submit to an x-ray vision strip search every time we board an airplane. Although we have laws that are intended to protect us against invasion of privacy, the laws are antiquated and in most cases were written before the computer age. They are profoundly inadequate to restrain the new electronic methods of data archiving, data retrieval and data mining. The information technology industry is growing at breakneck speed. We have to ask, is it possible to benefit from information technology while at the same time preserving our privacy? Without privacy do we have freedom?

Privacy is dead -- Get over it.

About once every two years since 1994, the magazine *2600: The Hacker Quarterly* has sponsored a conference in New York City called HOPE (Hackers on Planet Earth).[1] A frequent participant at these conferences has been a private detective named Steven Rambam, who is owner and CEO of a successful private investigation company.[2] At several of these conventions Mr. Rambam has given a presentation titled "Privacy is Dead – Get Over It."[3, 4, 5, 6] In it he presents overwhelming evidence and examples of how it is possible to develop a detailed description of the private life of nearly any random person in the United States by sitting down at a computer and accessing databases that are open to the public. And he also points out that there is more detailed information stored in databases that are open only to licensed investigators or government agents. This method of investigation can be called *data mining*.

A case study: In 2006, Rambam recruited a volunteer "mystery man" who gave Rambam his first name, his email address and his phone number. From this meager starting point, Rambam retrieved from various databases an elaborate and detailed profile describing many aspects of the mystery man's private life. His full name was Rick Dakan. He lived in Florida. He was an author of several books. Rambam obtained numerous photographs of Dakan. He also acquired Dakan's social security number, his driver's license number, his mother's maiden name, the addresses of all the places that Dakan had ever lived, the purchase price and equity value of his current condo as well as other properties he had owned, the identity and cost of all the cars he had ever owned, where he parks his car, his telephone logs, the logs of the websites he has visited (including a porn site), the names of his friends (from Myspace), his complete educational history including colleges where he had enrolled but failed to graduate, his complete employment history, his credit history and ratings, all the loans that he had ever obtained, his court records (no convictions), the names and address of his parents, his political party affiliation, clubs that he belonged to, his special interests (cryptobiology) and hobbies (weightlifting, martial arts). Rambam also turned up the name and photograph of a scammer in Alabama who was fraudulently using Dakan's social security number. All this took only four and one-half hours in front of his computer.[7, 8, 9] And this was in 2006. Since then there has been a huge increase in the number of ways that personal information is being stored. Facebook was barely off the ground in 2006.

Should we "get over it"?

The lack of personal privacy illustrated by this story is shocking to many. But many others have gotten over it. A Gallup Poll conducted in January, 2011 found that many users of Google Search and Facebook were not at all concerned about losing personal privacy. For Facebook users, 35% were not at all concerned; for Google search, 48% were unconcerned.[10]

For example, I was recently talking about internet privacy with an adult member of my family, who I will call Jack. He said, "Privacy is really not a problem unless you're a criminal." Jack was stating his version of the "something to hide" argument,[11] which says that "Only people with something to hide need privacy." This argument has been famously expressed by Eric Schmidt, who was until recently the CEO of Google. In an interview on CNBC on 3-Dec-2009, Schmidt said "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." Then he added, "If you really need that kind of privacy, the reality is that search engines - including Google - do retain this information for some time and it's important, for example, that we are all subject in the United States to the Patriot Act, and it is possible that all that information could be made available to the authorities." Jack apparently does not perceive "the authorities" or the Patriot Act to be a threat to him.

Another relative, who I will call Fred, has also gotten over it. He gave me a sophisticated version of the "Hey, it's free" argument, to justify his tolerance for loss of privacy. This argument says that *it's unfair to benefit from a service without paying for it*. According to Fred, institutions like Google, Facebook and the US Government need information from you and everyone else in order to make their services work better. Your information helps them improve the algorithms and statistical tables they use to formulate policy, distribute information and protect our security. This in turn results in a better life for everyone. If you were to withhold your information and then continue benefiting from the better life that their services provide, you would be guilty of *free loading* on the backs of others who are not so secretive.

Stated in another way, Fred's argument is: All of us inevitably and involuntarily benefit from modern database technology. The benefits are both direct, as when we conduct a Google search, and indirect, as when we benefit from the collective improvement in economic efficiency that is brought about by the general availability of Google searching. Therefore we owe Google (or Amazon.com, or the government) the use of our personal information in order to avoid being free loaders.

