# Recognition Markets and Visual Privacy

Ryan Shaw
UC Berkeley School of Information
ryanshaw@sims.berkeley.edu

Every year on April 20th, University of Colorado students gather in Farrand Field for an act of civil disobedience and hedonism: the mass consumption of marijuana. In 2006, the University of Colorado Police Department prepared for this event by placing cameras around the field and posting signs notifying visitors that all activity there would be photographed and videotaped. Confident in their numbers, the students ignored the signs, perhaps secure in their belief that though they might be seen, they wouldn't be recognized. The UCPD duly captured images of the ensuing conflagration, and then made a novel move: they posted the images on a public web server, with the explanation that anyone who successfully identified a pot-smoking miscreant would receive fifty dollars (Frauenfelder). Within days a substantial portion of those depicted had been recognized.[1]

The UCPD used the web to enroll a mass audience in the task of identification, in effect creating a human-machine hybrid technology of image recognition. Throwing images against a wall of eyeballs to see what sticks is not entirely new: consider the Most Wanted posters on the wall at the post office. What is new is the scale and speed at which the Internet can bring together those willing to sell their powers of recognition with those willing to buy. This realization has resulted in an explosion of proposals for, and some implementations of, new socio-technical systems which use "human-in-the-loop" approaches to solve image recognition problems. Often these systems are operationalized using economic models and treated as markets in which recognition services are exchanged for some form of capital. I will thus refer to such systems as "recognition markets." This paper will present an overview of the state of the art in recognition markets as well as possible developments in the future, discuss their implications for visual privacy, and suggest some guidelines for their ethical design and implementation.

## *Why recognition?*

Why focus on recognition rather than more generally on surveillance? Image capture technologies—tiny cameras, zoom lenses, and cheap sensors—have become incredibly sophisticated and ubiquitous. But despite the rapid development and proliferation of image capture devices, there still seems to be a sense that we can "hide in plain sight" of the unblinking eyes that surround us. Perhaps we are comforted by the sheer volume of images being captured, secure in the feeling that we are needles in haystacks. In other words, maybe we don't mind being seen, as long as we aren't recognized. If so, this suggests that the discussion about visual privacy should focus not on image capture technologies, but on image recognition technologies. Recognition links images to specific people, places, and things. It is these links that allow us to use images to evoke memories, provide evidence, establish proof, or spread propaganda.

## *Signal processing for recognition*

Traditionally, recognition systems have depended on signal processing. To electrical engineers, a

1 As witnessed by the author on the CU-Boulder Police Department's "420 Photo Album," <http://www.colorado.edu/police/420_Photo_Album/>, last accessed April 29, 2006.

"signal" is any measurable quantity that changes over time or space. Audio is a one-dimensional signal: frequency varying over time. An image, on the other hand, is a two-dimensional signal varying in the horizontal and vertical directions. Video is a three-dimensional signal, varying spatially within any particular frame like an image, but also varying over time like an audio signal. The field of signal processing is based upon the fundamental notion that all of these types of signals can be represented as combinations of a basic set of mathematical functions. Thus signal processing provides a universal language for describing and manipulating what appear to us as very different things. All of the many different ways in which perceptual phenomena manifest themselves are, through the lens of signal processing, transformed into "features" which can be measured and compared. The goal of recognition is to build models which use the presence or absence of these perceptual features to determine whether an image depicts some entity or concept. These entities or concepts, things like "Vegetation" or "Corporate Leader," are often referred to as "high-level features," and the recognition task is thus called "high-level feature extraction."[2]

Signal processing-based recognition systems follow a canonical design pattern, which I present a very simplified description of here. First, images of the entity to be recognized are collected and analyzed as signals. Each individual image or sequence of images is then represented as a collection of the signal features to which it has been reduced. Next, these sets of features are used to build a statistical model of the entity. There are a variety of ways to build this model, but the end goal is a function that will, when presented with a new image or video as input, tell whether or not it depicts that entity (perhaps along with a number representing the level of confidence it has that its answer is correct). When applied to an archive of images, such a function can be used to select a subset of images depicting the desired entity.

A common metric for evaluating the accuracy of a recognition system is "precision at 100."[3] The system is asked for 100 images of some entity it has been trained to recognize, such as "Homeless Person/Hobo."[4] Then those images are examined by human evaluators, and the number of images that actually do depict the object is counted. This number is the system's precision at 100. If the system is perfectly accurate, the precision at 100 will be 100. If the system is just randomly guessing, the precision at 100 will depend on how many images in the archive depict the query object, since even a random guesser will be right occasionally, given enough chances. A recognition system is considered successful if it consistently performs better than random guessing.

All else being equal, the more input data used to build a recognition model, the more accurate it will be. Building an accurate model requires not just a large number of images, but a large number of *correctly labeled* images—in other words, images that have been verified to depict the object to be recognized. But not all objects are equally recognizable. It turns out that recognizing the face or body of a specific individual is very difficult, even with huge amounts of input data. Even for very commonly photographed individuals like Madeline Albright, the very best recognition systems have a precision at 100 of around 30 (Naphade). This is far better than chance, but still very far from human-level recognition accuracy. Better results can be achieved by constraining the problem in various ways, for example by restricting the set of images to full-face, front-view portraits captured indoors under controlled lighting conditions. But in terms of recognizing people in large archives of arbitrary images, signal processing-based systems still

2 See the "TRECVID 2006 Guidelines" <http://www-nlpir.nist.gov/projects/tv2006/tv2006.html> for a specific example of a high-level feature extraction test and how it is evaluated.

3 The evaluation metric presented here is somewhat simplified. For a more detailed explanation of the kind of metric actually used, see "Inferred Average Precision and TRECVID 2006" <http://www-nlpir.nist.gov/projects/tv2006/infAP.html>.

4 This example was taken from the LSCOM Lexicon <http://www.ee.columbia.edu/dvmm/lscom/>, a list of concepts developed for the evaluation of recognition systems by a government-industry research consortium.

have a long way to go (Lew et al).

### *Using volunteer labor for recognition*

Purely signal-based approaches are not the only way to link images to the things that they depict. Humans are far better than machines at recognizing faces (though still far from perfect).[5] According to conventional wisdom, however, people are expensive. Much research into signal processing for recognition has been based upon the assumption that the recognition process needs to be fully automated to be feasible. People may be able to identify every picture of Bill Clinton without fail, but how long will it take them to examine thousands or millions of images? Better to have them examine relatively few—enough to train a statistical model—and leave the rest to the algorithms.

Such reasoning made sense before the spread of global, high-bandwidth communication networks. Now, however, it is possible to divide such tasks among millions of people. Harnessing large-scale cooperation among unpaid volunteers to construct information products in this manner has received a tremendous amount of attention in recent years. Law professor Yochai Benkler has coined the term "commons-based peer production" to refer to the phenomenon of flat, distributed networks of collaborators producing goods which they hold in common (Benkler). He argues that this form of production can outperform both markets and organizational hierarchies when the following conditions hold: first, that the "goods" being produced are information or culture, and second, that the means of producing these goods—computers and telecommunications networks—are widely distributed.[6] Benkler further claims that successful peer production systems have three characteristics. First, they must be modular, meaning the work to be done can split into pieces and handled incrementally and asynchronously. Second, the modules of work must be highly granular, meaning that participants can make even very small contributions to the overall effort. Finally, successful peer production systems must have automated or semi-automated systems for integrating contributions and exercising quality control.

The linkage of images to labels by masses of people can be seen as exhibiting all of Benkler's characteristics. Labels can be assigned to a given image in stages, by different people working independently. Photo-sharing and communication tools like Flickr[7] and Facebook[8] have made the linking and labeling of images and people and things quite easy, enabling even casual users to make contributions. Meanwhile there is considerable effort being put into the design of both systems of incentives for encouraging the contribution of "quality" information, and tools for identifying and weeding out "poor-quality" information. A few commercial media management systems such as Flickr appear to have successfully leveraged peer production of image labels to enhance the precision of their image retrieval. By allowing users to create labels that are useful for them personally, and then aggregating large numbers of these labels and making them (semi-) publicly available, these systems succeed both in encouraging a small minority of users to create labels, and in making those labels useful to many others.

In 1999 David Stork was among the first people to recognize the potential of combining peer production

5 For example, consider Levin's claim that people have difficulty recognizing faces with ethnic features to which they have not been regularly exposed.

6 I present Benkler's arguments here not to express my support for them, but to explain how the image recognition has been framed as a peer production problem. For a critical review of Benkler and others' claims for the superiority of peer production, see Duguid.

7 Yahoo! Inc., "Flickr – Photo Sharing," <http://flickr.com/>, last accessed October 29, 2006.

8 Facebook, <http://www.facebook.com/>, last accessed October 29, 2006.

with artificial intellingence or "machine learning," describing a system for harvesting and aggregating small bits of useful information from masses of people (Hearst et al). Luis Von Ahn later applied this concept to image labeling with the ESP Game (von Ahn & Dabbish). In this game, two anonymous players collaborate to describe an image. Both players are presented with the same image, and are asked to type labels that describe the image. Each player sees only her own labels. As soon as both players have entered the same label, they are considered to have "agreed" on that label, and the process begins again with a new image. The game is to find strategies that result in rapid agreement. A later variation, Peekaboom, uses a similar approach to label not just whole images but specific regions of images, making it possible for recognizers using those labels to recognize individuals in group photos (von Ahn et al). Recently Google has incorporated von Ahn's software into its image search engine.[9]

Human labeling of images can be combined with signal processing to accelerate the recognition process. Human-labeled images can be provided as training data for recognition models, and the results of human labeling can be compared to algorithmic results to check quality and make improvements (Muller et al). This technology is already making its way into the marketplace. Riya[10] and Polar Rose[11] are two recently formed companies hoping to use distributed annotations from their users to train recognition models, which can then be used to make the annotation process easier. The hope is that such systems will form a virtuous cycle, with the end result being a web of images as easily searchable as the text web is today.

The labeling of images with keywords representing concepts, as well as the algorithmic manipulation of images and their associated labels to enable search, are both forms of what Julian Warner calls "semiotic labor:" work done with and on symbols and signs (Warner). Warner categorizes semiotic labor into syntactic and semantic labor, where the former is concerned with formal representations of meaning, while the latter is concerned with meaning itself. He argues that the history of information systems has been to transform semantic labor into syntactic labor, suitable for algorithmic execution by computers. In the case of recognition systems, we see the opposite trend as well: syntactic systems replacing purely syntactic labor with hybrid systems that outsource their semantic labor to millions of humans. The digital economy has long relied on free labor (Terranova), so it is no surprise to see that systems for utilizing this labor are becoming thoroughly rationalized. Exchanges in which masses of workers who complete some micro-task are rewarded with money or entertainment, such as Amazon.com Inc.'s "Mechanical Turk"[12] and Mycroft Inc.'s "Mycroft Network,"[13] exemplify this new breed of labor market. Given that volunteer labor pools promise low-cost but bandwidth-intensive solutions to difficult problems, there is naturally a high level of interest in such systems. There has been a small but steady stream of academic papers devoted to the understanding of these systems [Kelly et al., Ludford et al., Beenen et al.], alongside a smaller, less steady trickle of critique.[14] Recently MIT announced the creation of cross-disciplinary center devoted to research into "collectively intelligent" assemblages of people and machines.[15]

### *Getting more personal*

These systems can efficiently recognize common objects and well-known people and places, but should they be cause for concern among ordinary people? Consider an image of yourself, perhaps a candid photo

9 Google Inc., "Google Image Labeler," <http://images.google.com/imagelabeler/>, last accessed October 26, 2006.
10 Riya Inc., "Riya – Visual Search," <http://www.riya.com/>, last accessed October 26, 2006.
11 Polar Rose, <http://www.polarrose.com/>, last accessed October 26, 2006.
12 Amazon.com Inc., "Amazon Mechanical Turk," <http://mturk.com>, last accessed October 26, 2006.
13 Mycroft Inc., "Mycroft – Technology Needs People," <http://mycroftnetwork.com/>, last accessed October 26, 2006.
14 A nice example of the latter is Aaron Coblin's Sheep Market <http://www.thesheepmarket.com/>.
15 MIT Center for Collective Intelligence, <http://cci.mit.edu/>, last accessed October 26, 2006.

of you shopping. Were this image to be processed by the ESP Game, it is very unlikely that you would be recognized. For this to happen two people, both of whom know what you look like and are able to recognize that the photo depicts you, would have to choose to play the game *and* happen to get matched up as collaborators by the system. But what if the system knew who your friends were and could present your image only to them? Suddenly the possibility of recognition becomes much greater. This is the approach taken by Facebook, a social networking site which rose to prominence due to to its widespread use on college campuses. Facebook allows users to upload photos to their profiles. Friends and contacts of that user can then identify the people depicted in the photos. Pending confirmation by the photo owner, these photos are then linked to the Facebook profiles of the people depicted.

Surveys of Facebook users have shown that they quickly assemble detailed public dossiers on themselves and their friends, often without regard for how easily this information can be harvested (Gross & Acquisti). Through their normal use of the system, Facebook users link hundreds of time-stamped images to detailed profiles of themselves and their friends. Such labor can produce both training data for facial recognition models and fine-grained contextual information about who was where, and when. The latter can be used to significantly improve the performance of (Davis et al.) or completely replace (Naaman et al.) the former.

### *A new application domain: Homeland security*

Hybrid assemblages of people and machines have recently been proposed or implemented as solutions to a number of controversial problems, with serious implications for visual privacy. In June 2006 Governor Rick Perry of Texas announced a plan to spend $5 million on a system that would put web cameras along the state's border with Mexico (Gonzalez & Ratcliffe). The cameras would be equipped with night vision sensors and accessible to anyone with an Internet connection. Would-be vigilantes could monitor the border from the comfort of their homes and call a toll-free number to report suspicious activities. As of October 2006, the cameras were in place but not yet online due to technical complications (Castillo).

Game designers have suggested that a similar system might serve to improve airport screening procedures (Koster, Walsh). Like the designers of the ESP Game, they propose that the problem of airport screening be re-imagined as a massively multi-player game in which distributed crowds compete to identify dangerous people without accidentally triggering searches of innocents. Though the game designers present this idea more as a thought experiment than a serious solution, in principle it does not differ much from Governor Perry's solution to the problem of border security. Should the Transportation Security Authority decide to adopt such an approach, they'll be glad to know that one game company has already done most of the work for them: Persuasive Games. In their game Airport Security players can test their baggage-screening skills from their cell phones or on the web.[16]

### *Implications for privacy*

Recognition links images to people. Increasingly, the time and location at which images were captured is automatically recorded, so that recognition links people to particular times and places as well. Thus recognition technologies carry all the privacy baggage of location-sensing technologies. Like location sensing technologies, recognition technologies can also reveal information about social networks, by

16 Persuasive Games LLC, "The Arcade Wire: Airport Security," <http://www.persuasivegames.com/games/game.aspx?game=arcadewireairport>, last accessed October 26, 2006.

revealing who was in the same place at the same time. But recognition technologies, by virtue of being visual, reveal far more than this. Location sensing technologies may tell us that two people were at the same party, but only recognition technologies can tell us whether they were simply in the same room, or whether they had their arms around each other. The image provides another dimension of visual information which we can use for interpreting the situation.

Recognition technologies also make searchable what was not previously considered searchable. I might be comfortable knowing that thousands of pictures of me are scattered around the photo albums and hard drives of my friends and family, maybe including a few here and there that have been made publicly visible on the web. I may be lulled into a false sense of comfort by current image search engines, which rely on image file names or surrounding text and thus only tend to find "official" photos from news stories or biographical profiles. But if companies like Riya and Polar Rose succeed in their stated goals, all of these photos will be collected into a result set with a single query. Careful management of permissions and security in theory can prevent private photos from being publicly viewed, but we know from our experiences with text documents that private information can easily make its way accidentally into search engine indexes. And even if accidents never happened, how is one to manage the complexities of access control? Just the simple act of allowing friend to identify people in photos in Facebook has resulted in a system that collapses social contexts, making one's every appearance in an image available to anyone in one's social network. People are just beginning to take notice of the implications of making personal data searchable and interconnected (St. John), even when access is theoretically limited to one's personal contacts. Now this data includes images as well.

### *Ethical design and implementation*

In the remainder of the paper I present some directions for the ethical design, implementation, and regulation of recognition markets. These include enforcing the contextually appropriate use of metadata, tracking provenance to combat recognition spam, understanding the limits of technological privacy protections, defining the responsibilities of image aggregators, and educating participants in recognition markets.

### *Enforcing the contextually appropriate use of metadata*

Annotations of images, and in particular annotations creating links between images and the people depicted in those images, need to be treated with the same respect for contextual privacy that the images themselves are. If a user of a photo-sharing service creates a link between an image and a person with the sole intent that the link will be used to allow her to easily find that image again, that link should not by default be used to allow global search for images of that person by *any* user of the service. Every effort should be made to ensure that image labelers understand the consequences of their actions, and that the uses to which labels are put do not change after the decision to label has been made.

One might think that this could be achieved simply by allowing the setting of access permissions on images. But even if the image itself is marked as private and not displayed to random strangers, there are ways in which the annotation might be used that violate contextual privacy. Consider for example a display of how many photos in the system depict a given person, shown on that person's public profile. More subtly, consider the use of those annotations to train a statistical model to recognize that person. Thought no one is seeing the images being used as training data, so that the access permissions are

technically being respected, the labels themselves are being used in a way that is inconsistent with the intent of the annotation creator. Just as authors often are unaware that their words will be used as input for marketing algorithms when they write to friends with free web-based email accounts, or post to a site that uses contextual advertising, neither do photo annotators necessarily know that their tags may be used as input for recognition algorithms.

Designers should seek to ensure that participants in recognition markets know for what purposes their annotation labor will be used, and should disallow novel uses of those annotations without the permission of the annotation creators. Imagine that there were a large-scale game in which users competed to find photos which depicted the same person. The effect of such a game is to connect a chain of specific places and times with the the person depicted. Now suppose that, unbeknownst to the players, this information were being used to track political protesters, in some cases resulting in their detainment or arrest. Imagine the psychological damage likely to be suffered were the players to discover that they had been unwitting participants in a reverse Milgram experiment, where what seemed to be just a game actually had quite serious consequences. In the interest of preventing incidents like this, participants in recognition systems need to be fully informed from the beginning about what data is being collected from their activity and how this data will be used.