The United States Census is an example of how the government collects information about us for the purpose of improving government services for everyone. In this case we are prohibited by law from denying our information to the Census Bureau.[12] Many government services are based directly on data collected by the census. To withhold your information would turn you into a free loader as well as degrade the government services that depend on representative sampling. Taxation is another example of this principle. It would be unfair for you to benefit from public goods like national defense, police protection, schools, roads, clean water, etc. unless you pay your share of the cost. You cannot refuse to benefit from these services, so you have to pay your taxes to avoid being a free loader.

Mark Zuckerberg, the creator, principal owner and CEO of Facebook, seems to have gotten over it. On his personal Facebook page Zuckerberg has listed "openness" and "information flow" as two of his five personal interests. (The other three were "making things", "eliminating desire", and "minimalism").[13] On his company's Facebook page it is stated that: "Facebook's mission is to give people the power to share and make the world more open and connected."[14] This statement apparently reflects Zuckerberg's personal values as well as his business goals.[15] In a televised interview published on November 7, 2011, Charlie Rose asked Zuckerberg about how he is managing to live with his fame and fortune; how he makes sure he is in command of it rather than it being in command of him. Zuckerberg replied:

> "I don't know…I spend a lot of time with my girlfriend and my dog…. We have a very open culture at the company where we foster a lot of interaction between not just me and people but between everyone else. It's an open floor plan. People have these desks where no one really has an office…Actually, it's really connected to the mission of the company. I think that more flow of information, the ability to stay connected to more people make people more effective as people. And I mean that's true socially. It makes you have more fun, right? It feels better to be more connected to all these people. You have a richer life….you just grow more when you get more people's perspectives… I mean, *I really try to live the mission of the company* [italics added]… and keep everything else in my life extremely simple." [16]

Zuckerberg's argument here is: "Openness is good for you." He implies that the benefits of transparency, as provided by Facebook, are greater than the benefits of privacy, which Facebook takes away. At several points in the Charlie Rose interview Zuckerberg denies that he is primarily trying to make money. Instead, he says, he wants to increase "openness" and do good. There is other evidence that Zuckerberg is not intensely motivated by large sums of money.[17] In 2006, Terry Semel, the former C.E.O. of Yahoo!, sought to buy Facebook from Zuckerberg for one billion dollars. Zuckerberg, about 22 years old at the time, turned down the offer. He said, "It's not about the price. This is my baby, and I want to keep running it, I want to keep growing it."[18] Semel commented, "I'd never met anyone—forget his age, twenty-two then or twenty-six now—I'd never met anyone who would walk away from a billion dollars." Tyler Winkelvoss, one of Zuckerberg's classmates at Harvard, later to become a competitor, said "He's the poorest rich person I've ever seen in my life."[19]

Jack may be sincere when he says "I have nothing to hide." Fred has a good point when he says "we have to do our fair share." Zuckerberg is not wrong when he says that "openness is good for you." However --and here is an important truth-- *openness requires trust*. The more people you are open with, the more people you must trust. As the saying goes, "Knowledge is power," and *knowledge about you is power over you*. In an ideal world we would trust everyone to use their power benevolently, as if all of us were each other's loving parent. In such a world we would have no worries about privacy or reputation.

But, alas, here on Earth we are confronted with competitors as well as teammates, enemies as well as friends. There are those who would steal from us, who are suspicious of us, who would profit from our loss, or who would take pleasure in our pain. If we give them unlimited information about us, we acquire the risk that they will use it. We need control over the kinds of information that different people have about us. What information would you entrust to your parents, your boss, your psychologist, your lawyer, the police, your child, your spouse, your ex-spouse? It would be either thoughtless or foolish to trust everyone unconditionally and equally. To have control over the flow of information about yourself is to have privacy.[20, 21]

Facebook, as a company, lives on the cusp between trust and fear. The company makes money when you trust it enough to reveal yourself, but it loses business when you get anxious and log off. Facebook, therefore, must strike the right balance between transparency and privacy. In general, the same is true for all companies that transact business in the digital cloud. Eric Schmidt has said, "If we [Google] violate the privacy of our users, they will leave us."[22] When you trust the cloud, you will use it. When you become anxious, you will fall back on less efficient but more trustworthy methods of communication. In order to make the right judgment about use of digital cloud, you need to be aware of all the ways in which your information can be disseminated and exploited. And in addition, you need the power to control where your information flows. Conversely, internet businesses must inspire trust in their customers by respecting personal privacy.[23]

Facebook has recently acknowledged the need for privacy. Zuckerberg defends his company by saying that Facebook, more than other companies, gives its clients the power to control who sees their personal information.[24, 25] A recent simplification in the way Facebook privacy settings work allows you to restrict access to a posting by clicking a button right next to your post. It is much easier now than in the past to specify that your posting will be visible only to yourself, your "family", your "friends", a specific list of people, or the general public. You can, in fact, change your mind and delete your Facebook posts. On Yahoo!, Amazon.com and most other companies you don't have this power. Note, however, when you make information about yourself accessible to your Facebook friends, your friends gain control of your information. They can pass it on to their friends or to the general public as they see fit. So you have to *trust* your friends to use your information benevolently. The take home lesson: Once your information is on someone else's website, someone else takes control of where it goes from there.

Information Technology Favors Transparency over Privacy

Social networks like Facebook and Linkedin are only a small part of the privacy landscape. To understand the big picture, we have to be clear about the capability and scope of modern information technology. The internet is an information sponge. It consists of a network of linked computers that pass information back and forth between each other. Together these computers have a truly massive capacity for information storage. This capacity grows by leaps and bounds every month. It is inherent in the way computers work that the information you enter is first securely stored. Then a program performs a series of logical operations on your data to achieve some objective. When the objective has been achieved, the data remain in storage. There is no necessity of deleting it. To delete it irreversibly requires extra programming effort and extra processor time.

For instance, if you send an e-mail message, your computer first stores your message. Then a program relays it via the internet to a second computer which immediately stores a copy of your message. The second computer then relays your message to a third computer which stores it, and so on, until your message finally arrives and is stored on the computer of the person you sent your message to. After your correspondent has read your message, she may delete it from her computer, she may keep it, or she may forward it to someone else. The various computers along the internet pathway are controlled by various unrelated people who work for various unrelated commercial or non-profit enterprises. None of these enterprises or individuals is strongly motivated to delete their copy of your message. At the whim of network administrators all along the line, your message can be placed on magnetic disks or other mass storage devices at very low cost. There it can sit for years waiting for a time when your information may be used by some other program for some other purpose. Your information may be sold to other enterprises who think they may have a use for it. It may be revealed by mistake. It may be stolen by a hacker. Or it may be handed over to the FBI.

A key feature of the information landscape is the database. A large pool of data stored in computer memory together with the software that is used to manage the data is called a database. A database can be analogized to a library. In a library there is a large store of books and there is a staff of librarians. The books are analogous to the large permanent store of information in a database, and the librarians are analogous to the software that manages the information. Database software has become very sophisticated in the past 30 years. Huge companies like the Oracle Corporation and IBM have made billions by producing database software and teaching companies how to use it. Organizations large and small, commercial and not-for-profit, all store their information with the help of this software. Databases have almost completely replaced file cabinets. Facebook is essentially a database operation that stores and organizes the personal data that its users provide. Phone companies scan all their old phone directories into databases so that you can look up phone numbers of people who lived in London in 1915.[26] The Church of Jesus Christ of Latter Day Saints has a project that aggregates birth and death records stored in courthouses and census records worldwide for the purpose of doing genealogical research.[27] Google Search is, of course, a database service, and it is an instructive example of how databases can be used to organize and retrieve information. Google is trying to create a giant database that contains digitized versions of all the books ever printed. However, this project has been stymied by complaints about copyright and antitrust violations.[28. 29] Nonetheless, Google plows ahead toward its ambition to be the company that knows everything and organizes it using database software. According to the company website, “Google’s mission is to organize the world‘s information and make it universally accessible and useful.”[30] Randall Stross, writing in the New York Times, quoted Eric Schmidt as saying, “When we talk about organizing all of the world’s information, we mean all.“[31] There is really no meaningful limit to the amount of information that can be entered, stored, organized, sorted, filtered and retrieved using electronic databases.