### *Tracking provenance to combat recognition spam*

As recognition markets grow in size, scope, and economic and strategic importance, there will be increasing efforts to sabotage the recognition process. The creators of the ESP Game recognized the potential for such abuse and outlined some defenses against the most straightforward attacks (Von Ahn & Dabbish). But as organizations which rely on a combination of human-contributed data and machine learning to fuel their economic engines have learned, fighting these abuses is a Sisyphean challenge. Web search and advertising companies spend enormous amounts of time and money fighting search index spam and advertising click fraud, yet it is still unclear whether they are solving these problems or merely keeping them at bay. Recognition markets are likely to face similar issues, with distributed groups coordinating their activity for economic or political gain. For this reason, system designers should be extremely careful to track the provenance of recognition labels so that they can provide audit trails in case of claims of willful mis-recognition.

### *Understanding the limits of technological privacy protections*

Current proposals for privacy-enhancing technologies to defeat recognition systems focus on the exploitation of weaknesses of signal processing-based approaches or the implementation of standards for crippling automated systems. The former includes things like masks or clothing that disrupt recognition algorithms (Alexander & Smith), while the latter focuses on the development of equivalents to "robots.txt,"[17] a file placed on web servers which automated indexing engines are expected to respect lest they be banned from accessing those servers. Neither of these approaches will be very effective against recognition markets. Human recognition is not as susceptible to disruption as machine recognition. Even hiding behind a veil may not interfere with a person's ability to recognize someone based on body shape, gait, or other characteristics. "Do not recognize" flags, on the other hand, are unenforceable against distributed groups. While a photo sharing service may be able to prevent a robotic recognizer that does

17 An explanation of the Robots Exclusion Protocol can be found at <http://www.robotstxt.org/wc/exclusion.html#robotstxt>.

not respect such flags from crawling its public photos, it cannot effectively prevent millions of users accessing those photos from various places around the world from pooling their recognition ability to achieve the same ends.

### *Defining the responsibilities of image aggregators*

In 2003, the California legislature passed Senate Bill 1386, which requires companies storing personal information about California customers to notify these customers in the event of a security breach resulting in theft of that data. This law created a powerful incentive for companies to invest in securing customer data, rather than simply focusing on keeping such incidents out of the press. But the kinds of detailed personal information which can be produced in a recognition market may not fall under the definition of personal information provided in SB1386. In fact, each individual piece of information may be freely contributed to a public database by users who are unaware of what can be done with their contributions. In recognition markets it is the comprehensive linking of various publicly or semi-publicly available pieces of data which threaten privacy, not the individual pieces themselves. Thus it is worth considering legislation to make visual data aggregators responsible for misuses of the data they collect. This might provide a stronger incentive for companies building recognition markets to ensure that participants are well-informed about how the labels they are contributing will be used, and that these labels will not be aggregated or used as training data in ways that threaten privacy.

### *Educating participants in recognition markets*

Ultimately, the best solution for protecting visual privacy in recognition markets may be education. In particular, people need to be aware of the consequences of indexing images for searchability and of linking images to other kinds of data. In the past people have been prodded into awareness by the sudden appearance of systems that thrust previously submerged issues into the limelight.[18] Designers of these systems sometimes make the argument that the only way to establish reasonable limits for privacy is to keep pushing the envelope until "failure"—that is, until people begin to have negative reactions to the system. This is akin to finding the sharp edges of an object by trying to cut oneself—effective but painful. The danger of this approach is that there may not be sudden, apparent failures until it is far too late to halt the growth and development of recognition markets. Regulating these markets at a late stage of development may prove difficult, if not impossible. Another possibility is that there will never be a shocking failure, but that people will slowly adjust to redefinition of acceptable privacy violation, like the proverbial frog being boiled. In either case, the "build it and see what happens" approach seems unreasonably short-sighted.

Perhaps the most effective brake on the development of recognition markets would be for participants to recognize the value of their labor. The economics of peer production rely on participants under-valuing their contributions, making it possible for savvy organizations to leverage their work for enormous profit. This isn't necessarily bad: as Terranova points out, the participants may be having fun and finding fulfillment in the creative and affective labor in which they are engaging, and they may not particularly care about ownership rights in what they are creating. This is why the commons that Benkler celebrates can exist. But in practice there is often little distinction made between adding to the commons and donating labor to a profit-making organization. If people begin to feel exploited they may begin to

18 In addition to the recent Facebook incident described by St. John, the appearance of the first large web archives of old web pages and newsgroup messages in the 1990s prompted waves of concern (e.g. Lasica).

demand a greater piece of the pie, as did AOL chat room volunteers in 1999 (Margonelli), or leave en masse to start competing projects, as did CDDB contributors in 1998 (Lemos). This kind of reaction could make peer production sufficiently expensive or difficult that recognition markets cannot be built.

Some readers may view the suggestions made here as overly critical of peer production or blind to the potential benefits of recognition markets. My view is that peer production is an interesting and potentially quite useful means for achieving some ends, but the ends toward which it is applied are not inherently virtuous. We can damage through open collaboration just as easily (perhaps more easily) than we can build. Others may argue that we are too early in our exploration of the design space of such systems to begin prescribing guidelines. While I agree that we ought not stop experimenting and exploring, it is never too early to begin integrating ethical considerations into our research and design practices. Now is the time for debates about how recognition markets should work and how they will be applied. It will only become more difficult to see how things might have been otherwise.

Alexander, James, and Jonathan Smith. “Engineering Privacy in Public: Confounding Face Recognition.” *PET 2003: Proceedings of the 3rd Privacy Enhancing Technologies Workshop.* (2003): 88-106.

Beenen, Gerard, et al. “Using social psychology to motivate contributions to online communities.” *CSCW '04: Proceedings of the 2004 ACM conference on Computer supported cooperative work.* (2004): 212-221.

Benkler, Yochai. “Coase's Penguin, or, Linux and "The Nature of the Firm".” *The Yale Law Journal.* 112.3 (2002): 369-446.

Castillo, Juan. “Cameras on border work, but system not on Web.” *Austin American-Statesman.* (October 5, 2006): B1.

Davis, Marc, et al. “Towards context-aware face recognition.” *MULTIMEDIA '05: Proceedings of the 13th annual ACM international conference on Multimedia.* (2005): 483-486.

Duguid, Paul. “Limits of self–organization: Peer production and 'laws of quality.'” *First Monday.* 11.10 (2006). <http://firstmonday.org/issues/issue11_10/duguid/index.html>.

Frauenfelder, Mark. “Dirty snitches earn $50 for fingering fellow students smoking pot.” *Boing Boing.* (April 28, 2006). <http://www.boingboing.net/2006/04/28/dirty_snitches_earn_.html>.

Gonzalez, John W., and R. G. Ratcliffe. “Eyes of Texas to be on border.” *Houston Chronicle.* (June 2, 2006): A1.

Gross, Ralph, and Alessandro Acquisti. “Information revelation and privacy in online social networks.” *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society.* (2005): 71-80.

Hearst, Marti A., Robin D. Hunson, and David. G. Stork. “Building intelligent systems one e-citizen at a time.” *IEEE Intelligent Systems and Their Applications.* 14.3 (1999): 16-20.

Kelly, Sean Uberoi, Christopher Sung, and Shelly Farnham. “Designing for improved social responsibility, user participation and content in on-line communities.” *CHI '02: Proceedings of the SIGCHI conference on Human factors in computing systems.* (2002): 391-398.

Koster, Raph. “Treating players like numbers.” (January 4, 2006). <http://www.raphkoster.com/?p=242>.

Lasica, Joseph D. “Your Past Is Your Future, Web-Wise.” *Washington Post.* (October 11, 1998): C1.

Lemos, Robert. “Companies fight over CD listings, leaving the public behind.” *CNET News.com.* (May 24, 2001). <http://news.com.com/Access+denied+A+copyright+battle/2009-1023_3-258109.html>.

Levin, Daniel T. “Race as a visual feature: Using visual search and perceptual discrimination tasks to understand face categories and the cross-race recognition deficit.” *Journal of Experimental Psychology.* 129.4 (2000): 559-574.

Lew, Michael, et al. “Content-based multimedia information retrieval: State of the art and challenges.” *ACM Trans. Multimedia Comput. Commun. Appl.*. 2.1 (2006): 1-19.

Ludford, Pamela J., et al. “Think different: increasing online community participation using uniqueness and group dissimilarity.” *CHI '04: Proceedings of the SIGCHI conference on Human factors in computing systems.* (2004): 631-638.

Muller, Henning, et al. “Using heterogeneous annotation and visual information for the benchmarking of image retrieval systems.” Santini, Simone, Raimondo Schettini, and Theo Gevers, eds. *Internet Imaging VII.* SPIE-6061 (2006): 34-45.

Naaman, Mor, et al. “Leveraging context to resolve identity in photo albums.” *JCDL '05: Proceedings of the 5th ACM/IEEE-CS joint conference on Digital libraries.* (2005): 178-187.

Naphade, Milind R., and John R. Smith. “On the detection of semantic concepts at TRECVID.” *MULTIMEDIA '04: Proceedings of the 12th annual ACM international conference on Multimedia.* (2004): 660-667.

St. John, Warren. “When Information Becomes T.M.I.” *The New York Times.* (September 10, 2006).

Terranova, Tiziana. “Free Labor: Producing Culture for the Digital Economy.” *Social Text.* 18.2 (2000): 33-58. <http://muse.jhu.edu/journals/social_text/v018/18.2terranova.html>.

Von Ahn, Luis, Ruoran Liu, and Manuel Blum. “Peekaboom: a game for locating objects in images.” *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems.* (2006): 55-64.

Von Ahn, Luis and Laura Dabbish. “Labeling images with a computer game.” *CHI '04: Proceedings of the SIGCHI conference on Human factors in computing systems.* (2004): 319-326.

Walsh, Tony. “Airport Screening Is A Badly-Designed Game.” Clickable Culture. (April 15, 2006). <http://www.secretlair.com/?/clickableculture/entry/airport_screening_is_a_badly_designed_game/>.

Warner, Julian. “Forms of labour in information systems.” *Information Research.* 7.4 (2002). 27 October 2006 <http://informationr.net/ir/7-4/paper135.html>.

# Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements

**Nathaniel S. Good[1], Jens Grossklags[1],Deirdre K. Mulligan[2], Joseph A. Konstan[3]**

[1]School of Information, UC Berkeley
102 South Hall, Berkeley, CA
{ngood,jensg}@ischool.berkeley.edu

[2]Boalt School of Law, UC Berkeley
346 Boalt Hall, Berkeley, CA
dmulligan@law.berkeley.edu

[3]Department of CS&E, University of Minnesota
200 Union Street SE, Minnesota, MN
konstan@cs.umn.edu

**ABSTRACT**

Spyware is an increasing problem. Interestingly, many programs carrying spyware honestly disclose the activities of the software, but users install the software anyway. We report on a study of software installation to assess the effectiveness of different notices for helping people make better decisions on which software to install. Our study of 222 users showed that providing a short summary notice, in addition to the End User License Agreement (EULA), before the installation reduced the number of software installations significantly. We also found that providing the short summary notice after installation led to a significant number of uninstalls. However, even with the short notices, many users installed the program and later expressed regret for doing so. These results, along with a detailed analysis of installation, regret, and survey data about user behaviors informs our recommendations to policymakers and designers for assessing the "adequacy" of consent in the context of software that exhibits behaviors associated with spyware.

## Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces: *interaction styles, standardization, user-centered design*
J.4 [**Social and Behavioral Sciences**]: *psychology*
K.4.1 [**Computers and Society**]: Public Policy Issues – *privacy and regulation*
K.5.2 [**Legal Aspects of Computing**]: Governmental Issues – *regulation*

**Author Keywords**

Privacy, Security, Notice, End User License Agreement, Timing, Spyware

## INTRODUCTION

Spyware, broadly defined, is fundamentally a challenge for HCI research as much as it is a technical one. At its core, fully disclosed spyware presents users with a trade-off: users gain the functionality of software in exchange for giving up private data, tolerating advertising messages, or both. While some examples of spyware are primarily fraudulent, others disclose the functionality of the spyware in a manner similar in form to the disclosure practices generally found in the software industry. Individual users have different needs and tolerances, and in the absence of public policy limiting their choices, the disclosures provided by spyware vendors would provide the basis for individuals to effectuate their policy choices in the marketplace. In an ideal market users would make decisions to install software, including spyware, where the trade was in their interest.[1] At times law constrains individual choice based on externalities or other market failures, or normative decisions about the values at issue. In the U.S., with respect to privacy and other issues commonly dealt with in mass-market software contracts there is little constraint on the substantive terms with respect to privacy, reliability, or security that can be presented to consumers.

It is not an ideal world. Study after study shows that people unwittingly install malicious or unwanted software [4][13]. It is easy to identify reasons for this disconnect. Certainly some of it is due to the software not disclosing what it does. Equally certainly, most users don't bother to read the lengthy and legalistic End User License Agreements (EULAs) or Privacy Agreements[27]. Even if the EULA is accurate, and the user reads it, the agreements may be so long and confusing as to prevent meaningful knowledge and consent. Some users may mistakenly believe that their operating system, antivirus software, or other precautions will protect them. But there are other reasons. Users may be too eager to use the software to be concerned about spyware—at least at that moment. And users who have just selected the action to install may be too committed to that

[1] We want to emphasize that we do not wish to downplay the problems associated with malicious software that fails to disclose its true behavior; as we discuss below, there are legal remedies for such deception. However, in this work we restrict our attention on supporting users in making correct decisions when faced with disclosed trade-offs.

action to suddenly change course (just as Norman suggests that immediate confirmation of deleting a file is useless or worse [22]).

Our work builds upon a previous study of 31 subjects that showed that short summary notices, as a supplement to EULAs, have promise in helping users identify which software they feel comfortable installing [18]. We studied 222 subjects, observing their installation behavior in one of three information conditions: 1) an ordinary EULA, 2) a short summary notice before installation additional to the EULA, 3) a short summary notice (with an opportunity to uninstall) immediately after installation additional to customary EULA. We also surveyed users about their behavior in both computer use, more general use of legal documents (e.g., signing such documents without reading them) and actions regarding several online risks. The results of this study provide significant opportunities for designing software systems that better support users in protecting themselves against unwanted spyware, and might even generalize to a broader set of "in-the-moment" decisions.

The fact that users do not read EULAs may appear to be a truth in need of little proof. But for the current policy debates this finding is important. The courts, absent fraud or unconscionability, largely hold individuals responsible for the terms of legal agreements regardless of this reality. However, because a defining element of spyware is the context—in particular the consent experience—around its acquisition state and federal regulatory agencies and the private sector are developing new policy that establishes procedures aimed at providing an "adequate" consent experience. While reflective of HCI in some respects there has been little transfer of knowledge or prior research to determine the likely effect of these enhanced procedural rules. Thus, there is much to be gained from a cross-disciplinary conversation around the HCI contributions toward these reforms.

## RELATED WORK

As some experimental research demonstrates, users stated privacy preferences do not always align with their behavior [2][23]. For small monetary gains (e.g., a free program) or product recommendations, users are willing to trade off their privacy and/or security [2][23]. Moreover, users are more likely to discount future privacy/security losses if presented with an immediate discount on a product [2]. Notices often fail to dissuade individuals from making decisions that contradict their own clearly stated preferences [23][27].

HCI practitioners have been concerned about privacy concerns on the web in general, and recent work in HCISec (HCI and security)[2] has been concerned with cookie management [15][16], spyware [24], phishing [12], as well as online privacy notices [10][20] and incidental privacy issues with web browsing [19] and filesharing [17].

HCI practitioners are uniquely positioned to contribute to the conversation on designing more effective notices by, for example, improving on timing and visualization. However, contributions to notice design are challenging because users are simply trained to ignore consent documents. This challenge of attracting attention to important events is not a new one in HCI. A number of researchers are studying the effects of notification systems in computing. They examine the nature of interruptions and people's cognitive responses to work-disruptive influences. Notification systems commonly use visualization techniques to increase information availability while limiting loss of users' focus on primary tasks [11][26][25]. From control room and cockpit indicators to desktop notifiers, substantial research has been devoted to identifying visual and auditory displays that attract attention and to designing interaction sequences that prevent automatic dismissal of information.

Work on privacy notices for web sites spans several different areas. P3P[3] and privacy bird[4] were popular efforts to inform users about a Web site's privacy preferences, as well as to give users control over the types of information exchanged with interaction partners. The P3P design called for web designers and companies to provide easy to read, privacy statements in a standard format that is usable, for example, by P3P-aware browsers to communicate this information to the end user.

Recent research by Karat *et al.* [21] aims at providing design methodologies and tools to assist in the creation of more usable privacy policies that can be verified by automated techniques. A main objective is to achieve consistency between notices, as well as better compliance with emerging privacy standards.

Friedman *et al.* [15] work towards improving interfaces for informed consent through implementing value sensitive design methodologies. Their design approach targets users' comprehension and suggests methods to facilitate consent between the user and the application based on shared knowledge and trust.

Early work with privacy in HCI was focused on the notion of feedback and control, introduced by Bellotti and Sellen [6]. The concept of feedback and control suggests that users are given ample feedback on the actions a system is taking, whether it is video taping someone or sending information to a third party, and that users are given adequate means of

[2] See the HCISec Bibliography for the most important contributions to this field. http://www.gaudior.net/alma/biblio.html

[3] W3C Platform for Privacy Preferences Initiative. Platform for Privacy Preferences (P3P) Project. http://www.w3.org/P3P.

[4] http://www.privacybird.com/

controlling the flow of this information, such as being able to turn off recording or specify which information is sent to third parties.

The concept of feedback and control is related to the legal explanations of informed consent. Informed consent emphasizes that end users must receive notice (signs, readable language, etc.), and must be able to provide consent to the action. Essentially, to use a term in contracts, both parties have to establish a "meeting of the minds" where they are both consenting to and are agreeing to the same shared set of knowledge.