Your Web Footprint

In the course of living a normal life in the 21st Century, you create a “web footprint.”[32] In addition to the record of your past that is stored in your brain and in the brains of your friends, there is another record stored in cyberspace. Google (Gmail) and Yahoo! scan the content of your e-mails in order to find out what you are interested in. They use this information to send you ads for products that they think you might want to buy. For the same reason Amazon and eBay find it valuable to store information about the products you purchase, bid on or place on your wish list. They save the names and addresses of the friends you send gifts to making it easier for you to buy more gifts. Phone companies hold information about whom you have called and who has called you. There are records of your current and past whereabouts, minute to minute, as indicated by the stored records of the automatic communications between your cell phone and cell phone towers. Information about your whereabouts at particular times is also contained in the stored records from traffic cameras, automatic toll booth transactions, ATM transactions and credit card transactions.

Databases at Amazon.com contain the identity of the books that you have downloaded to your Kindle and the marginal notes that you have taken while you read. Google computers record your search terms, the addresses you locate on Google maps, the web pages you click on and how much time you spend on each page. With this information Google can infer your tastes and interests.[33] The same with Bing, Yahoo! and MapQuest. Insurance companies store records of your insurance claims. Banks and credit card companies have records of your financial transactions. Some of this information is passed on to the United States Treasury Department in Washington, D.C which maintains a database of financial transactions for the purpose of detecting illegal money laundering.[34]

Hospital and pharmaceutical databases contain detailed information about your health status. I was told by a psychiatrist that the notes she takes during sessions with patients are available to all of the medical personnel who have access to the medical records database of the health maintenance organization where she works. This is about 2,000 people locally and an unknown larger number at other affiliated hospitals in the Northwest.

Government databases contain information about your census status, real estate transactions, the value of the houses you have owned, your taxes, your social security records, your court records, your salary and retirement benefits if you are a public employee, your political party affiliation and the elections you have voted in. Who you have actually voted for is still secret, as of this writing.

All this information is your web footprint. It should really be called your web portrait. It contains more information about your life, than you can remember yourself. If this information had been collected by a live person by peeking through your windows, listening in on your phone, steaming open your mail, and sneaking into your house to rifle through your check book, you would be outraged. But your web foot print has been constructed by machine without your objection. There is no person to get mad at. The human spies and voyeurs can examine your web footprint at their leisure and at no risk to themselves.

Who wants to see your web footprint?

Information mined from web footprints is commercially valuable. One of the main uses of the information is for locating customers for commercial products. But it is valuable in many other ways as well. There are data aggregation companies, like Lexus/Nexus,[35] Acxiom,[36] Equifax,[37] that specialize in collecting information from all the databases they can gain access to. They then combine and organize the data into a mega database that seeks to contain, in one convenient location, all the information that anyone would ever want to know about any person in the world living or dead.[38, 39] As of January 1, 2012, Acxiom claimed to be "updating" 32 billion database records per month, managing 20 billion "customer and prospect" records, and "integrating" 4 billion records per day.[40] By "customer and prospect" they mean "person like you". By "updating" they mean adding new information about you to the information they already have. By "integrating" they mean "combining information about you from multiple databases." Acxiom then sells your information to various consumers. These include advertising agencies, personnel departments, lenders, and private investigators. Government agents can obtain your information by simply buying it, or if that doesn't work, by serving Acxiom with a legal document to demand it.

In 2001, following the terrorist attack in New York, the US Congress passed the USA Patriot Act. The full name of the act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001." [41] With this law the government gave itself the power to secretly access commercial databases in investigations involving national security without first obtaining a search warrant or other sanction by an open court. [42, 43, 44] Thus the FBI and other federal law enforcement authorities have acquired nearly unchecked access to the web footprint of anyone who they speculate might harbor information about a security threat.[45] The Patriot Act embodies great potential for abuse of power. The threat to privacy was well expressed recently by Senator Patrick Leahy of Vermont when he spoke before the U.S. Senate Judiciary Committee, Subcommittee on Privacy Technology and the Law in January, 2012: "I worry," he said, "that the availability of vast stores of information via corporate databanks … makes this information readily available to the Government, which has almost unfettered power to obtain information with an administrative subpoena and so-called national security letters. These are issued unilaterally, without any judicial check or warrant requirement beforehand."[45] Muslims beware![46]

You may think that there is little risk to you personally. Who, after all, would pay good money to find out about your personal life? You may think you are not a member of any unpopular group. You don't know any terrorists or terrorist sympathizers. To your knowledge, you have not materially contributed to a terrorist organization. Like Jack, you may feel you have "nothing to hide." But upon reflection, you will realize that the possibilities are endless. There are businesses who want to attract your attention to their products. Employers want to screen you for employment. Landlords want to evaluate you as a prospective tenant. Bankers want to check your credit worthiness. Identity thieves want to steal money from your bank account and buy stuff with your credit card. If you're in business, your competitors want to steal your trade secrets. If you're famous, journalists want to reveal your personal secrets. If you're in politics, your opponents want to embarrass you. Singles want to screen potential dates. Angry spouses want to catch their partners cheating. Rejected lovers want to stalk. Police agencies want to identify actual and potential perpetrators. In short, no matter who you are, there is someone out there who is interested in your information.