Courts typically enforce EULAs. Courts have enforced shrinkwrap agreements that purport to bind users to EULA terms that appear on software packaging simply because the user opened the package.[5] Courts typically find that installing or using the software is sufficient to establish acceptance of EULA terms even when users are not required to click "I Agree."[6]

There is a growing body of literature questioning the courts generally unquestioning and superficial review of the context of contract formation, specifically around notice and consent. Within the legal literature and policy circles questions about the adequacy of consent, in particular the form, content, presentation and timing of disclosures in relation to programs that exhibit behaviors associated with spyware, are being raised [14][7][8][28][29][5][3][1].The Federal Trade Commission and the State Attorney Generals are challenging the courts' laissez-faire attitude towards contract formation demanding heightened procedural, and to a lesser extent substantive, protections for contract formation in the context of spyware enforcement actions. The rules they are establishing in this context will likely inform the agencies, and in time the courts, views on contract formation with respect to downloadable software in general.

Given the connection between the privacy and security decisions of individual users and the overall security of the network, the questions about externalities bear particular attention. If we are to rely on a private contractual approach to privacy in the U.S. we need to make sure that private choices don't undermine collective security and that users are capable of understanding and making the privacy and security decisions necessary to protect their interests.

Our report adds to the growing literature on HCI and security/privacy but also makes important connections to the ongoing legal and policy reforms around notice and consent.

[5] *Bowers v. Baystate Technologies, Inc.* , 320 F.3d 1317 (Fed. Cir. 2003).

[6] See Tarra Zynda, Note, *Ticketmaster Corp. v. Tickets.com, Inc.: Preserving Minimum Requirements of Contract on the Internet*, 19 Berkeley Tech. L.J. 495, 504-505 (2004).

## EXPERIMENTAL DESIGN

### Experimental Setup

Our experimental setup consisted of an experimental portion, followed by two surveys. Subjects were given a unique number, and sheet outlining the basic scenario of the experiment. All of the experiments and surveys were done by each subject independently on a computer located in a laboratory with dividers. As the user passed each portion of the experiment, the application would record the actions and provide the next portion of the experiment. We describe the details of each portion of the experiment below.

### Experimental Framework

The experimental portion of our framework was designed to mimic the experience of installing software applications, but also allows us to modify the notice and consent process encountered. Previous experiments showed us that pop-up windows and warnings are quickly ignored by users who are accustomed to click through them. In order to have users "notice" the notice conditions, we decided to build them into the install experience.

We constructed a windows application in C# that would not only depict the installation process as realistic as possible, but also log all user actions (e.g., buttons clicked, time per screen) during the study. Additionally, the application we constructed would provide a launching pad that could dynamically configure each subject's experience based on their user number we provided at the beginning of the experiment. Users were given a user id, which was matched up against a list of acceptable identifiers and associated with a treatment and a counter-balanced program ordering.

We constructed two surveys, which could be accessed from the application launching pad. After the experimental portion was completed, users could click on the survey buttons to answer each respective survey. When both surveys were completed, the user was returned to the launching pad, and told that the experiment was completed.

### Notice Treatments

Our design consisted of three notice conditions: two treatments with customized short notices that included abbreviated EULAs for the programs plus the original EULA (all without brand information) and one control condition that only consisted out of the original EULA (again all without brand information):

PRE - Short notice before installation presented on the Install Option Screen plus the original EULA on the EULA screen;

POST - Short notice after installation on the Post Install Warning Screen plus the original EULA on EULA screen; and

CONTROL/None - No short notice at all, but with the original EULA on the EULA screen.

Each notice condition was integrated into three programs with consistency maintained for each portion of the controlled experiment by providing similar screens, but changing the content of the information in key screens for the different programs. Figure 1 below details the screens involved in the installation process for each user.

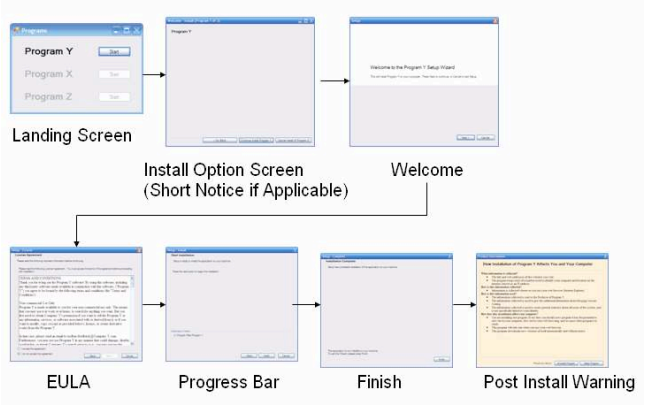



**Figure 1 Process of installation screens in experiment**

The Post Install Warning screen only occurs when a user is in the post notice condition. However, the Install Option Screen displays the Short Notice in the Pre condition, but appears also in the other two treatment conditions without specific information. At any time, a user may cancel the installation and return to the landing screen to start with the next program. Additionally, users may move back and forth between screens as in typical installation programs by hitting the back key.

We selected programs from our previous study [18] to facilitate comparability of the results and user experience. We chose a browser toolbar, a weather information service and a file sharing application. For the experiment each brand name was removed and replaced with a generic title. The program titles and descriptions are listed below:

- Program X – Weather Information Program
- Program Y – Browser Toolbar
- Program Z – File Sharing Program

To summarize, we ran a 3x3 mixed methods study, consisting of 3 *between*-subjects factors and 3 *within*-subjects factors. The between subjects factor were the notice conditions (None/Control, Pre, Post) and the within-subjects factors were the programs (Filesharing, Weather Service and Browser Toolbar). Within subjects factors were counter-balanced within the population. We want to add that it is of methodological interest to us to understand the relative strengths and weaknesses between the small scale user study and the current large experiment with hundreds of users.

### Notice Construction

Our short notices were designed by distilling the long EULAs from three programs included in our study. We used the same short notices as we constructed in a previous study. Each notice condition that included a short notice (Pre and Post) had the same text for a specific program. The only difference between each treatment was the timing where each notice was shown. Examples of how the short notice for Program Z would appear during the experiment in the pre-notice and post-notice treatments are presented in Figure 2 and Figure 3, respectively.

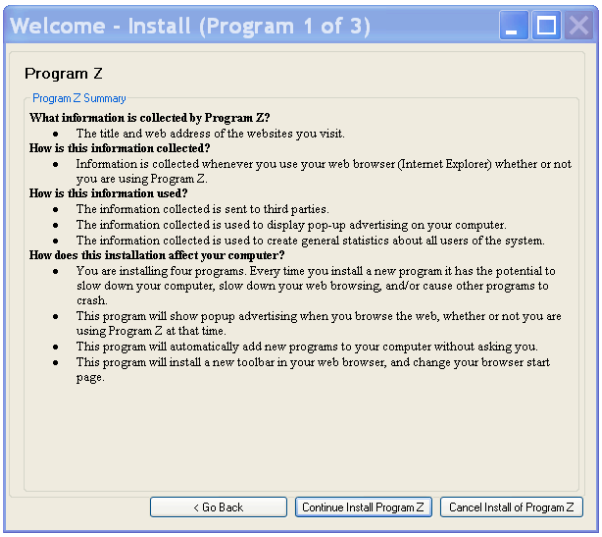



**Figure 2 Pre-installation short-notice (would appear on Install Option Screen in Pre-Notice treatment)**

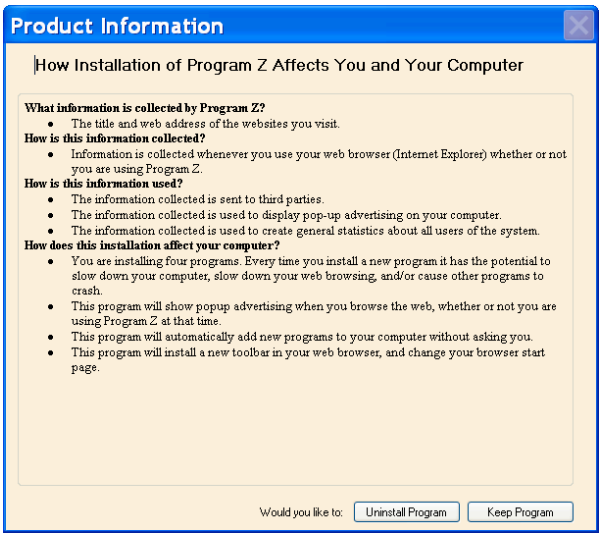



**Figure 3 Post-installation short-notice (would appear on Post Install Warning Screen in Post-Notice treatment)**

### Surveys

Our study included two surveys that were presented to the user after the installation experiment. The surveys included different question types, for example, open ended, Likert

scales, and simple yes/no questions. The purpose of the survey was to understand the subjects' concerns regarding a representative selection of online risks and stated behaviors related to software notices, as well as to determine how the users perceived the programs in the experiment as well as whether or not they regretted the actions they performed in the experiment after being provided with an (additional) chance to review the short notice.[7]

The first survey consisted of demographic and behavioral information, while the second survey consisted of questions regarding the experimental experience. In total, we anticipated that the two surveys plus the experiment section could be passed by the average subject in about one hour.

**Table I Self-reported behavior regarding online risks**

| | Total | |
|---|---|---|
| | Mean | Std. Deviation |
| Try Functionality | 4.41 | 2.64 |
| Research on Web | 5.14 | 2.64 |
| Once Installed wont remove | 2.24 | 1.72 |
| Accept Popups for free stuff | 3.36 | 2.42 |
| Install programs that look interesting | 3.55 | 2.35 |
| Install only if I know exactly what it does | 6.41 | 2.06 |

## RESULTS

### Subjects

240 subjects participated in the study, of which we were forced to remove some entries due to missing data leaving us with 222. Subjects were paid $20 for their participation, and were recruited by a university service with access to a subject pool of several thousand students. Our subjects are divided into three treatment groups: 64 users in the control condition, 80 in the pre-notice condition and 78 in the post-notice condition. We used chi-squared to analyze differences between the discrete variables of install and regret, and ANOVA to analyze the differences between the continuous variable of time.

64.2% percent of our subjects were female. 39.5% indicated their age as less than 20 years-old. An additional 57.7% were between the ages of 20 and 25. The dataset also includes a small group of 2.7% over 25 years of age. On average we had a very computer-experienced group of users. For example, 85.2% stated that they maintained their home computer themselves.

[7] Of course, subjects in the control group and those in the post notice treatment that canceled early had not seen the notice before.

### Attitudes towards online risks

We asked users to rate concerns on a scale of 1-9, with higher numbers expressing more concern. Subjects expressed high concern towards 5 different risk types and nuisances often encountered in online interactions: identity theft, spyware, viruses, pop-up advertisements, and privacy intrusions.

Surprisingly, our young subject pool was somewhat less alarmed about identity theft and privacy compromises, compared to being subject to spyware attacks and pop-up advertisements. Possible damages caused by viruses topped the list.

We employed *k*-means multivariate clustering techniques to classify subjects according to their risk attitudes. Hierarchical clustering (single linkage) preceded the data analysis. We selected the best partitioning using the Calinski-Harabasz criterion [9]. We derived two distinct clusters: a first group with a substantially higher degree of unease about online risks along all measured dimensions (62.2%) and a second less worried and comparatively smaller group (37.8%).

### Self-reported behavior regarding online risks

Our subjects are forthcoming about their good computer hygiene practices (see Table I; values are reported on scale from 1-9). On average, while they are interested in trying new content, they report to somewhat often research programs on the Web before using them, claim that they only install program when they are well informed about them, and report that they hardly leave them installed if found undesirable. They rarely agree with the statement that free software in exchange for intrusive advertisements is acceptable. Only few wholeheartedly admit that they would frequently download and install programs that look interesting.

### Self-reported reading practices for legal documents

Only very few users reported reading EULAs often and thoroughly when they encounter them (1.4%). Members of a larger group categorize themselves as those who often read parts of the agreement or browse contents (24.8%). However, 66.2% admit to rarely reading or browsing the contents of EULAs, and 7.7% indicated that they have not noticed these agreements in the past or have never read them.

**Table II Self-reported reading practices for legal documents**

| | Total | |
|---|---|---|
| | Mean | Std. Deviation |
| Financial Privacy Notices | 5.97 | 2.78 |
| Read Web Privacy Notices | 4.24 | 2.28 |
| Read Shrinkwrap Licenses | 3.81 | 2.25 |

In Table II we report on subjects' reading behavior for other important notices (values are reported on a scale from 1-9 from "never read" to "always read". Web privacy notices and shrinkwrap licenses are read less frequently in comparison to, for example, financial privacy notices. Less related to our field of investigation, we found that food nutrition labels and credit card statements are read almost twice as often as shrinkwrap licenses by our subject group (means of 6.8 and 7.3, respectively).

**Table III Occurrences of canceled installations for each screen**

| Treatment | Cancellation Screen | Program X | Program Y | Program Z |
|---|---|---|---|---|
| None | Install option | 15.6% | 9.4% | 9.4% |
| | Welcome | 15.8% | 0.0% | 0.0% |
| | EULA | 4.7% | 0.0% | 4.7% |
| | Install Progress | 0.0% | 0.0% | 0.0% |
| | TOTAL CANCELED | 32.1% | 9.4% | 9.4% |
| Pre | Install option | 69.2% | 28.2% | 69.2% |
| | Welcome | 1.2% | 0.0% | 0.0% |
| | EULA | 0.0% | 0.0% | 0.0% |
| | Install Progress | 0.0% | 0.0% | 0.0% |
| | TOTAL CANCELED | 70.4% | 28.2% | 69.2% |
| Post | Install option | 13.8% | 2.5% | 11.3% |
| | Welcome | 0.0% | 0.0% | 1.3% |
| | EULA | 11.3% | 1.3% | 5.0% |
| | Install Progress | 1.3% | 0.0% | 0.0% |
| | Post Install Warning | 51.3% | 28.6% | 58.8% |
| | TOTAL CANCELED | 77.7 | 32.4% | 76.4% |

**Behavior in the experiment: Installation**

Chi-squared tests showed that both notice conditions had significantly lower instances of installation than the control condition ($p<.001$). This effect is robust independent of whether the unit of investigation are the whole treatment groups or individual programs ($p<.001$)

This result demonstrates that the short notice treatments had a significant behavioral impact on subjects. It also supports what we have seen in previous studies and have observed in the field - users that are presented with the omnipresent overly long and complex presentation of EULAs are prone to installing applications more often. As we saw in our previous small-scale ecological user study[18], the toolbar application was most frequently installed, followed by the file sharing application and finally the weather information service. For the control treatment we attribute the difference between programs to a combination of two effects: preference for a program type (e.g., toolbar vs. filesharing client) vs. desirability of contractual terms. Users seem to be able to discriminate between programs even without additional cues such as brand information and familiar user interface design. The results we present in following sections rest on the variation of treatment variables.

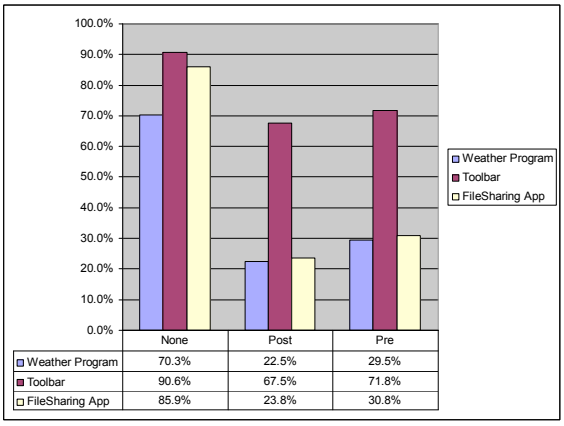



**Figure 4 Programs installed by users**

**Behavior in the experiment: Cancellations/Uninstalls**

Interestingly, of those that canceled the installation in the control and post-notice treatments the preferred action (always more than 50%) was to leave the program immediately on the very first screen (that is Install option screen). Only between 0% and 42.8% of subjects ended up visiting the EULA screen. This result is of importance for program developers interested in increasing their installed base. It seems that although many people might enter an installation they often will immediately leave even without gathering further information.

Table III reports the percentage of all individuals that canceled on particular screens for the three different treatments. It demonstrates the dominance of the short notice screens (Install Option for pre-notice and Post Install Warning for post-notice) in comparison to the EULA screen.

Note that the short notices contained information from the original EULA, however, presented in a unified and abbreviated format. Therefore, the data for the post notice treatment clearly demonstrates the inadequacy of the long and complex EULA. All subjects that canceled on the Post Install Warning screen have seen the original EULA on the screens they passed to reach the warning screen. But only on the short notice screen they decided to cancel.

**Behavior in the experiment: Timing and reading notices**

*Pre-notice*

In our experiment there is only one screen per program that was visited by everybody independent of treatment condition and whether they installed or canceled the installation at some point of the process. This is Install Option Screen. In Table III we have already shown that

many subjects decided to cancel at this point of installation. It, however, is also interesting to note that there are significant differences in time spent by the subjects at this point of the experiment.

**Table IV Time in sec for Install Option Screen (Program X)**

| Treatment | Installation completed | Mean time (sec) |
|---|---|---|
| None | Yes | 1.9 |
| | No | 13.5 |
| | Significance result | p<0.0037 |
| Pre | Yes | 3.4 |
| | No | 59.2 |
| | Significance result | p<0.0000 |
| Post | Yes | 0.5 |
| | No | 8.3 |
| | Significance result | p<0.0002 |

First, individuals that decided not to install a program are significantly slower than installers for all three treatments (see Table IV).[8]

Second, not surprisingly, individuals that do not install the programs spent more time on the Install Option Screen if they are members of the pre-notice treatment group compared to those in the control or post-notice treatments (with at least $p<0.05$ for all programs, but stronger for most). They are obviously paying attention to the notice.

Third, for those that installed the programs there is no such statistically significant difference noticeable. It should be added that installers in the pre-notice condition also passed quicker through the Install EULA screen than the control and post-notice group; that is, they did not pass quickly through the pre-notice screen with the intention of reading the actual EULA carefully.[9] Accordingly, they are consistently quicker than others. Or, to phrase it differently, they are ignorant towards notices.

We conclude that one main difference between installers and those that decline the program offerings is the time they spent deliberating at the start of the program installation. Even for the two treatments where no pre-notice was displayed on the Install Option Screen non-installers are considerably slower. One interpretation is that more deliberate individuals take additional time to study the short notice.

[8] Result does not hold for program y in the control treatment. However, the group of non-installers is extremely small for this program which makes it an outlier case.

[9] The group mean comparison test is significant for program x and z ($p<0.005$). For program y the differences have the expected direction, however, are not significant.

**Table V Comparison of pre and post-notice reading time**

| Program installed | Cancellation Screen | Time for Program X (in sec) | Time for Program Y (in sec) | Time for Program Z (in sec) |
|---|---|---|---|---|
| Yes | Mean Pre-notice | 3.4 | 8.5 | 0.0 |
| | Mean Post-notice | 14.5 | 35.6 | 15.6 |
| | Significance | p=0.01 | p<0.0000 | p<0.0000 |
| No | Mean Pre-notice | 59.2 | 81.0 | 44.2 |
| | Mean Post-notice | 30.2 | 37.1 | 30.8 |
| | Significance | P<0.0000 | p<0.0006 | p<0.005 |

*Post-notice*

Finding a natural comparison standard for the reading time in the post-notice treatment is more difficult since the Post Install Warning Screen appeared only in this treatment. We believe that comparing pre-notice and post-notice reading time is the most natural approach.

Table V strongly supports the finding that individuals who eventually installed a program passed slower through the Post Install Warning screen compared with the Install Option Screen. However, subjects that did not install a particular program took more time reading the pre-notice.

Assuming that increased reading times improve consumer decision-making this demonstrates a conundrum. On the one hand, we observed for the pre-notice that only non-installers read the notice (or even become aware of the notice). This is different for the post-notice where reading times even for subjects that completed installations are significantly distinct from zero. On the other hand, if subjects became aware of the pre-notice they spent a considerably longer amount of time absorbing the information which usually led to a cancellation of the installation process.

From a behavioral point of view it appears that subjects are very much willing to cancel an installation at the beginning of the process if they are adequately informed about the terms of the transaction. However, the risk is that they are too involved in the flow of conducting the necessary installation steps in order to notice the additional warning terms.

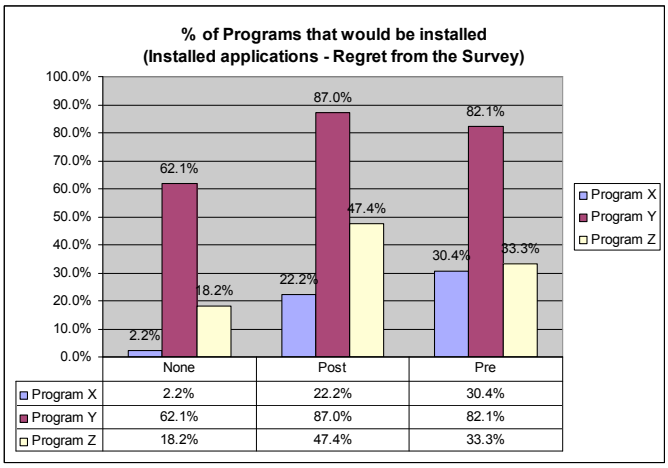
In contrast, the post-notice serves to slow down a majority of the individuals. It seems that subjects at this time of the installation process are able to notice and digest further information; that is, they have left the flow state. However, reading the notice does not necessarily result in the uninstallation of the program. One interpretation is that subjects have made an emotional investment into the program installed. Or they might be interested in trying the program even if they dislike its terms since it is already

installed at this point. As a result, not all users are willing to reverse their decisions. Another potential explanation is that subjects who keep the program feel that it adequately reflects their preferences for a consumer program. The distinction between these hypotheses is left for future work, but we present further evidence on this question in the next section.

**Correlation Survey and Experiment: Regret**

In Post Survey 2, we showed all subjects the short notice for each program, and asked them if they would install the program described in the short notice or not. We used this measure as a means of calculating the user's regret. In the post case, we calculated regret after users had seen the post notice, and had made the decision to keep or uninstall the program. We determined that users would have two types of regret, regret that they installed a program (and would like to remove it) and regret that they chose not to install a program (and they would like to install it). The second case we expected to be less common.

Overall regret was high for programs that users installed. Only in the case of program Y, the toolbar, do we see that over 50% of the users were happy with their installation choices. Regret is still very high for the programs that users consider the least usable, namely program X. In the best case, the pre notice, 70% of the users still regret installing the application. Although short notices may help, there is still much room for improvement.




| | None | Post | Pre |
|---|---|---|---|
| Program X | 2.2% | 22.2% | 30.4% |
| Program Y | 62.1% | 87.0% | 82.1% |
| Program Z | 18.2% | 47.4% | 33.3% |

**Figure 5 Graph of percent of users who were happy with their installation choices**

*Reading and Regret*

The high regret we saw lead us to wonder as to whether regret was different in cases where users actually spent more time on the notice screens, either the short notices and/or the EULAs themselves. We decided to analyze cases where users had made it to at least one notice screen (EULA and/or short notice), and compared the time that users spent on each screen to their stated regret. By using time as an implicit measure of reading we were able to determine if the notice reading time had an effect on regret.

Overall, we found a strong difference between the control treatment and the pre treatment in terms of regret ($p<.05$). We found that in most cases, users who spend more time reading the short notices in both the pre and post conditions had less regret. Details of regret in each treatment condition are given below.

*Regret and the Short Notice Condition*

Not surprisingly, in the short notice case, we saw a significantly lower level of regret ($p<.05$) for users who spent more time reading. Users who had less regret spent on average 20 – 30 seconds more per notice, approximately double the average time in most cases.

*Regret and the Post Notice Condition*

At a first glance, the post notice condition seemed similar to the control condition. Because the post condition comes after users look at the EULAs, the combined post notice and EULA time may be dominated by behaviors we see in the EULA only case. For this reason, we ran another case where we separated the EULA time from the post notice time, and looked at how time on the post notice related to regret.

In this case, we found that the post noticed behaved similarly to the short notice, but the effect was not as strong across all program types. Users who spent more time on the post notice had significantly lower regret for the least desirable program, program X, but not across the other program types. We found this to be interesting because users in the post notice condition had to decide to keep the program or uninstall it. It was also the last notice that the users saw, so we were surprised that post notice had still had high cases of regret. It may be the case that for some users, after they have committed to an installation they feel they have some investment in the program or momentum and would like to continue to install. In the future, we plan to use more sophisticated modeling techniques to derive more comprehensive and powerful explanations of these kinds of user behavior.

*Regret and the Control Condition*

We found that in the control condition, users had a high amount of regret, whether they spent time reading the EULA or not across most programs. The control case, users had significantly higher values of regret ($p<.001$) for programs x and z. and a moderately higher value than the pre condition in program y ($p<.10$). In some cases, users who read more had significantly higher cases of regret than those that read less ($p<.05$). There is evidence that the EULAs could be confusing and misleading [18]. One user from our survey said she was "befuddled by the language" another mentioned that "they're often very very long [and] not easy reading, either." Users also mentioned that if they

have concerns, they look for certain terms such as “pop ups” or other things that may adversely affect their computer. One user mentioned “[I would look at them] if [they were] precise and clear, and the agreement is short, so it’s not too time-consuming. And the words are keywords, so I could just browse it very quickly at a glance. Besides, I will read it when the program alerts me the bad consequences of not reading the agreements.” This result emphasizes the need to have common terms across software licenses, especially for cases that deal with issues users are generally concerned about (performance, pop-ups, monitoring, etc).

### *Summary of Reading & Regret Results*

From our analysis of reading and regret, we have learned that if we can get users to spend time reading the notices, they may experience significantly less regret. In this case, it is important for HCI practitioners to determine what can be done in terms of interfaces to get more users to slow down and read notices.

## DISCUSSION

### *Observations and Implications*

Four observations have very clear design implications for software installation systems and for efforts in the public and private sector to make the consent experience meaningful.

First, the experiment validates the use of short summary notices as a mechanism for reducing the installation of unwanted software. There are many ways in which such notices could be provided, ranging from legal solutions (where the use of such notices could be necessary for documenting informed consent) to technical and business ones (e.g., the creation of subscription services that provide such "installation reviews" for users). Efforts at state and federal regulatory agencies to simplify and highlight core software behaviors and draw attention to particular terms appear promising based on our research.

Second, the effectiveness of post-install notices suggests an alternative strategy for reducing unwanted spyware – delaying the actual irrevocable installation of software. Users might be well-served by systems that "pretend" to install software, then warn about the consequences before really completing the installation. (This approach could be a variant of the "to finish installation, you must reboot" barrier.) Or in some cases, it may even be worth preventing immediate use of software to provide a period of reflection. Efforts in the private sector to create virtual machines or sand boxes of sort that would allow consumers to test out software without allowing it fully onto their machine appear promising.

Third, from the regret data in the pre- and post-experimental conditions, we know that substantial regret exists even with these short notices. Accordingly, it is important to continue to explore other remedies to the spyware problem, including legal protections, technical protections, and interfaces that intercept the problem before the installation decision is made. Indeed, Google's warning that forces confirmation from people following a link to certain web sites (primarily cracking-related) could be adapted, or better yet, tools tied to ratings services could label links to software with indicators of the negative consequences of its use. It also points to the need for users to be provided with simple means to restore their machines to pre-installation state. Recent spyware enforcement actions have focused on this requirement.

In general, our research conclusions support the additional procedural constraints the FTC and State AGs are placing on spyware vendors. Given the contextual and individually subjective decisions about what is spyware our research would support the expansion of these protections to a broader range of software installations. The question is how broad a range is appropriate given that enhanced notices about everything is likely to undermine the utility and effectiveness of these “express consent” procedures where users face the greatest risks.

Finally, the presence of individual differences in reading behavior and other behaviors correlated with spyware installation suggests that personalized solutions have promise. Some users are well-served by the current system, or would be with short summary notices. Others seem likely to ignore such notices and might be willing to accept more restrictions on their installation (e.g., longer delays sequences of confirmations, or approval from another individual) in order to reduce their own risk and later regret. There are many paths to explore in this direction. To the extent that the overall security of the network is influenced by the decisions of users some of who ignore the processes established to engage them in good decision making, it is worth asking whether some private choices to tolerate spyware—particularly spyware that creates opportunities for others to remotely assume control of computers—are just too damaging to the network to remain in the realm of private choice.

## FUTURE WORK

The research reported here opens as many questions as it resolves. It is our goal in future work to better understand the factors that lead individuals to install spyware, and how those factors vary in different demographic groups (including older users) and in different situations. We recognize the limitations of a laboratory study, and are hopeful that it will be possible to conduct more extensive studies of software installation, and more general questions of a personal computer's life cycle, on computers installed in individual homes and offices. Further, we believe that appropriate notice can help reduce installation of unwanted spyware, but also recognize that "appropriate" may vary by individual. We would particularly welcome further research into possible negative effects of excessively long

and impenetrable EULAs, and other explorations into interfaces for more effectively presenting the relevant information to users for meaningful, informed, consent.

## ACKNOWLEDGEMENTS

We wish to thank Microsoft for funding our work. We also appreciate the help of Tye Rattenbury, Frances Tong and Xin Wang concerning statistical analysis. We are greatly indebted to Susheel Daswani for constructing the experimental framework. Finally, we thank Becca Shortle, Chris J. Hoofnagle, Ira Rubenstein and the anonymous reviewers for their valuable feedback and suggestions. This work is supported in part by the National Science Foundation under ITR award ANI-0331659.

## REFERENCES

1. Abrams, M., M. P. Eisenhauer, and L.J. Sotto Letter to Federal Trade Commission. March 29, 2004. Re: alternative forms of privacy notices, project no. P034815. Hunton & Williams: The Center for Information Policy Leadership.
2. Acquisti, A., and J. Grossklags. 2005. Privacy and rationality in individual decision making. IEEE Security & Privacy 3(1): 26–33.
3. Anti Spyware Coalition, Anti Spyware Coalition Definitions and Supporting Documents, Working Report (June 29, 2006), available at http://www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf
4. AOL and National Cyber Security Alliance. 2004. AOL/NCSA online safety study, (October). http://www.security.iia.net.au/downloads/safety_study_v04.pdf
5. Bellia, P. L. Spyware and the Limits of Surveillance Law, 20 Berkeley Tech. L.J. 1283 (2005)
6. Bellotti, V. and A. Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In Proceedings of The Third European Conference on Computer Supported Cooperative Work (ECSCW'93). Milan, Italy: Kluwer Academic Publishers.
7. Blanke, J. M. "Robust Notice" and "informed Consent:" the Keys to Successful Spyware Legilsation, 7 Coum. Sci & Tech. L. Rev. 2 (2006)
8. Buenaventura, M. A. Teaching a Man to Fish: Why National Legislation Anchored in Notice and Consent Provisions is the Most Effective Solution to the Spyware Problem, 13 Rich. J.L. & Tech. 1 (2006)
9. Calinski, R.B. and Harabasz, J. 1974. "A Dendrite Method for Cluster Analysis," Comm. in Statistics, vol. 3, pp. 1–27.
10. Cranor, L.F., J. Reagle, and M. S. Ackerman.1999. Beyond concern: Understanding net users' attitudes about online privacy. In Ingo Vogelsang and Benjamin M. Compaine, eds. The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy. Cambridge, Massachusetts: The MIT Press, p. 47-70
11. Cutrell, E., M. Czerwinski, and E. Horvitz. 2001. Notification, disruption, and memory: Effects of messaging interruptions on memory and performance. Proceedings of Interact 2001: IFIP Conference on Human-Computer Interaction, Tokyo, Japan. http://research.microsoft.com/~cutrell/interact2001messaging.pdf.
12. Dhamija, R., Tygar, J. D., and Hearst, M. 2006. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). ACM Press, New York, NY, 581-590.
13. Earthlink. 2005. Earthlink spy audit: Results complied from Webroot's and Earthlink's Spy Audit programs, http://www.earthlink.net/spyaudit/press.
14. Federal Trade Commission, Monitoring Software on Your PC: Spyware, Adware, and Other Software, http:www.ftc.gov/os/2005/03/050307spywarerpt.pdf
15. Friedman, B., Howe, D., and Felten, E. 2002. Informed Consent in the Mozilla Browser: Implementing Value Sensitive Design. In Proceedings of the 35th Annual Hawaii international Conference on System Sciences (Hicss'02)-Volume 8 - Volume 8 (January 07 - 10, 2002). HICSS. IEEE Computer Society, Washington, DC, 247.
16. Goecks, J. and Mynatt., E.D. 2005. Supporting Privacy Management via Community Experience and Expertise, Proceedings of 2005 Conference on Communities and Technology, p. 397-418.
17. Good, N. S. and Krekelberg, A. 2003. Usability and privacy: a study of KaZaA P2P file-sharing. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Ft. Lauderdale, Florida, USA, April 05 - 10, 2003). CHI '03. ACM Press, New York, NY, 137-144.
18. Good, N., Dhamija, R., Grossklags, J., Thaw, D., Aronowitz, S., Mulligan, D., and Konstan, J. 2005. Stopping spyware at the gate: a user study of privacy, notice and spyware. In Proceedings of the 2005 Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 06 - 08, 2005). SOUPS '05, vol. 93. ACM Press, New York, NY, 43-52
19. Hawkey, K. and Inkpen, K. M. 2006. Keeping up appearances: understanding the dimensions of incidental information privacy. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). ACM Press, New York, NY.
20. Jensen, C., and C. Potts. 2004. Privacy policies as decision-making tools: An evaluation on online privacy notices. In CHI 2004 Connect: Conference Proceedings: April 24-29, Vienna Austria: Conference on Human Factors in Computing Systems 6(1): 471–78. New York: Association for Computing Machinery.
21. Karat, C., Karat, J., Brodie, C., and Feng, J. 2006. Evaluating interfaces for privacy policy rule authoring. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson, Eds. CHI '06. ACM Press, New York, NY, 83-92.
22. Norman, D. A. The Design of Everyday Things, 1988.
23. Spiekermann, S., J. Grossklags, and B. Berendt. 2001. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In Proceedings of the Third ACM Conference on Electronic Commerce, Association for Computing Machinery (ACM EC'01), 38-47. New York: ACM Press.
24. Stiegler, M., Karp, A. H., Yee, K., Close, T., and Miller, M. S. 2006. Polaris: virus-safe computing for Windows XP. Commun. ACM 49, 9 (Sep. 2006), 83-88.
25. Trafton, J. G., E. M. Altmann, D. P. Brock, and F. E. Mintz. 2003. Preparing to resume an interrupted task: Effects of prospective goal encoding and retrospective rehearsal. International Journal of Human Computer Studies 58(4): 583–603.
26. Van Dantzich, M., R. Daniel, E. Horvitz, and M. Czerwinski. 2002. Scope: Providing awareness of multiple notifications at a glance. Proceedings of Advanced Visual Interfaces 2002, Trento, Italy.
27. Vila, T., R. Greenstadt, and D. Molnar. 2004. Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market. In Economics of Information Security. Vol 12 of Advances in Information Security, eds. L.J. Camp and S. Lewis, 143-154. Boston: Kluwer Academic Publishers.
28. Wayne R. Barnes, Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance, 39 U.C. Davis L. Rev 1545 (2006)
29. Winn, J. Contracting Spyware by Contract, 20 Berkeley Tech. L.J. 1345 (2005)

# GEORGIA LAW REVIEW

VOLUME 41 FALL 2006 NUMBER 1

ARTICLES

## PROTECTING THE INNER ENVIRONMENT: WHAT PRIVACY REGULATION CAN LEARN FROM ENVIRONMENTAL LAW

*Dennis D. Hirsch**

TABLE OF CONTENTS



* Associate Dean and Professor, Capital University Law School. The author would like to thank the following for their insights about privacy and environmental law and/or their comments on drafts of this Article: Kirk Herath, Benita Kahn, Professors James Beattie, Mark Brown, Alex Cameron, Charles Cohen, Shi-Ling Hsu, Daniel Kobil, Stephen Johnson, J.B. Ruhl, James Salzman, Daniel Solove, Daniel Steinbock, Katherine Strandburg, Peter Swire, Jonathan Weinberg, and the members of the Ohio Legal Scholarship Workshop. He would also like to thank Capital University Law School for supporting the writing of this Article with a summer research grant, and Tiffany Auvdel for the diligent and useful research assistance that she provided.

steal Donna's name, credit card number, and security code. An identity thief runs up $10,000 in purchases on her credit card. Donna has to spend much time and money sorting out this mess and is never able to re-establish her good credit rating. The Information Revolution has indeed damaged Donna's privacy.