You may think that personal information in electronic databases is protected by security measures such as passwords and encryption. But this often is not true. A lot of the information is public, as demonstrated by the Rick Dakan example, and a lot of it is thoughtlessly made public by people themselves, as is the case with personal blogs, and posts to Facebook. Thus, a significant part of the threat to privacy arises not from breeches of secrecy, but from the sheer efficiency with which modern information technology can sense, retrieve and organize information that is publically available.[47] In 2006, Steven Rambam assembled a detailed dossier of Rick Dakon by spending four and one-half hours in front of his computer. In 1970 he could have achieved the same result, but it would have required a prohibitive amount of legwork, time and expense. During the oral arguments in a recent Supreme Court case[48] in which the court considered whether the police must get a warrant when they want to attach a GPS tracking device to a suspect's car, Justice Samuel Alito remarked "…in the pre-computer, pre-Internet age, much of the privacy – I would say most of the privacy – that people enjoyed was not the result of legal protections or constitutional protections. It was the result simply of the difficulty of traveling around and gathering up information."[49]

Encryption of data is secure when it is used. But using encryption requires that you spend extra time and effort. People don't bother with it for ordinary communications like e-mail. Even in cases where data are encrypted, such as bank records or government communications, there is always the possibility that a disgruntled employee might maliciously reveal it. The exposure of a quarter-million secret State Department cables is a famous example that occurred in 2010. In this case Bradley Manning, a dissenting intelligence analyst in the US Army, delivered copies of the secret cables to Julian Assange of Wikileaks. Wikileaks then passed the information on to several newspapers.[50] At the time of the leaks, Manning was emotionally distressed about issues related to his sexual orientation and the American war policy in Iraq. He regarded himself as a whistle blower. But this didn't protect him from facing a Court Martial, and he is likely to serve a long prison term.[51, 52]

Intrigue among insiders was at work in a case of unethical corporate spying at the Hewlett Packard Corporation in 2005 and 2006? In this case the Chairman of the Board of Directors was upset because she suspected that one or more of her colleagues on the board had leaked to the press some corporate information that she thought should have remained confidential. So she hired a private detective to obtain the personal cell phone records of the suspected board members. By impersonating the suspects, the detective was able to convince AT&T to send the suspect's cell phone records to his alleged e-mail address. The e-mail address linked to an anonymous proxy that could not be traced back to the detective.[53]

Data is frequently allowed to leak due to negligence or lax management. Between 2005 and 2009, multiple employees of the UCLA Health System were caught and fired for unwarranted snooping in the medical records of dozens of show business celebrities. An example is the case of Dr. Huping Zhou, a researcher who worked for the UCLA Health System. In 2003, he used his access to the database of the UCLA hospital system to snoop in the medical records of his lab supervisor and various show business celebrities who had been patients in UCLA hospitals. The later included Tom Hanks, Arnold Schwarzenegger and Drew Barrymore. Zhou ended up being convicted on four counts of violating privacy provisions of the Health Insurance Privacy and Accountability Act.[54, 55] Another UCLA employee filched information from Farah Fawcett's medical records and sold it to The National Enquirer. Other victims were Michael Jackson, Britney Spears and then California first lady Marie Shriver.[56]

In response to these invasions of patient privacy, the Department of Health and Human Services Office for Civil Rights brought a regulatory action against UCLA Health Services, and UCLAHS paid $865,500 in partial settlement. Other parts of the settlement included an agreement that UCLA would tighten up administrative policies pertaining to the protection of patient data, strengthen the enforcement of these policies, improve employee training regarding the sanctity patient records, and periodically report to HHS on the progress of their managerial improvement.[57]

But this legal reprimand was not enough to solve the problem. In September 2010, a burglar broke in to the home of a doctor who worked for the UCLA Health System and stole an external hard drive containing personal information relating to 16,288 patients. The doctor was working at home and he needed the records to carry out his work. The records were encrypted, but the encryption key was written on a piece of paper lying beside the hard drive. The paper disappeared along with the hard drive. Neither the drive nor the paper has been recovered.[58]

These examples show that your sphere of privacy, the sphere where you can control the flow of information about yourself, does not presently include your web footprint.