## III. PRIVACY INJURIES ARE LIKE ENVIRONMENTAL HARMS

The privacy injuries of the Information Age are structurally similar to the environmental damage of the smokestack era. Two key concepts that have been used to understand environmental damage—the "negative externality" and the "tragedy of the commons"—also shed light on privacy injuries.

### A. NEGATIVE EXTERNALITIES

Negative externalities exist whenever someone utilizes a resource but is able to impose on others the costs of that use.[135] The costs are said to be "external" to the user and to result in "negative externalities."[136] For example, a manufacturer of steel pipes must pay to use resources such as iron or labor. If it wishes to emit pollutants, however, the costs (such as respiratory problems among the surrounding populace) are borne not by the manufacturer but by others in society. Since it does not have to bear these costs, the company has little incentive to minimize them. Instead, it will wastefully "use up" the clean air resource in the way that it would never consume iron, labor, or any other resource for which it had to pay.[137] This leads the company, and others like it, to create too much air pollution and other negative externalities. To solve this problem, it is necessary to force the company to bear or "internalize" the costs of the pollution that it is creating. Only then will it have an incentive to reduce it.[138]

---

(describing data spill by credit card processor that may have led to identity theft).

[135] *See* SALZMAN & THOMPSON, *supra* note 30, at 17–18 (noting externality exists where factory pollutes air but does not have to pay costs associated with this pollution).

[136] *Id.* at 18.

[137] *Id.*

[138] *Id.* ("[Where] factory has to pay for the external harm it causes, then it will reduce its pollution. The process for forcing the factory to recognize environmental and social costs is

B. THE TRAGEDY OF THE COMMONS

The "tragedy of the commons" explains how economically rational, self-interested use of a commonly owned resource can result in the destruction of that resource.[139] The classic example, drawn from an essay by Garrett Hardin, concerns cattle herders who graze their animals on a commonly owned field of grass.[140] Hardin theorized that from the perspective of the individual cattle herder it is rational to increase the number of his cattle that are grazing in the field. He gets the full benefit of adding another animal but shares the cost of using up the grass with all others who have the right to graze in the field.[141] The individual herder, pursuing his self-interest, will accordingly add another head of cattle to the field, then another, and so on. So will the other herders. Eventually, there will be so many cattle that they will eat down the grass to the point that it cannot regenerate itself, rendering the field useless for grazing purposes. All cattle herders will lose access to the resource. What was individually rational turns out to be collectively ruinous.[142] The same dynamic can be seen when fishermen exploit ocean stocks to the point that the fish population crashes or when farmers draw water from a common acquifer at such a rate that it is not able to recharge itself and stops producing plentiful water.[143] In each of these situations, the users' over-exploitation of the resource ends up depriving them of its benefits. It is this characteristic that separates a "true" tragedy of the commons from other situations in which exploiters of common resource impose externalities but do not diminish their own ability to utilize the resource.[144]

---

known as *internalizing the externalities*.").

[139] The tragedy of the commons thus serves as a counterpoint to Adam Smith's "invisible hand" which posits that the pursuit of individual self-interest will enhance the wealth of the larger society. *See* Shi-Ling Hsu, *What Is a Tragedy of the Commons? Overfishing and the Campaign Spending Problem*, 69 ALB. L. REV. 75, 78–79 (2005) (contrasting Hardin and Smith).

[140] *See generally* Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968) (discussing phenomenon known as "tragedy of the commons").

[141] *Id.* at 1244.

[142] *See id.* ("Freedom in a commons brings ruin to all."); *see also* SALZMAN & THOMPSON, *supra* note 30, at 16 ("[I]ndividually rational behavior is collectively deficient.").

[143] SALZMAN & THOMPSON, *supra* note 30, at 16–17.

[144] *See* Hsu, *supra* note 139, at 76 ("[A] true tragedy of the commons specifically involves

C. SPAM, EXTERNALITIES, AND THE TRAGEDY OF THE COMMONS

These concepts provide insight into the spam problem. A spammer incurs small costs for computer equipment and labor[145] but imposes the larger costs of his activity—the time spent deleting spam, the cost of filters, the lost email messages, and the higher connection fees—on the recipients of his email barrage.[146] Spam spewed from a computer thus creates a negative externality in much the same way that air emissions from a smokestack do.[147] Since spammers have no incentive to limit these external costs, they wastefully use up the "inbox" resource sending as many as 250 million spam emails *per day*.[148] As in the environmental context, the way to get spammers to reduce this flow is to force them to internalize the costs of their spam.

The failure to do so may well lead to a classic tragedy of the commons.[149] To understand this, it is important to view the situation from the spammer's perspective. Any spammer in possession of the proper email address may use it to market a

---

a situation in which the resource users are detracting from their own ability to continue to exploit the resource.").

[145] The cost to a spammer of sending an email message is roughly 0.019 cents per message. MARTIN ABADI ET AL., BANKABLE POSTAGE FOR NETWORK SERVICES 2 (Springer-Verlag 2003) (copy on file with author), *available at* http://research.microsoft.com/research/sv/pennyblack/demo/ticketserver.pdf.

[146] *See* Zhang, *supra* note 87, at 305 ("Unlike traditional methods of advertising, spam imposes the bulk of advertising fees on recipients rather than spammers."); *see also supra* notes 88–94 and accompanying text (describing these costs).

[147] *See* Mossoff, *supra* note 27, at 665 ("In economists' terms, spammers are *creating negative externalities* through the use of their email accounts.") (emphasis added); *see also* Hirsch, *supra* note 28, at 244. In at least one respect, spam may appear to differ from environmental pollution. In the environmental context, the polluter intends to make a useful product and pollutes as an incidental side-effect of this activity. In the spam situation, the spammer intends to send the email, and the harm arises directly from this. But are the situations really so different? A spammer's intent is to market a product, not to clog up an inbox. In fact, most spammers will not want to overcrowd an inbox since this will be detrimental to spam marketing. Much like a polluter, the spammer intends to produce something useful from his viewpoint (an advertisement) but ends up damaging others as an inherent side-effect of this behavior. It may be more difficult to distinguish the beneficial from the harmful side of the spammer's activity because both are contained within the same email message. But that does not change the fact that, as in the environmental arena, the spammer's activity has both a positive and a negative component, and the harmful side is externalized onto others.

[148] *See supra* note 85 and accompanying text.

[149] Hirsch, *supra* note 28, at 244–45.

product,[150] and so all may be said to have access to this resource. From the spammer's perspective, the benefit to sending an additional email lies in the increased chance of making a sale. The cost lies in using up the attention that the recipient can devote to reading email, thus decreasing the chance that the recipient will actually view any given marketing message. As with Hardin's cattle herder, the spammer appropriates the full benefit of each email (in terms of the opportunity to make a sale) but shares the cost (in terms of the recipient's reduced attention) with all other spammers who are trying to market to that recipient. Moreover, the spammer knows that if he refrains from sending an email in order to reduce the recipient's email burden, his competitors are likely to fill the space he has left free.[151] These circumstances, coupled with the minimal cost of sending additional email,[152] will cause the rational spammer to send out more and more email just as they convince cattle herders to continue to add more and more cattle. This explains the alarming trend in the number of spam emails over the past few years—140 billion spam messages in 2001,[153] 261 billion in 2002,[154] and 2 trillion in 2004[155]—with no end in sight. Spammers have become like cattle herders, driving more and more of their beasts into the commons to gobble up the available grass, although here the cattle are spam messages, the commons is the available space in the inbox (or conceptualized differently, the available

---

[150] *See* Hsu, *supra* note 139, at 79 n.25 (defining "open access" resource). Filtering devices can edit out some spam messages and thus limit access to the inbox commons. But the emergence of these programs has led to little more than a technological arms race with the spammers, who are continually coming up with ways to circumvent the filters. Mossoff, *supra* note 27, at 630. Moreover, if the filters become too fine, then desired emails might be diverted or deleted, thereby destroying the utility of email—another tragedy, but this one achieved by means of excessive fencing rather than excessive use.

[151] *See* Hsu, *supra* note 139, at 94 (noting that in true tragedy of the commons, users of resource are generally rivals in their race to exploit it).

[152] As noted above, the cost is 0.019 cents per message. ABADI ET AL., *supra* note 145, at 2; *see also* Robert E. Kraut et al., *Pricing Electronic Mail to Solve the Problem of Spam* 4 (Yale Int'l Ctr. for Fin., Working Paper No. 05-24, 2005) (copy on file with author), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=753664 (arguing that low cost of sending email makes it "economically rational for individual commercial emailers to distribute their messages as widely as possible").

[153] *See supra* note 86 and accompanying text.

[154] Mossoff, *supra* note 27, at 627.

[155] Zhang, *supra* note 87, at 304; *see also supra* note 87 and accompanying text.

attention of the recipient), and the grass is the lucrative business of selling Viagra, mortgages, or pornography.

As with the grazing field, the logical result of this behavior will be to ruin the inbox as a valuable marketing resource. Individuals will receive so many spam messages that they will begin to ignore all of them, filter them all out, or abandon email for other modes of communication and shut down their inboxes (under our analogy, this would be equivalent to the destruction of the grazing field). Congress has recognized this very risk, stating that "[l]eft unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool."[156] It may turn people off from using email, thereby destroying the very resource that spammers relied on in the first place.[157] This makes the spam phenomenon a true tragedy of the commons since those exploiting the inbox (the spammers) will have damaged their own ability to make use of this resource for their marketing campaigns (in addition to causing a lot of harm to individual email users along

---

[156] S. REP. NO. 108-102, at 6, *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2352; *see also* Hansell, *supra* note 90 (noting that Internet service providers believe email is becoming "an increasingly unreliable" mode of communication); Kraut et al., *supra* note 152, at 3 (stating that spam is "growing rapidly and threatens to choke off e-mail as a reliable and efficient means of communication over the Internet").

[157] *See "Unsolicited Commercial Email" Before the U.S. Senate Committee on Commerce, Science and Transportation*, 108th Cong. (2003), *available at* 2003 WL 21187271 (statement of Mozelle W. Thompson, Commissioner, Federal Trade Commission) ("[T]he volume of unsolicited email is increasing exponentially and . . . we are at a 'tipping point,' requiring some action to avert deep erosion of public confidence in email that could hinder, *or even destroy*, it as a tool for communication and online commerce.") (emphasis added); Dennis O'Reilly, *Is E-Mail Doomed?*, PC WORLD, June 21, 2004, http://www.pcworld.com/article/id, 116606/article.html (stating that some experts worry "it won't be possible to sufficiently stem the tide" as people are moving away from email); *see also* CAN-SPAM Act of 2003, 15 U.S.C.A. § 7701(a)(2) (West 2003) (finding that "[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail"); S. REP. NO. 108-102, at 7 ("[I]ndustry analysts are concerned that this trend could influence millions of consumers to abandon the use of e-mail messaging as a viable means of communication.").

the way).[158] Left unchecked, spam will result in the killing of "the killer ap."[159]

### D. PERSONAL INFORMATION, EXTERNALITIES, AND THE TRAGEDY OF THE COMMONS

When a website gathers and sells personal information about one of its users, or an Internet marketer or data miner uses this information, they cause that individual to lose a degree of privacy. This cost is borne by the user and is external to the business. It is a negative externality.[160] As in the environmental context, this means that the companies involved have little incentive to curtail their use and so will tend to over-engage in the activities that create the externalities.[161] "In economic terms, the companies collecting personal information impose a negative externality on consumers. Because these companies benefit from the information they collect, but do not face the costs they impose (i.e., the violation of consumers' privacy), they collect 'too much' information."[162] Just as factories have no reason to refrain from filling the air with pollutants, these

---

[158] When excessive spam causes an individual to abandon email, this harms more than the spammers. It also injures the individual associated with that email account (the recipient) and those who send nonspam messages to that person. Yet these additional injuries do not change the core fact that the spammers, through their over-exploitation of the inbox resource, are also damaging themselves. It is this that makes the spam situation a true tragedy of the commons. Hsu, *supra* note 139, at 76, 80–82. Were they to recognize the long-term implications of the situation and have a means of reaching a rough consensus, such users might well invite regulation in order to avoid the destruction of their common resource. *Id.* at 80.

[159] *See* O'Reilly, *supra* note 157. The process is already underway. According to a 2003 poll by Pew Internet and American Life Project, 25% of respondents said that spam is already causing them to curtail their use of email. Jonathan Krim, *Senate Votes 97–0 to Restrict E-Mail Ads: Bill Could Lead to No-Spam Registry*, WASH. POST, Oct. 23, 2003, at A01.

[160] *See* Hirsch, *supra* note 28, at 245.

[161] *See* Schwartz, *supra* note 37, at 833 (noting that users of personal data are likely to engage in "wasteful behavior" because they do not have to pay true costs of using it).

[162] Hahn & Layne-Farrar, *supra* note 66, at 16; *see also* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (Brookings Inst. Press 1998) (noting companies "internalize[ ] the gains from using the information but can externalize some of the losses and so ha[ve] a systematic incentive to overuse it"); Nehf, *supra* note 28, at 79–80 (noting misuse of personal information, like environmental damage, "imposes significant external costs"); Samuelson, *supra* note 11, at 1132–33 ("[F]irms collect and process personal data . . . [b]ecause they are not forced to internalize the societal costs of private sector processing of personal data.").

companies will not hesitate to collect, use, and flood the market with detailed, personal information.[163]

Once again, a tragedy of the commons lurks around the corner.[164] Here, the "commons" is the collective willingness of individuals to reveal their personal information on the Web. It is the trust that their informational privacy will, more or less, be respected. Each time a website sells personal data, a data miner infers sensitive information, or a data spill exposes people to identity theft, a bit of that trust is lost, and a bit of the commons disappears. Websites, marketers, and data miners receive all the benefits of their use of personal information but share the cost (in terms of the erosion of trust) with all others who depend on individuals to provide personal information on the Web. This gives them an incentive to continue collecting, selling, and using as much personal information as they possibly can.[165] Companies that refrain from doing so will generally lose out to competitors who are not so temperate.[166] This increases the incentive to make use of the information while the individual is still willing to share it. The end result promises to eat up and destroy the very willingness to reveal personal data that these businesses depend on. As with spam, this will be a true tragedy of the commons because over exploitation of the personal information resource will end up harming those who are engaged in the exploitation.[167] Studies show that this is already happening. According to one poll, "an overwhelming majority of Americans consistently report that they are deterred from using the Internet more than they currently do because of privacy-related fears."[168]

---

[163] Of course, the factory harms the external environment, while the privacy loss is an internal one. If the phrase is not too glib, such privacy harms could accordingly be referred to as "*internal* externalities." I am indebted to Professor Craig Nard for helping me coin this (hopefully) amusing phrase.

[164] Hirsch, *supra* note 28, at 245–46.

[165] *See* TURKINGTON & ALLEN, *supra* note 3, at 420 ("Disclosure of personal data is costless to firms and may net profits, creating incentives to overuse such data.").

[166] The exception would be the company that is able to "brand" itself as being especially protective of consumer privacy and turn this into a competitive advantage.

[167] Hsu, *supra* note 139, at 76 (defining a "true" tragedy of the commons).

[168] Litan, *supra* note 3, at 1058 & n.46 (citing Harris survey finding that "92% of consumers are 'concerned' and 67% are 'very concerned' about misuse of their personal data online"). Others recount that "an installed base of millions of users can quickly evaporate if customers do not trust the provider" to treat their personal information with care. Samuelson, *supra* note 11, at 1160.

Carried to its logical conclusion, this trend will lead consumers to abandon e-commerce and other online activities for "real" equivalents that protect privacy better.[169] Consumer trust—the commons on which the data driven businesses rely—will erode. This will undermine the viability of e-commerce and other beneficial online activities.

## IV. ENVIRONMENTAL LAW AND POLICY AS A MODEL FOR PRIVACY REGULATION

How can we avoid the tragedy of the commons that threatens email, e-commerce, and other online activity? Here, too, there is much to learn from environmental law and policy. The field has spent forty years preventing just such tragedies in the natural world. Many programs have been implemented, regulatory experiments conducted, reports written, and policy discussions held. This abundance of activity has made environmental law and policy—perhaps more than any other area of administrative practice—the center of creative thinking about regulation.[170]

This experience could greatly benefit the privacy field. Today, there is a growing sense that the Information Revolution has produced unprecedented damage to privacy. There have been numerous calls for legislation and regulation,[171] and some has been enacted.[172] Yet even as the desire for government intervention has

---

[169] Samuelson, *supra* note 11, at 1129 ("The trust necessary for electronic commerce to flourish requires the interests of individuals in information privacy to be given appropriate deference. . . ."); *accord* Netanel, *supra* note 79, at 474 ("[C]onsumers will not use the Internet for electronic commerce unless they are assured about personal privacy protection.").

[170] SALZMAN & THOMPSON, *supra* note 30, at 41.

[171] *See* Hahn & Layne-Farrar, *supra* note 66, at 29–50 (surveying recent and proposed privacy legislation).

[172] *See, e.g.*, Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12, 15, 16 & 18 U.S.C.) (protecting financial data); Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501–6506 (2000)) (protecting children under thirteen from online collection of personal information); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2520, 2701–2711, 3121–3127 (2000)) (protecting against monitoring of electronic communications such as telephone calls or emails); Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C. § 1028(a)(7), (b)(1), 28 U.S.C. § 994 (2000)) (making identity theft a crime); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of

It also offers lessons for program design. Under the environmental model, the government, not a private party, collects the emission fees. By departing from this model, Gates, AOL, and Yahoo opened themselves to the charge of profiteering. A proposal, such as the one recommended in this Article, that employs a government-imposed fee would stand on stronger footing. The environmental experience also suggests that Gates's more ambitious proposal was preferable to Yahoo and AOL's limited plan. The Yahoo and AOL proposal would not meaningfully change spammers' incentives and would allow them to continue sending free email if they chose not to opt for the "preferred" system. It would thus seek payments from those who send messages that have real value, while allowing the most abusive spammers to escape paying for the costs of their activities. It would also give the ISPs (AOL and Yahoo) an incentive to filter out more and more "spam" email so as to push business to pay for the certified status. Just as an emission fee system includes all sources of pollution, an email fee system should cover all sources of email. Gates was on the right track with his more ambitious idea, although he erred by proposing that Microsoft collect the fee.