People Still Value Privacy

Since nearly everyone uses the web, a logical person might conclude that almost no one values personal privacy anymore. But this is not true, as illustrated by the experience of Elinor Mills of CNET News when she wrote an article about how Google and other web service providers were handling the issue of personal privacy in the course of their business.[59] In her article, Mills was not critical of Google. She pointed to items in Google's privacy policy that seemed to indicate that Google was making an effort to protect user privacy. But at the beginning of her article Mills recounts how she spent 30 minutes googling Eric Schmidt using Schmidt's own Google search engine. Schmidt was then the CEO of Google. She found his home address and his wife's name. She found that the Schmidts had attended a $10,000 a plate political fundraiser for Al Gore during Gore's campaign for president in 2000. At the fundraiser, Al and his wife Tipper danced while Elton John sang "Bennie and the Jets". She also found that Schmidt is an avid amateur pilot, and that he "…roamed the desert at the Burning Man Art Festival in Nevada."[60] This involuntary public exposure was apparently too much for Schmidt. After Mills' article appeared, the Google public relations officer called CNET's editor to complain about the exposure of private information and then in another call announced that Google personnel would be prohibited from speaking with any CNET reporter for a year.[61]

Mark Zuckerberg doesn't like involuntary public exposure either.[62] In November of 2007, Luke O'Brien, wrote an article about the early days of Facebook for the online magazine *02138* (now defunct). Included in the article was information about a court case, *ConnectU v. Facebook*[63] in which the owners of ConnectU accused Zuckerberg of using code that he had written under contract with ConnectU to create his own Facebook website. While researching the case, O'Brien examined various documents made available to him by the court. O'Brien went ahead and published some of the court documents as attachments to his article. Along with other information, these documents revealed Zuckerberg's social security number, the full name of his girlfriend, the address, names and telephone number of his parents, portions of Zuckerberg's online personal diary, and his application for admission to Harvard. Immediately Zuckerberg, acting through his Facebook legal team, petitioned the court to take down these leaked court documents, which, according to Facebook, should have been sealed and unavailable to the public. The judge, however, ruled against Zuckerberg, saying that the public had the right to know. In any case the sensitive information had already been copied and passed around the web, so it would have been impossible to re-privatize it.[64, 65]

EPILOGUE

The take-home lesson is: Even Mark Zuckerberg and Eric Schmidt have something to hide. No one is a saint. In anyone's web footprint, there may be found embarrassing incidents, perhaps even evidence of minor crimes. Also, some of the information in your web footprint is bound to be erroneous, and you usually have no way to make corrections. If you are like most people, you would not voluntarily allow a government agent, or even a spouse, to snoop freely through your web footprint. We all assume and expect that the details of our private lives are not going to be publicized for all the world to see. In the private sphere of life, which is not concerned with public affairs, people have an *expectation of privacy.* When information from this private sphere is exposed and publicized against our will, we call it an *invasion of privacy,* and we regard it as unfair, inappropriate, a violation of our dignity and maybe illegal.

The new technology for cheap storage and manipulation of data is a spectacular development of human culture. Its potential for changing our lives is very great, perhaps as great as the invention of machine power about two and one-half centuries ago. The new technology has many obvious benefits. But there are also harms. There has already been significant loss of privacy. How much further will this process go? How will it change the way we are governed and policed? In the future, will we have to worry about who is reading our e-mail, who knows how much money we have on the books, who knows what we have said to our psychiatrist, who knows what political party we support. Worries like these are the burdens of tyranny. Their absence is what we call liberty. But we can't go back to file cabinets and library card files. Our only alternative in the information age is to seek ways to limit the harms while preserving the benefits of information technology. We must think seriously and carefully about how the information industry can be regulated to promote democracy and freedom.

Acknowledgments

This paper was prepared under the umbrella of the Education Committee of the ACLU of Oregon. The author thanks committee members Laura Berg, Barbara Gordon-Lickey, Stuart Kaplan, Candace Morgan, and Bobbin Singh for many helpful suggestions, comments and corrections. Any errors of commission or omission are strictly the responsibility of the author.