## VI. USING REGULATORY COVENANTS TO PROTECT INFORMATIONAL PRIVACY

The environmental experience can also provide insight into current efforts to protect informational privacy. In 1996 and 1997, the Federal Trade Commission (FTC) told the largest online businesses that if they did not do more to protect informational privacy, it would require them to do so.[283] This caused AOL, Hewlett-Packard, IBM, and others to form the Online Privacy Alliance (OPA) and to develop, on their own, a set of industry guidelines for the collection, use, distribution, and security of personal data.[284] As a result, the FTC held off on federal regulation.

---

[283] Keith Perine, *The Persuader*, INDUS. STANDARD, Nov. 13, 2000, *available at* LEXIS.

[284] *Id.*; *see also* Litan, *supra* note 3, at 1059 (stating that OPA initiative was "prompted by the threat of actual regulation"). The OPA Guidelines require all organization members to implement the following five measures: (1) adopt and put into practice a "policy for protecting the privacy of individually identifiable information" and encourage the adoption of such

Subsequently, it became apparent that the OPA Guidelines would not be sufficient. Only a hundred or so companies and associations joined the group, with major players such as Amazon.com and Lycos choosing to remain on the sidelines.[285] Pressure has again begun to build for federal regulation, leading even the OPA to conclude that it has "come up short."[286]

The FTC and OPA's experiment was more significant than most realize. Viewed through the lense of environmental policy, it can be seen as a step, albeit an incomplete one, toward use of a second generation tool known as a regulatory covenant. The environmental experience suggests that regulatory covenants can be very useful in situations—such as the one that the privacy field currently faces—where society needs to regulate but wants to minimize interference with the regulated industry.[287] A fuller understanding of environmental covenants shows how this instrument might be effectively employed to protect informational privacy.

Under the environmental covenant approach, government officials sit down with the regulated industry and hammer out an agreement on pollution reduction. The conversation usually takes place against a backdrop of threatened prescriptive (first generation) regulation.[288] The government offers that it will not impose such requirements if an agreement is reached.[289] Sometimes, the negotiation includes a respected environmental group that functions

---

policies by those organizations with whom they do business; (2) make sure that the privacy policy is "easy to find" and understand and that it states clearly the content, use, and distribution of the information being gathered and the choices available to individuals with respect to the collection, use, and distribution of their information; (3) provide individuals with a choice regarding how their information will be used that, at least, includes the ability to "opt-out" of such use; (4) take measures to assure data reliability and to avoid "data loss, misuse[,] or alteration"; and (5) implement procedures to assure that the data are "accurate, complete [,] and timely" and provide a mechanism to correct inaccuracies. *See* Online Privacy Alliance, Guidelines for Online Privacy Policies, http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited Oct. 25, 2006).

[285] Perine, *supra* note 283.

[286] *Id.*

[287] *See supra* notes 171–80 and accompanying text (describing how privacy field faces these competing, and somewhat contradictory, demands).

[288] JOHNSON, *supra* note 212, at 258.

[289] *Id.* at 259.

as a third-party observer but retains the ability to go public and discredit the process if it smells a "rat."[290]

Industry has more input in developing a covenant than a command-and-control regulation, tending to make covenants more practical and workable from an industry point of view.[291] Covenants often take the form of pollution reduction benchmarks or performance goals, rather than specific, technology-based requirements, which leaves an industry with significant flexibility in determining how to achieve the objectives.[292] In addition, covenants often employ longer time frames that fit with the normal cycles of business planning and investment.[293] These features make covenants attractive to regulated parties. Government can benefit too; it often seeks and obtains steeper pollution reductions than those that political realities would allow it to achieve through prescriptive regulation.[294] This benefit can attract environmental and community group support. The covenanting approach thus follows "the rationality of consensus—based on Coasian bargaining principles."[295] It allows the parties to negotiate an arrangement that all view as superior to that which they would face without such an

---

[290] *See* Stewart, *supra* note 29, at 61 (noting importance of having "all relevant social interests with a stake in the outcome [be] adequately represented at the bargaining table").

[291] *Id.* at 82.

[292] *Id.* at 81–82.

[293] *See* Daniel J. Fiorino, *Toward a New System of Environmental Regulation: The Case for an Industry Sector Approach*, 26 ENVTL. L. 457, 486 (1996) (stating that length of covenants "allow industry to take a long-term strategic perspective in their environmental planning"); Stewart, *supra* note 29, at 82 (revealing that covenants often specify "a fixed, normally multi-year period" in which industry must come into compliance). This longer time frame allows industry to research the most cost-effective way of achieving the end result and to undertake a longer term research and investment plan. Stewart, *supra* note 29, at 82. Government usually commits not to pass regulation during this time period unless it is urgently required. *Id.*

[294] Stewart, *supra* note 29, at 82–83 ("In return for the flexibility and extended compliance schedule provided, government will generally insist on steep reductions."); *see also* JOHNSON, *supra* note 212, at 236 (noting governments and environmental groups enter covenants because they can "obtain commitments . . . [for] greater protection for the environment than would be required under traditional command-and-control laws"). Industry often views this as the "price" of the increased flexibility, time, and control that it is receiving. Stewart, *supra* note 29, at 83. In addition, covenants can also allow government to achieve effective controls more quickly and at less administrative cost than traditional methods since the agreement does not have to go through protracted regulatory processes. *Id.*

[295] Stewart, *supra* note 29, at 61.

agreement.[296] In theory, it *must* yield such a result since the parties enter into environmental covenants voluntarily.[297] Thus, any who did not benefit could theoretically withhold their consent.

The Dutch have been the leading practitioners of this method and their Energy Efficiency Benchmarking Covenant illustrates it well.[298] International agreements on climate change required the Netherlands to reduce significantly its carbon dioxide ($CO_2$) emissions.[299] Concerns about regulatory costs led regulators to employ the covenanting method rather than prescriptive regulation.[300] They offered to sit down with the most energy-intensive industries to negotiate a reduction plan, and the industries, knowing that they would otherwise face direct regulation, embraced this opportunity.[301] The resulting covenant sets out a flexible approach to improving energy efficiency over an extended time frame,[302] covers over 80% of Dutch industrial energy use, and has already been credited with reducing $CO_2$ by more than five million tons per year.[303]

Covenants can allow the regulated industry to focus the reduction burden on those facilities that can achieve it at least cost, thereby avoiding some of the inefficiencies of uniform, prescriptive regulation.[304] Their flexible, performance-based standards and longer time frames encourage business investment in cost-effective means of achieving environmental results.[305] Covenants can

---

[296] JOHNSON, *supra* note 212, at 235 ("In theory, everybody wins.").

[297] Stewart, *supra* note 29, at 81.

[298] *See* Commissie Benchmarking, Energy Efficiency Benchmarking Covenant, http://www.benchmarking-energie.nl (Dutch government website providing information on covenant) (last visited Oct. 26, 2006). European governments and the Japanese have used covenants to a greater degree than the United States has. Stewart, *supra* note 29, at 80–81. The European Union has encouraged their use by member states and has published guidelines directing how they can be used. Stephen M. Johnson, *Economics v. Equity II: The European Experience*, 58 WASH. & LEE L. REV. 417, 442–44 (2001). As of the mid-1990s, member states in the European Union have entered into more than 300 agreements with industrial sectors, firms, and associations. *Id.* at 444.

[299] *See* Commissie Benchmarking, *supra* note 298.

[300] *Id.*

[301] *Id.*

[302] *Id.*

[303] *Id.*

[304] JOHNSON, *supra* note 212, at 240.

[305] *Id.* at 236, 240; Stewart, *supra* note 29, at 81–82. Covenants should also reduce a government's administrative costs since the government would no longer need to go through

accordingly represent "an important means of addressing the shortcomings of command-and-control."[306] The approach also has its weaknesses. One is the risk that industry will use political influence and closed-door discussions to negotiate "sweetheart" deals.[307] Having a respected environmental group at the table can reduce this threat. The differentiation that comes from increased flexibility can also make it more difficult to enforce covenants than technology-based regulation.[308] This difficulty is best addressed through effective monitoring of actual emissions, where this is possible, and by stiff penalties for noncompliance. Finally, the legal status of environmental covenants is still unsettled under U.S. law.[309]

The covenanting approach could be used to protect informational privacy. Just as the Dutch government was getting ready to regulate $CO_2$ emissions, the federal government is now considering actions to protect informational privacy.[310] This should give information-intensive industries a reason to seek a deal. The existence of respected privacy advocacy groups[311] that might add ideas and credibility to the negotiation also augurs well. The conditions are right for the federal government to sit down with the industries that collect and use personal information and to negotiate protective measures that are also workable for business.

---

the process of identifying the "best" technology.

[306] Stewart, *supra* note 29, at 80; *accord* JOHNSON, *supra* note 212, at 240 ("[R]egulatory contracting arguably redresses many of the traditional criticisms of command-and-control regulation.").

[307] Stewart, *supra* note 29, at 83.

[308] *Id.* at 85; *see also* JOHNSON, *supra* note 212, at 259 (stating that voluntary agreements are often criticized for lack of "sufficient provisions to monitor compliance").

[309] JOHNSON, *supra* note 212, at 259 ("[T]he legal status of a voluntary agreement is ambiguous."); *see also* Stewart, *supra* note 29, at 84–85 (presenting many questions that lack clear answers). There are open questions about who can enforce these agreements and what the remedies for breach should be. Stewart, *supra* note 29, at 84. For example, it is not clear whether a citizen has standing to enforce the agreement against industry. *Id.* Similarly, questions exist as to industry's rights in the event that government does not abide by the agreement and issues prescriptive regulations: can industry bring suit based on the agreement? *Id.* Background principles of law are not yet well developed on these issues. At present, it is advisable to address such matters in the text of the covenant itself.

[310] R. Christian Bruce, *Look for Comprehensive Privacy Bill in Spring 2006, Senate Staffer Says*, 4 Privacy & Sec. L. Rep. (BNA) 1048 (Aug. 15, 2005); *see also* Perine, *supra* note 283 (describing growing consensus for regulation to protect online privacy).

[311] The Center for Democracy and Technology is one such group. *See* Ctr. for Democracy and Tech., http://www.cdt.org (last visited Oct. 25, 2006) (providing information about this organization).

While the FTC and OPA took a tentative step in this direction, the environmental experience shows that they could have handled it better in several regards. First, FTC initiated the discussion but then allowed the OPA to develop the guidelines on its own.[312] This resulted in standards that lacked an official imprimatur, were too friendly to industry, and ultimately lacked sufficient credibility and breadth.[313] Had the FTC followed the environmental model, it would have directly negotiated the standards with the OPA. Second, the FTC failed to follow through on its threat of prescriptive regulation for those companies that did not sign on to the agreement.[314] Thus, the members of the OPA took on commitments while their competitors faced none. Once again, this departed from the environmental model in which those who fail to participate in the covenant face prescriptive regulation. Finally, unlike environmental covenants, the FTC gained no power to enforce the guidelines. This left the Commission with no middle-ground course of action, forcing it to either remain passive or seek full regulation. Had the FTC and industry followed the environmental model more closely, they might have emerged with a more effective arrangement.

This discussion is not idle speculation. The Dutch have used covenants to protect information privacy, and their effort appears to be working much better. The Dutch Personal Data Protection Act of 1999[315] establishes the conditions under which it is lawful to process personal data,[316] mandates notice to the government before initiating certain data processing operations,[317] requires processors to share certain information with the data subject,[318] and imposes other protections. As an alternative to these requirements, the Act allows an industry sector to draw up a code of conduct for processing of personal data and to submit it to the Data Protection Agency.[319] If

---

[312] *See supra* notes 283–86 and accompanying text.

[313] *See supra* notes 283–86 and accompanying text.

[314] *See supra* note 285 and accompanying text.

[315] Wet bescherming persoonsgegevens [Personal Data Protection Act], Stb. 3022 (2000) (Neth.), *translated in* http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple.

[316] *Id.* ch. 2.

[317] *Id.* ch. 4.

[318] *Id.* ch. 5.

[319] *Id.* ch. 3, art. 25(1).

approved, compliance with the code is deemed compliance with the Act,[320] and the Agency gains the right to enforce it through the imposition of civil penalties.[321] An approved code thus becomes a tailored compliance plan geared specifically to the "particular features" of the sector.[322] As of 2002, the agency had approved twelve codes of conduct covering such sectors as banking, insurance, direct marketing, health, and pharmaceutical research.[323] By way of illustration, the code for financial institutions establishes industry standards for the use of personal data in assessing potential customers[324] and in marketing[325] and provides special protections for sensitive categories of personal data, such as health information[326] or data related to criminal offenses.[327] The rapid proliferation of these agreements suggests that both government and industry like them and that the public is accepting them. They show that covenants could play an important role in privacy protection.

A covenant governing the data mining industry might have helped our hypothetical American, Donna. As in the Dutch Code of Conduct for Financial Institutions, the government could have targeted health information for special protection. Backed by the threat of prescriptive regulation, it could have negotiated restrictions on the collection and sale of such data especially where it is tied to a specific individual. The data mining industry might have accepted this restriction in exchange for clear authorization to continue core features of its business, such as the selling of information for credit checks or marketing. Industry would be at the table and could communicate whether the strategy was workable, while the presence of a reputable privacy organization would promote accountability. The parties might well have arrived at an

---

[320] *Id.*

[321] *Id.* ch. 10, art. 65.

[322] *Id.* ch. 3, art. 25(1).

[323] Peter J. Hustinx, *Co-Regulation or Self-Regulation by Public and Private Bodies—The Case of Data Protection*, *in* FREUNDESGABE BULLESBACH 283, 285 (2002).

[324] Dutch Data Prot. Auth., Code of Conduct for the Processing of Personal Data by Financial Institutions § 5.2, *available at* http://www.dutchdpa.nl/downloads_gedragscode/ged_banken_vzm.pdf?refer=true&theme=purple.

[325] *Id.* § 5.4.

[326] *Id.* § 6.1.

[327] *Id.* § 6.2.

agreement that both protected Donna and provided the industry with sufficient latitude to prosper.

## VII. USING PUBLIC DISCLOSURE TO PROTECT INFORMATIONAL PRIVACY

Another second generation environmental strategy—Pollution Release and Transfer Registers (PRTRs)—would also serve as a useful model for privacy protection. PRTRs inform the public about pollution releases from specific facilities, thereby giving these organizations an incentive to pollute less. For example, the Emergency Planning and Community Right to Know Act (EPCRA) requires companies annually to report the quantity of hazardous chemicals that they have released into the environment or transferred off-site.[328] EPA incorporates this information into the Toxic Release Inventory (TRI), a national computerized database that is available to the public over the Web,[329] and issues an annual report naming those facilities that have released the most toxic substances.[330] No company wants to be near the top of this list.[331] Publication of the TRI accordingly creates a strong incentive for businesses to reduce their toxic releases and "ha[s] been credited with stimulating a dramatic reduction in on-site inventories and releases of toxic chemicals."[332] Between 1988 and 1998, toxic releases reported on the TRI decreased by 45.3%.[333] Notably, TRI

---

[328] 42 U.S.C. § 11023(f)(1)(A)&(B) (2000) (defining toxic chemical threshold amounts); JOHNSON, *supra* note 212, at 197.

[329] 42 U.S.C. § 11023(j); JOHNSON, *supra* note 212, at 197. The public can access the TRI data at http://www.epa.gov/triinter/tridata/index.htm.

[330] JOHNSON, *supra* note 212, at 199.

[331] Disclosure of negative information about a company can lead to a decline in sales, loss of business goodwill, loss of relationships with companies that do not want to be associated with such a business, decline in stock prices, and low retention of employees. *Id.* at 210.

[332] Stewart, *supra* note 29, at 139; *see also* ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 36 (stating TRI has caused substantial drop in toxic air emissions). *See generally* Shameek Konar & Mark A. Cohen, *Information as Regulation: The Effect of Community Right to Know Laws on Toxic Emissions*, 32 J. ENVTL. ECON. & MGMT. 109 (1997) (discussing these effects).

[333] JOHNSON, *supra* note 212, at 211. Similar programs exist at the state level. California's Air Toxics "Hot Spots" Information and Assessment Act of 1987 requires facilities to report on their toxic air emissions. CAL. HEALTH & SAFETY CODE § 44340 (West 2006); *see also* JOHNSON, *supra* note 212, at 202 (describing program). The Massachusetts Toxics Use Reduction Act requires those facilities that use large quantities of toxic materials to provide an inventory of the chemicals that they use. The state government then publishes this inventory to the public

achieved this result without issuing a single, substantive requirement. Instead, it used information disclosure to encourage companies to come up with their own ways of improving environmental performance. In this sense, PRTRs are very much a second generation strategy.

Just as no smokestack company wants to be known as a big polluter, no information-based business will want to be known as one that has "spilled" large amounts of personal information. The incentives may be even stronger in the digital economy. Individuals often cannot choose which producers of industrial chemicals they will patronize. Yet they make direct choices about which credit cards they hold, where they bank, and which e-commerce sites they visit. Recent studies show that they will avoid companies that are more prone to data spills.[334] This should make pollution release registries an effective tool for protecting informational privacy.

Such a federal program—which could be called the Data Release Inventory (DRI)—would require companies that collect and use personal information to report annually how much of it they released that year. As with the TRI, the report should include both intentional releases (e.g., transfers of information to affiliates or other third parties) and unintentional ones (e.g., data security breaches). It should provide these figures both as a single, total amount, and in disaggregated form broken out by whether the release was intentional or unintentional. Government officials would compile this information and publicize it on the Web along with an annual ranking of individual company performance. If the environmental experience is any guide, newspapers and advocacy groups would likely latch onto this data and broadcast it widely. This would create strong incentives to better protect this

---

and posts it on the Internet. MASS. GEN. LAWS ch. 21I, § 3(B) (2002); JOHNSON, *supra* note 212, at 202–03 (describing program).

[334] *See Many Customers Sever Ties with Businesses After Breach Notice, Law Firm Survey Shows*, 4 Privacy & Sec. L. Rep. (BNA) 1214, 1214 (Oct. 3, 2005) (reporting that survey shows data security breach at business causes 19% of consumers to cease dealing with that company and causes 40% to consider doing so). This survey demonstrates that organizations " 'lose customers when a breach occurs,' and that means data security breaches directly impact corporate bottom lines." *Id.* *See also* Larry Ponemon, *What Do Data Breaches Cost Companies? Beyond Dollars, Customers Are Lost*, 4 Privacy & Sec. L. Rep. (BNA) 1310, 1310 (Oct. 24, 2005) (revealing data security breaches increase loss of customers).

information.[335] Indeed, a recent survey found that health care organizations that experienced a data security breach were not doing more to close the leaks because they anticipated that noncompliance would not lead to any " 'public relations or branding problems.' "[336] A public listing of companies' data protection performance would change this.

Such a system might have helped Donna. Credit card companies compete fiercely and will lose clients if they gain a reputation for poor protection of personal information. A DRI would have given Donna's credit card company incentive to improve its data management and security efforts. This might well have protected Donna from the data spill and ensuing identity theft.[337]

By contrast, prescriptive regulation would prove extremely difficult here. Many businesses collect and use personal data. Government regulators would face a mammoth task in trying to learn enough to design and prescribe data management and security practices for them. Even if they could manage this, business and technological developments in these fast-evolving industries would soon render the standards obsolete. A second generation approach that takes advantage of firms' ability to redesign their own operations would work much better.

## VIII. GOVERNMENT SUPPORT FOR ENVIRONMENTAL MANAGEMENT SYSTEMS AS A MODEL FOR IMPROVING THE PROTECTION OF PERSONAL INFORMATION

---

[335] The data security breach statutes that some states have recently passed have already begun to create such incentives. *See, e.g.*, CAL. CIV. CODE § 1798.82 (2006) (requiring disclosure when business experiences data security breach); *California's Breach Disclosure Law Causes Consternation, Questions for Privacy Officers*, 2 Privacy & Sec. L. Rev. (BNA) 1277 (Nov. 10, 2003). One weakness of these statutes is that they may generate so many notices the consumers begin to tune all of them out. *Id.* The DRI approach avoids this problem because it provides only one, well-publicized report per year that summarizes the relevant information. It also allows consumers to compare company performance by looking at a single document, which the breach disclosure statues do not.

[336] Todd Sloane, *Not So Confidential: Patients Have Reason to Be So Worried About Who Is Seeing Their Medical Records*, MODERN HEALTHCARE, Nov. 14, 2005, at 22.

[337] *See* Eric Dash, *Lost Credit Data Improperly Kept, Company Admits: Files Used for Research*, N.Y. TIMES, June 20, 2005, at A1 (describing major data spill by credit card processor that resulted, in part, from credit card companies' failure to monitor and enforce requirement that processor discard personal information immediately after transaction).

At the 2005 Summit Meeting of the International Association for Privacy Professionals, the chief privacy officer (CPO) of a Fortune 500 corporation stated that one of her first actions upon assuming the position was to ask for a copy of the firm's environmental management system (EMS) and adapt it for use in privacy protection.[338] Many of the other privacy officers in the room did not appear to know what an EMS was.[339] The CPO's action points the way to another second generation measure—government promotion of EMS—that could be adapted for use in protecting personal information.

To understand this protection, it is necessary first to know how the EMS has revolutionized environmental management.[340] Traditionally, an environmental officer remained largely independent of other company departments.[341] She was responsible for environmental compliance but was not involved in core decisions about what products the company would manufacture or how it would produce them. Others would make these calls, largely without reference to their environmental effects. An EMS takes down the walls between departments and gets many employees involved in improving environmental performance.[342] It does this through a management system—a set of organizational practices and procedures—that links the environmental manager to other employees and gets them thinking about the environmental dimension of their jobs.[343] For example, an EMS might get a product designer, who traditionally would not have thought much about the environmental consequences of a given design, to consider the

---

[338] Harriet Pearson, CPO, IBM Corp., Remarks at the International Association of Privacy Professionals National Summit Broader Perspectives Track (Mar. 10, 2005).

[339] *Id.*

[340] For a helpful discussion of environmental management systems and how they are designed, see generally Christopher L. Bell, *The ISO 14001 Environmental Management Systems Standard: A Modest Perspective*, [1997] 27 ENVTL. L. REP. (Envtl. Law Inst.) 10,622 (Dec. 1997).

[341] JASON MORRISON ET AL., MANAGING A BETTER ENVIRONMENT: OPPORTUNITIES AND OBSTACLES FOR ISO 14001 IN PUBLIC POLICY AND COMMERCE 40 (Pac. Inst., 2000).

[342] *Id.*; *see also* Gunningham, *supra* note 189, at 356 (stating EMS can change "enterprise's environmental protection culture").

[343] Paula C. Murray, *Inching Toward Environmental Regulatory Reform – ISO 14000: Much Ado About Nothing or a Reinvention Tool?*, 37 AM. BUS. L.J. 35, 47 (1999) (stating that under EMS approach "[e]very employee, at every level, must be accountable for environmental performance within the scope of his or her job responsibilities").

environmental side of her decisions.[344] It might lead her to substitute a nonhazardous raw material for a toxic one, thereby eliminating a hazardous waste stream that required expensive disposal. This could improve both the company's environmental performance and its bottom line.[345] As the U.S. EPA has recognized, EMSs can enhance compliance, pollution prevention, and environmental results.[346] EMSs also provide firms with a means to communicate their environmental commitment to shareholders, consumers, and the public at large.[347] In 1996, the International Organization for Standardization established a voluntary standard, known as ISO 14001, for evaluating environmental management systems.[348] Firms that certify that their EMS complies with the standard are entitled to adapt their existing logo to reflect their precise ISO certification.[349] More than 90,000 organizations are now ISO 14001 certified.[350]

Just as an EMS improves environmental performance, a privacy-focused analogue—call it a Personal Information Management System (PIMS)—could protect informational privacy. The typical privacy officer, much like the traditional environmental manager, is compartmentalized in the privacy "box" and is often unable to affect the core, strategic decisions that are at the root of the company's privacy impacts. A PIMS would connect the privacy officer to other employees in the organization and allow her to work with them to improve the company's privacy performance. It would make her less of an internal compliance officer, who spends the day getting others to meet legal requirements, and more of a *manager* of others'

---

[344] MORRISON ET AL., *supra* note 341, at 40.

[345] *Cf.* EPA Position Statement on Environmental Management Systems and ISO 14001, 63 Fed. Reg. 12,094, 12,095 (Mar. 12, 1998) (discussing EPA's promotion of and generation of EMS's pollution prevention ideas).

[346] U.S. EPA, DRAFT EMS ACTION PLAN FOR PUBLIC COMMENT 16 (Dec. 20, 1999) (copy on file with author).

[347] *See* Murray, *supra* note 343, at 53 (stating EMS provides "the marketing and public relations benefits of independent evidence of environmental commitment").

[348] MORRISON ET AL., *supra* note 341, at ix–x; Murray, *supra* note 343, at 42–43.

[349] *See* INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, PUBLICIZING YOUR ISO 9001:2000 OR ISO 14001:2004 CERTIFICATION 4 (2005), http://www.iso.org/iso/en/iso9000-14000/certification/publicizing/index.html.

[350] *See* Press Release, ISO, Latest ISO Survey Confirms Integration of ISO 9001 and ISO 14001 with World Economy (Sept. 15, 2005), *available at* http://www.iso.org/iso/en/commcentre/pressreleases/archives/2005/Ref967.html.

privacy-related actions. This is what the CPO of the Fortune 500 company was trying to achieve when she adapted her firm's EMS for privacy purposes.

Had OmniData adopted such a system, it might not have sold Donna's health information to prospective employers.[351] Instead, the designer of this product might have paid more attention to privacy and focused instead on providing services that did not rely on sensitive medical information. For example, OmniData might be able to use its databases to deduce whether a prospective employee is the type who moves from job to job. Employers concerned about turnover might find such information to be even more valuable than knowing about the applicant's past illnesses.[352] Much like pollution prevention, such proactive planning would have prevented Donna's privacy-related harm.

In the environmental field, government has played an important role in encouraging and facilitating the use of EMSs. It reduces inspection frequency[353] and enforcement penalties[354] for organizations that adopt an EMS. It has also developed resources for firms interested in implementing an EMS.[355] Government could play an even greater role in promoting the PIMS.[356] It could help to develop the PIMS and explain its potential to industry. Government could even create a standard for evaluating PIMS and could issue certificates to those firms that meet it. None of these measures would require firms to adopt a PIMS or to take any other action.

---

[351] *See supra* notes 131–33 and accompanying text.

[352] It may be difficult to draw this line. Why should information about a potential employee's propensity for leaving a job be fair game but data about that person's health problems be out of bounds? It all depends on how society defines the amount of privacy that an individual has a right to expect. Government—the accountable representatives of the public—could properly claim a role in defining how to draw these lines. Under the PIMS approach outlined above, it would then be up to the regulated parties themselves to figure out how to implement and achieve these publicly defined goals.

[353] For example, the Oregon Green Permits program offers reduced inspection frequency, among other benefits, as an incentive to encourage firms to adopt an EMS. *See* OR. DEP'T OF ENVTL. QUALITY, THE OREGON GREEN PERMITS PROGRAM GUIDE 4–1 (2000) (setting out benefits of adopting EMS and participating in program).

[354] *See* U.S. EPA, *supra* note 346, at 12–13.

[355] These include publication of an EMS implementation guide, establishment of an EMS resource center, and the creation of a database of existing EMSs. *Id.* at 16.

[356] The federal government would probably have to be in charge to avoid duplicative efforts and emerge with a single standard, although states could play a role in initiating this effort.

Instead, these second generation strategies would encourage these companies to internalize the goal of privacy protection and to come up with ways to achieve it. In the complex, fast-moving information economy, this strategy could be an effective way to enhance privacy protection.

## IX. CONCLUSION

From the AOL/Yahoo proposal to the OPA Guidelines to the Fortune 500 company's adaptation of its EMS for privacy purposes, the information economy seems to be groping its way towards second generation strategies for protecting privacy. This Article has shown why this should be so. It has demonstrated that second generation strategies are well suited to regulate industries—such as those that make up the information economy—that undergo rapid change, face stiff competition, and have the capacity for socially beneficial innovation. This Article has also expressly identified and more fully explained the second generation strategies that these sectors need. It has shown how these regulatory tools could be most effectively employed to protect privacy.

Although command-and-control regulation is not the best fit for the information economy, we should not give up on government action to protect privacy. To the contrary, the information economy needs such initiatives. Without them, a tragedy of the commons threatens email, e-commerce, and other online activity. To borrow one final environmental analogy, regulators need to develop strategies that will allow for the "sustainable development" of the information economy.[357] Such policies will support innovation and prosperity but will do so in a way that sustains the personal privacy on which the digital economy itself depends. Second generation environmental laws and policies offer valuable lessons for the design of this new regulatory framework and for the protection of privacy in the Information Age.

---

[357] PERCIVAL ET AL., *supra* note 183, at 1108 (defining "sustainable development" as "development that occurs on a scale that does not exceed the carrying capacity of the biosphere").

# 6 The Gaze of the Perfect Search Engine: Google as an Infrastructure of Dataveillance

Michael Zimmer

Information Society Project, Yale Law School, 127 Wall Street, New Haven, CT 06520 USA

## Abstract

Web search engines have emerged as a ubiquitous and vital tool for the successful navigation of the growing online informational sphere. The goal of the world's largest search engine, Google, is to "organize the world's information and make it universally accessible and useful" and to create the "perfect search engine" that provides only intuitive, personalized, and relevant results. While intended to enhance intellectual mobility in the online sphere, this chapter reveals that the quest for the perfect search engine requires the widespread monitoring and aggregation of a users' online personal and intellectual activities, threatening the values the perfect search engines were designed to sustain. It argues that these search-based infrastructures of dataveillance contribute to a rapidly emerging "soft cage" of everyday digital surveillance, where they, like other dataveillance technologies before them, contribute to the curtailing of individual freedom, affect users' sense of self, and present issues of deep discrimination and social justice.

## 6.1 Introduction

In January 2006 it was revealed that the U.S. Justice Department asked a federal judge to compel the Web search engine Google to turn over records on millions of its users' search queries as part of the government's effort to uphold an online pornography law (Hafner and Richtel 2006; Mintz 2006). Google resisted, but America Online, Microsoft, and Yahoo! complied

with similar government subpoenas of their search records (Hafner and Richtel 2006). Later that year, America Online released over 20 million search queries from 658,000 of its users to the public in an attempt to support academic research on search engine usage (Hansell 2006). Despite AOL's attempts to anonymize the data, individual users remained identifiable based solely on their search histories, which included search terms matching users' names, social security numbers, addresses, phone numbers, and other personally identifiable information. Simple keyword analyses of the AOL database also revealed an "innumerable number of life stories ranging from the mundane to the illicit and bizarre" (McCullagh 2006b). Upon being identified by the *New York Times* based solely on her search terms in the AOL database, a Georgia woman exclaimed, "My goodness, it's my whole personal life…I had no idea somebody was looking over my shoulder" (Barbaro and Zeller Jr 2006). Together, these events brought to light the fact that search engine providers keep detailed records of users' searches, and created anxiety among searchers about the presence of such systematic monitoring of their online information-seeking activities (Barbaro and Zeller Jr 2006; Hafner 2006; Levy 2006; Maney 2006).

The freedom to move through both physical and intellectual space is a central theme of various American mythologies, such as the desire to explore unknown frontiers and acquire new knowledge, the overcoming of artificial barriers of distance for mass communication and commerce, and the ability to control one's relations and position in the world. This freedom of mobility becomes embodied in the set of values deemed vital for the success of our society, including privacy, autonomy, and liberty. The emergence of systematic modes of data surveillance – otherwise referred to as "dataveillance" (Clarke 1988) – within our spheres of mobility threatens the preservation of these fundamental values. Without the ability and opportunity to move, navigate, inquire, and explore physical, intellectual, and, increasingly, digital spaces, we cannot gain the sort of understanding of our world and develop the awareness and competencies necessary for effective participation in social, economic, cultural, and political life. This chapter will examine the particular dataveillance threats of Web search engines, paying specific attention to the dominant search engine Google, and will reveal how the aggregation of one's online information-seeking activities within the online sphere of intellectual and informational mobility contributes to the creation of a technological gaze of everyday surveillance, inflaming a growing environment of discipline and social control.

This chapter is divided into four parts. Part one builds from theories of surveillance and power to introduce the concept of dataveillance, paying

particular attention to the role of information technology and data accumulation in the functioning of disciplinary power. Part two introduces the role of Web search engines as the prevailing information interface for accessing the vast amount of information available on Internet, concluding that as search engines have become the "center of gravity" for navigation within this vital sphere of information, important concerns over privacy and surveillance emerge. Part three describes the quest for the "perfect search engine" and how Google's integration of Web cookies, detailed server logs, and personal user accounts within and across its diverse product suite provides a powerful infrastructure of dataveillance to monitor, record, and aggregate information about users' online activities. Part four warns of how Google's infrastructure of dataveillance exerts its gaze, harboring concerns over its role in the exercise of disciplinary power, panoptic sorting of its users, and the challenges of resisting its "gravitational pull" in the face of default settings which require the sharing of information. The chapter concludes with a brief discussion of how an intervention in the technical design of the perfect search engine might help mitigate the effects of its disciplinary gaze.

## 6.2 The Gaze of Dataveillance

According to sociologist David Lyon, surveillance is the "collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (Lyon 2001, p. 2). Surveillance "tries to make visible the identities or the behaviors of people of interest to the agency in question" (Lyon 2002, p. 2). Surveillance, then, encompasses a diverse range of activities and processes concerned with scrutinizing people, their actions, and the spaces they inhabit. Surveillance, of course, has existed for centuries, and its methods have been continuously refined to broaden its reach and effectiveness. One notable example is English philosopher Jeremy Bentham's model penitentiary, the Panopticon (Bentham 1995). Conceived in 1791, Bentham's Panopticon prison was designed to maintain (by allusion, if not by fact) perpetual surveillance of its inhabitants: by placing prison guards in central tower with a one-way observation system surrounded by rooms for those to be watched, the subjects were unable to determine when they were being watched. Through this unique architectural design, Bentham believed that the constant threat that one could be surveilled at any time would force the subjects to internalize the effects of surveillance:

> The more constantly the persons to be inspected are under the eyes of the persons who should inspect them, the more perfectly will the purpose of the establishment have been attained. …This being impossible, the next thing to be wished for is, that, at every instant, seeing reason to believe as much, and not being able to satisfy himself to the contrary, he [the watched] should *conceive* himself to be so. (Bentham 1995, p. 3)

Through such an arrangement, Bentham believed disciplinary power would be automatic, and thus exercised with minimal effort, or, as Michel Foucault later reflected, the Panopticon would "induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault 1977, p. 197). This automatic functioning of power manifested itself through a panoptic and disciplinary gaze:

> There is no need for arms, physical violence, material constraints. Just a gaze. An inspecting gaze, a gaze which each individual under its weight will end by internalizing to the point that he is his own overseer, each individual thus exercising this surveillance over, and against, himself. A superb formula: power exercised continuously and for what turns out to be a minimal cost. (Foucault 1980, p. 155)

For Foucault, the Panopticon became a "generalizable model of functioning; a way of defining power relations in terms of the everyday life of men… it is in fact a figure of political technology" (Foucault 1977, p. 205). He viewed the Panopticon as the quintessential disciplinary apparatus of modern society, where the panoptic gaze extended beyond Bentham's specific architectural form, and manifested itself in various contexts of everyday life: the home, the school, the hospital, the workplace, and so on. The gaze of the Panopticon expands to become "a whole complex mechanism, embracing … stricter methods of surveillance [and] more efficient techniques of locating and obtaining information" (Foucault 1977, p. 77). By suggesting a link between the Panopticon and "more efficient techniques of locating and obtaining information," Foucault reveals a pivotal feature of the modern panoptic gaze: the functioning of power through data accumulation.