References

1 *2600 The Hacker Quarterly Website*, 2012.

2 *Pallorium, Inc. Website*, 2012.

3 Steven Rambam, "Privacy Is Dead - Get Over It", *ToorCon.org Information Security Conference*, 09/30/2006.

4 Steven Rambam, "Privacy is Dead -- Get over It", *HOPE2604*, July, 2008.

5 Steven Rambam, "Privacy is Dead -- Get Over It (Part 1)", *Vimeo.com*, 07/06/2010.

6 Polly Springer, "Sun on Privacy: 'Get Over It'", *Wired.com*, 01/26/1999. The quote, "You have zero privacy anyway. Get over it" originated with Scott McCleary of Sun Microsystems in 1999 during a press conference in which McCleary was introducing a new of Sun product.

7 Steven Rambam, "Privacy Is Dead - Get Over It", *ToorCon.org Information Security Conference,* 09/30/2006.

8 Steven Rambam, "Privacy is Dead -- Get over It", *HOPE2604*, July, 2008.

9 Steven Rambam, "Privacy is Dead -- Get Over It (Part 1)", *Vimeo.com*, 07/06/2010.

10 Lymari Morales, "Google and Facebook Users Skew Young, Affluent, and Educated", *Gallup website*, 02/17/2011

11 Daniel J. Solove, *Nothing To Hide*, 2011, Yale University Press, New Haven.

12 U.S. Census Bureau, "Frequently Asked Questions: Do I have to respond to the American Community Survey / Puerto Rico Community Survey?", December, 2012, *US Census Bureau website*.

13 Mark Zuckerberg, *Mark Zuckerberg Facebook Page*, November, 2012.

14 Facebook, "Facebook Mission Statement", *Facebook website*, 01/30/2012.

15 Jose Antonio Vargas, "Letter from Palo Alto: The Face of Facebook", *the New Yorker*, 09/10/2010.

16 Charlie Rose, "Mark Zuckerberg & Sheryl Sandberg on 'Charlie Rose' (full transcript)", *venturebeat.com*, 11/07/2011.

17 Jose Antonio Vargas, "Letter from Palo Alto: The Face of Facebook", *the New Yorker*, 09/10/2010.

18 Jose Antonio Vargas, "Letter from Palo Alto: The Face of Facebook", *the New Yorker*, 09/10/2010.

19 Jose Antonio Vargas, "Letter from Palo Alto: The Face of Facebook", *the New Yorker*, 09/10/2010.

20 Judith DeCew, "Privacy, *the Stanford Encyclopedia of Philosophy (fall 2008 edition)*, Edward N. Zalta (ed.), 2008.

21 Yael Onn et al., "Privacy in the Digital Environment", Niva Elkin-Koren and Michael Birnhack, eds., Haifa Center of Law & Technology, 2005.

22 Ken Auletta, *Googled: The end of the world as we know it*, Penguin, New York, 2009, p 198.

23 Ozer, Nicole A., "Privacy and Free Speech: It's Good for Business", *dotrights.org*, February, 2009.

24 Ryan Singel, "Mark Zuckerberg: 'I Donated to Open Source' Facebook Competitor", *Wired.com*, 05/28/2010.

25 Mark Zuckerberg, “Our Commitment to the Facebook Community”, *the Facebook Blog*, 11/29/2011

26 Steven Rambam, “Privacy is Dead -- Get over It”, *HOPE2604*, July, 2008.

27 Church of Jesus Christ of Latter Day Saints, “FamilySearch”, FamilySearch.org, 2008

28 Ken Auletta, *Googled: The end of the world as we know it*, Penguin, New York, 2009, pp 123-128.

29 Grant McCool, Dian Baertz, Richard Chang, Andre Grenon, “Judge slaps down Google's digital library settlement”, Reuters, 03/22/2012

30 Google, Google website, 01/18/2012

31 Randall Stross, ‘Google Anything, So Long as It's Not Google”, *New York Times*, 08/28/2005.

32 Mike Francis, “In 21st Century America, privacy, truly, is gone”, *The Oregonian*, 10/30/2011.

33 Ken Auletta, Googled: The end of the world as we know it, Penguin, New York, 2009.

34 Financial Crimes Enforcement Network, *fincen.gov*, 02/13/2012.

35 LexisNexis, *lexisnexis.com*, 2012.

36 Acxiom, “About Axciom”, *acxiom.com*, 01/31/2012.

37 Equifax, “About Equifax”, Equifax.com, 01/31/2012

38 Jay Stanley, “The Surveillance-Industrial complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society”, *aclu.org,* ACLU, 8/2004.

39 Steven Rambam, “Privacy Is Dead - Get Over It, *ToorCon.org Information Security Conference,* 09/30/2006.

40 Acxiom Corporation, About Axciom, acxiom.com, 01/31/2012.

41 United States Congress, “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and obstruct Terrorism (USA Patriot Act) Act of 2001”, US Govt. Printing Office, 10/26/2001.

42 United States Department of Justice, “Highlights of the USA Patriot Act”, *Justice.gov*, 2012

43 Electronic Frontiers Foundation, “EFF Analysis of the Provisions of the USA Patriot Act”, *w2.eff.org.* 2003.

44 Michael German and Michelle Richardson, “Reclaiming Patriotism: A Call to Reconsider the Patriot Act”, *aclu.org*, 2009.

45 Jay Stanley, The Surveillance-Industrial complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society, ACLU, 8//2004.

45.1 Patrick Leahy, Statement before The Senate Committee On The Judiciary, Subcommittee On Privacy, Technology And The Law Hearing On “The Video Privacy Protection Act: Protecting Viewer Privacy In The 21st Century”, January 31, 2012.

46 Chris Hawley, “NYPD monitored Muslim students all over northeast”, *Associated Press*, 02/18/2012.

47 Solove, Daniel J., *Nothing to Hide*, 2011, Yale University Press, New Haven, Chapter 10.

48 Supreme Court of the United States, “United States v. Jones Number 10-1259”, *supremecourt.gov*, 01/23/2012.

49 Supreme Court of the United States, “United States vs Antoine Jones No. 10 - 1259 Oral Argument”, *supremecourt.gov*, 11/8/2011.

50 Scott Shane and Andrew Lehren, Andrew, “Leaked cables offer raw look at U.S. Diplomacy”, *New York Times*, 11/28/2010.

[51] David Dishneau - The Associated Press, “Army Rules Manning Will Face Court Martial”, *Army Times*, 02/03/2012.

[52] New York Times, “Times Topics: Bradley E. Manning”, *topics.newyorktimes.com*, 02/19/2012.

[53] David A. Kaplan, “Suspicions and Spies in Silicon Valley”, *Newsweek*, 09/17/2006.

[54] U.S. Attorney’s Office, District of California, “Ex-UCLA Healthcare Employee Pleads Guilty to Four Counts of Illegally Peeking at Patient Records”, *fbi.gov*, 01/08/2010.

[55] Caroline Black, “Hanks, Barrymore, Schwarzenegger: Medical files Breached at UCLA, Researcher Convicted.”, *CBS News*, 04/29/2010.

[56] Molly Hennessy-Fiske, “UCLA Hospitals to Pay $865,500 for Breaches of Celebrities' Privacy”, *Los Angeles Times*, 07/08/2011.

[57] Molly Hennessy-Fiske, “UCLA Hospitals to Pay $865,500 for Breaches of Celebrities' Privacy, *Los Angeles Times*, 07/08/2011.

[58] The Associated Press, “U.C.L.A. Health System Warns About Stolen Records”, *newyorktimes.com*, 11/04/2011.

[59] Elinor Mills, “Google Balances Privacy and Reach”, *news.cnet.com*, 07/14/2005.

[60] Elinor Mills, “Google Balances Privacy and Reach”, *news.cnet.com*, 07/14/2005.

[61] Randall Stross, Google Anything, So Long as It's Not Google, New York Times, 08/28/2005.

[62] Jose Antonio Vargas, “Letter from Palo Alto: The Face of Facebook”, *the New Yorker*, 09/10/2010.

[63] Massachusetts District Court, Boston Office, “ConnectU v. Facebook, Inc. et al”, *dockets.justia.com*, 03/23/2011.

[64] Jose Antonio Vargas, “Letter from Palo Alto: The Face of Facebook”, *the New Yorker*, 09/10/2010.

[65] Carolin McCarthy, “Seeking 'Veritas' in Facebook's Latest Legal Battle”, *cnet.com*, 11/30/2007.