The functioning of the Panopticon depended on perpetual surveillance and the "continuous registration, perpetual assessment and classification" of those under its gaze (Foucault 1977, p. 220). Oscar Gandy recognized this perpetual and disciplinary gaze of personal data accumulation when he warned of the "panoptic sort" (Gandy 1993), whereby individuals are continually identified, assessed and classified for the purpose of coordinating and controlling their access to consumer goods and services, a process he insists in inherently discriminatory. Gandy's concern with panoptic sorting has been expanded beyond the consumer realm into a broader social milieu

(Lyon 2003a), where the notion of "social sorting" highlights the growing drive in our modern surveillance society for identification and classification. Since classification has been shown to be closely entwined with the exercise of power (Bowker and Star 1999; Foucault 1971; Suchman 1997), the consequences of panoptic and social sorting – and the technological gaze which form their foundation – present issues of "deep discrimination…and social justice" (Lyon 2003b, p. 1).

The catalyst triggering both Gandy and Lyon's anxiety was the rapid emergence of a complex set of technologies and practices that involve "the collection, processing, and sharing of information about individuals and groups that is generated through their daily lives as citizens, employees, and consumers (Gandy 1993, p. 15). This technological apparatus represents what is referred to as dataveillance, defined as both "the massive collection and storage of vast quantities of personal data" (Bennett 1996, p. 237) and "the systemic use of [such] personal data…in the investigation or monitoring of one or more persons" (Clarke 1988, p. 499). Clarke's (1988) introduction of the term dataveillance revealed how the disciplinary gaze of the panopticon has extended from a single, centralized source (Bentham's guard tower) into the realm of advanced information technologies and computer databases that facilitate the collection and exchange of information about individuals. Yet, the resulting effect of dataveillance's technologically distributed gaze matches that of Bentham's Panopticon envisioned two hundred years before – the subversion of individual freedoms and liberties:

> An administrative apparatus that has data available to it from a wide variety of sources tends to make decisions on the person's behalf. Hence, a further, more abstract, yet scarcely less real impact of dataveillance is reduction in the meaningfulness of individual actions, and hence in self- reliance and self- responsibility. Although this may be efficient and even fair, it involves a change in mankind's image of itself, and risks sullen acceptance by the masses and stultification of the independent spirit needed to meet the challenges of the future. …In general, mass dataveillance tends to subvert individualism and the meaningfulness of human decisions and actions. (Clarke 1988, p. 508)

Since Clarke's first conceptualization of dataveillance almost twenty years ago, advances in digital networking, data storage capacity and processing power have enabled previously unimaginable levels of interconnectivity, aggregation, and real-time analysis of a wide array of personal information. Increasingly, everyday interactions with health care providers, online retailers, highway tollbooths, local grocery stores and libraries result in the collection, analysis, storage and sharing of information about

one's address, purchasing habits, age, education, health status, travel activity, employment history, phone numbers and much more, into what legal scholar Daniel Solove (2004) calls "digital dossiers."(Solove 2004, p. 2) The rising ubiquity of dataveillance in everyday life and resultant sophistication of "digital dossiers" has led to widespread concern over the social and ethical implications of this new digital panoptic gaze (see, for example Elmer 2004; Gandy 1993; Garfinkel 2000; Lyon 2003a; Lyon and Zureik 1996; Regan 1995; Solove 2004; Staples 2000). As Clive Norris and Gary Armstrong argue in their study of the introduction of computer databases into video surveillance systems, the pervasiveness of digital dossiers (or, using their term, "digital personas") have "more than just an electronic existence: they have concrete material effects" (Norris and Armstrong 1999, p. 221). Such effects relate not only to personal privacy, but also issues of discrimination, social justice, and personal freedom. Law professor Michael Fromkin (2000) summarizes these effects best:

> Reams of data organized into either centralized or distributed databases can have substantial consequences beyond the simple loss of privacy caused by the initial data collection, especially when subject to advanced correlative techniques such as data mining. Among the possible harmful effects are various forms of discrimination, ranging from price discrimination to more invidious sorts of discrimination. Data accumulation enables the construction of personal data profiles. When the data are available to others, they can construct personal profiles for targeted marketing, and even, in rare vases, blackmail. For some, just knowing that their activities are being recorded may have a chilling effect on conduct, speech, and reading.
>
> …A further danger is that the government or others will attempt to use the ability to construct persona profiles in order to predict dangerous or antisocial activities before they happen. People whose profiles meet the criteria will be flagged as dangerous and perhaps subjected to increased surveillance, searches, or discrimination. (Froomkin 2000, p. 1469-1471)

The role of modern information and communication technologies within infrastructures of dataveillance cannot be understated: frequent shopping cards connect purchasing patterns to customer databases (Ward 1998), intelligent transportation systems enable the tracking and recording of vehicles as they travel the highways (Bennett et al. 2003; Zimmer 2005), electronic key cards manage access to locations while creating a record of one's movements (Stalder and Lyon 2003), and biometric technologies digitize one's intrinsic physical or behavioral traits for automated identification and authentication (Agre 2003; Brey 2004). Recently, the Internet has emerged as not only a revolutionary technology for communication, commerce and the distribution of information, but also as an ideal infrastructure of dataveillance, enabling the widespread monitoring and collec-

tion of personal and identifiable information about its millions of users (Center and 1999). The privacy and surveillance concerns with various Internet technologies have been well documented and debated, ranging from the use of Web cookies and tracking bugs (Bennett 2001; Kang 1998; Mayer-Schönberger 1997), the emergence of spyware and digital rights management systems (Cohen 1996, 2003), workplace monitoring of electronic communications (Froomkin 2000), the aggregation and data-mining of personal information available online (Garfinkel 2000; Solove 2004), and the widespread monitoring of Internet traffic by law enforcement agencies (Regan 2001; Ventura et al. 2005). The design and deployment of each of these new Internet technologies represents an expansion of the gaze of dataveillance online, which is intensified with the growing power and ubiquity of Web search engines and the larger information infrastructures on which they rely.

## 6.3 Web Search as the Center of Gravity

As the Internet has become increasingly important to modern citizens in their everyday lives (see Horrigan and Rainie 2006), Web search engines have emerged as an indispensable tool for accessing the vast amount of information available on this global network. According to the Pew Internet & American Life Project, 84% of American adult Internet users have used a search engine to seek information online (Fallows 2005, p. 1). On any given day, more than 60 million American adults send over 200 million information requests to Web search engines, making searching the Web the second most popular online activity (behind using e-mail) (Rainie 2005). Originally designed to provide easy access to Internet websites, search engines now provide gateways to online images, news reports, Usenet archives, financial information, video files, e-mail and even one's desktop files. Recently, search engine providers, such as Google, have started to digitize items in the "material" world, adding the contents of popular books, university libraries, maps, and satellite images to their growing, searchable indices. Reflecting on the rapid emergence of search-related applications, Silicon Valley venture capitalist Roger McNamee noted that "search is the new center of gravity for the computer industry" (McNamee 2005). The same can be said more generally for the role of search engines as today's dominant information interface: Search engines have become the center of gravity for people's everyday information-seeking activities.

Consider, for example, the Web search engine Google. Google has become the prevailing interface for searching and accessing virtually all in-

formation on the Web. Originating in 1996 as a Ph.D. research project by Sergey Brin and Larry Page at Stanford University (see Brin and Page 1998; Page et al. 1998), Google's Web search engine now dominates the market, processing almost 3.6 billion search queries in February 2007, over half of all Web searches performed (Nielsen//NetRatings 2007).[1] Google's mission, stated quite simply and innocuously, is to "organize the world's information and make it universally accessible and useful" (Google 2005a). In pursuit of this goal, Google has developed dozens of search-related tools and services to help users organize and use information in multiple contexts, ranging from general information inquiries to academic research, news and political information, communication and social networking, personal data management, financial data management, shopping and product research, computer file management, and enhanced Internet browsing (see Table 6.1). Consequently, users increasingly search, find, organize, and share information through Google's growing information infrastructure of search-related services and tools. They also use these tools to communicate, navigate, shop, and organize their lives. By providing a medium for various social, intellectual, and commercial activities, "Planet Google" has become a large part of people's lives, both online and off (Williams 2006).

**Table 6.1.** Google Suite of Products and Services (partial list)

| Product | Description | Notes |
|---|---|---|
| *General Information Inquiries* | | |
| Web search | Query-based website searches | |
| Personalized Homepage | Customized Google start page with content-specific modules | Use in conjunction with Google Account is encouraged |
| Alerts | E-mail alerts of new Google results for specific search terms | |
| Image Search | Query based search for website images | |
| Video | Query based search for videos hosted by Google | Google Video Player available for download |

[1] Nielsen/NetRatings figures represent U.S. searches only, and include local searches, image searches, news searches, shopping searches and other types of search activity from Google's various services. If only Web searches at www.google.com are considered, Google's share increases to 60% (Sullivan 2006).

| Product | Description | Notes |
|---|---|---|
| Book Search | Full text searches of books scanned into Google's servers | Google Account required in order to limit the number of pages a particular user can view |
| *Academic Research* | | |
| Scholar | Full text searches of scholarly books and journals | |
| *News and Political Information* | | |
| News | Full text search of recent news articles | With a Google Account, users can create customized keyword-based news sections |
| Reader | Web-based news feed reader | Google Account required |
| Blog Search | Full text search of blog content | |
| *Communication and Social Networking* | | |
| Gmail | Free Web based e-mail service with contextual advertising | Creation of Gmail account automatically results in activation of Google Account<br>Logging into Gmail also logs user into their Google Account |
| Groups | Free Web based discussion forums | Includes complete Usenet archives dating back to 1981<br>Google Account required for creation of new Group; |
| Talk | Web-based instant messaging and voice calling service | Google Account and Gmail e-mail address required |
| Blogger | Web-based blog publishing platform | Google Account required |
| Orkut | Web-based social networking service | Invitation-only<br>Google Account required |
| Dodgeball | Location-based social networking service for cellphones | |
| *Personal Data Management* | | |
| Calendar | Web-based time-management tool | |

| Product | Description | Notes |
|---|---|---|
| *Financial Data Management* | | |
| Finance | Portal providing news and financial information about stocks, mutual funds; Ability to track one's financial portfolio | Google Account required for posting to discussion board |
| *Consumer Activities* | | |
| Catalog Search | Full text search of scanned product catalogs | |
| Froogle | Full text search of online retailers | Google Account required for shipping lists |
| Local / Maps | Location specific Web searching; digital mapping | |
| *Computer File Management* | | |
| Desktop Search | Keyword based searching of computer files<br>Ability to search files on remote computer | |
| *Internet Browsing* | | |
| Bookmarks | Online storage of website bookmarks | Google Account required |
| Notebook | Browser tool for saving notes while visiting websites | Google Account required |
| Toolbar | Browser tool providing access to various Google products without visiting Google websites | Some features require Google Account |
| Web Accelerator | Software to speed up page load times for faster Web browsing | |

The emerging social and cultural impacts of this increasing reliance on search engines – and the resultant rise of "Plant Google" – are being studied from a variety of disciplines. Scholars have explored the biases of search engine results (Diaz 2005; Introna and Nissenbaum 2000), the political economy of the search engine marketplace (Van Couvering 2004), the legal ramifications of search engine practices (Elkin-Koren 2001; Goldman 2005), the structure of user queries and their searching skills (Hargittai 2002; Jansen et al. 2000), the practice of paid placement of search results (Jansen and Resnick 2005; Wouters 2004; Zimmer 2006), and general user awareness and trust in how search engines work (Fallows 2005; Marable 2003).

Scholarly attention also been paid to the particular ethical issues related to the dominant position of search engines in our lives (Nagenborg 2005; Norvig et al. 2006), including discussions of the privacy issues related to search engine practices (Hinman 2005; Tavani 2005). However, most treatments of the privacy implications of Web search engines have tended to focus on how search engines provide improved access to personal information that happens to exist online – the erosion of "security through obscurity" in the face of ever-expanding search engine indexes (Ramasastry 2005; Swidey 2003). While these particular privacy problems demand attention, we must expand the investigation of search-related privacy problems from concerns over the personal information about other people that can be *found* via search engines, to include critical exploration of the personal information that is routinely *collected* when users rely on search engines for their information-seeking activities. As we recall, the AOL searcher from Georgia mentioned above was not identifiable due to a search engine finding information about her on the Web, but rather because the Web searches *she* performed on various topics were recorded, and later released, by AOL. Of course, this dataveillance of users search queries by the search engine provider is not unique to AOL. In fact, it forms the very basis for the ultimate goal of the Web search industry: the quest for perfect search engine.

## 6.4 Dataveillance and the Quest for the Perfect Search Engine

Since the first search engines started to provide a way of interfacing with the content on the Web, there has been a quest for the "perfect search engine," one that has indexed all available information and provides fast and relevant results (see Andrews 1999; Gussow 1999; Kushmerick 1998). A perfect search engine would deliver intuitive results based on a user's past searches and general browsing history (Pitkow et al. 2002; Teevan et al. 2005), and deliver advertisements that are deemed useful or desirable for that particular user (Hansell 2005). Journalist John Battelle summarizes how a perfect search engine might provide a nearly perfect answer to every query:

> Imagine the ability to ask any question and get not just an accurate answer, but your perfect answer – an answer that suits the context and intent of your question, an answer that is informed by who you are and why you might be asking. The engine providing this answer is capable of incorporating all the world's knowledge to the task at hand – be it captured in text, video, or audio. It's capable of discern-

ing between straightforward requests – who was the third president of the United States? – and more nuanced ones – under what circumstances did the third president of the United States foreswear his views on slavery?

This perfect search also has perfect recall – it knows what you've seen, and can discern between a journey of discovery – where you want to find something new – and recovery – where you want to find something you've seen before. (Battelle 2004)

Given a search for the phrase "Paris Hilton," for example, the perfect search engine will know whether to deliver Web sites about the celebrity heiress or a place to spend the night in the French capitol, and whether to provide advertisements for Parisian bistros or celebrity news sites.

The search engine company Google recognized early on the importance of designing a perfect search engine: The company's very first press release noted that "a perfect search engine will process and understand all the information in the world…That is where Google is headed" (Google 1999). Google co-founder Larry Page later reiterated the goal of achieving the perfect search: "The perfect search engine would understand exactly what you mean and give back exactly what you want" (Google 2007). When asked what a perfect search engine would be like, Brin replied quite simply, "like the mind of God" (quoted in Ferguson 2005, p. 40).

To attain such an omnipotent and omniscient ideal, Google must, borrowing Battelle's words, provide results that suit the "context and intent" of the search query; it must have "perfect recall" of who the searcher is and her previous search-related activities. In order to discern the context and intent of a search for "Paris Hilton," for example, the perfect search engine would know if the searcher has shown interest in European travel, or whether she spends time online searching for sites about celebrity gossip. Attaining such perfect recall requires search engine providers to collect as much information about their users as possible. To accomplish this, Google, like most Web search engines, relies on three technical strategies in order to capture the personal information necessary to fuel the perfect recall: the maintenance of server logs, the use of persistent Web cookies, and the encouragement of user registration.

Maintained by nearly all websites, server logs help website owners gain an understanding of who is visiting their site, the path visitors take through the website's pages, which elements (links, icons, menu items, etc.) a visitor clicks, how much time visitors spend on each page, and from what page visitors are leaving the site. In other words, a website owner aims to collect enough data to reconstruct the entire "episode" of a user's visit to the website (Tec-Ed 1999). Google maintains detailed server logs recording each of the 100 million search requests processed each day (Google 2005c).

While the exact contents are not publicly known, Google has provided an example of a "typical log entry" for a user who searched for the term "cars" (Google 2005b):

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars - Firefox 1.0.7; Win-
dows NT 5.1 - 740674ce2123e969
```

In this sample entry, `123.45.67.89` is the IP address[2] assigned to the user by the user's Internet service provider, `25/Mar/2003 10:15:32` is the date and time of the query, `http://www.google.com/search?q=cars` is the requested page, which also happens to identify the search query, "cars," `Firefox 1.0.7; Windows NT 5.1` is the browser and operating system being used, and `740674ce2123a969` is the unique cookie ID[3] assigned to this particular browser the first time it visited Google. To help further reconstruct a user's movements, Google also records clickstream data, including which search results or advertising links a user clicks (Google 2005b). Given Google's wide array of products and services, their server logs potentially contain much more than simply a user's Web search queries. Other searches logged by Google include those for images, news stories, videos, books, academic research, and blog posts, as well as links clicked and related usage statistics from within Google's News, Reader, Finance, Groups, and other services.

Logging this array of information – the user's IP address, cookie ID, date and time, search terms, results clicked, and so on – enhances Google's ability to attain the "perfect recall" necessary to deliver valuable search results and generally improve its search engine services. For example, by cross-referencing the IP address each request sent to the server along with

[2] An Internet Protocol (IP) address is a unique address that electronic devices use in order to identify and communicate with each other on a computer network. An IP address can be thought of as a rough equivalent of a street address or a phone number for a computer or other network device on the Internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network (Wikipedia contributors 2007).

[3] A Web cookie is a piece of text generated by a Web server and stored in the user's computer, where it waits to be sent back to the server the next time the browser accesses that particular Web address. By returning a cookie to a Web server, the browser provides the server a means of associating the current page view with prior page views in order to "remember" something about the previous page requests and events (see Clarke 2001; Kristol 2001). Google's user of Web cookies allows it to identify particular browsers between sessions, even if that browser's IP address changes.

the particular page being requested and other server log data, it is possible to find out which pages, and in which sequence, a particular IP address has visited. When asked, "Given a list of search terms, can Google produce a list of people who searched for that term, identified by IP address and/or Google cookie value?" and "Given an IP address or Google cookie value, can Google produce a list of the terms searched by the user of that IP address or cookie value?", Google responded in the affirmative to both questions, confirming its ability to track user activity through such logs (Battelle 2006a, 2006b).

Sole reliance on IP logging and Web cookies to reconstruct a users' browsing and searching activities completely and consistently has its limitations. Some Internet service providers frequently change the IP address assigned to a particular user's network connection. Alternatively, multiple users accessing the Internet through a university proxy server or through some ISPs (such as AOL) might share the same IP address. Privacy concerns have also led more savvy Internet users to disguise their IP address with anonymous routing services such as Tor (Zetter 2005). Similarly, as the privacy concerns of the use of cookies to track users' online activities increases (Kristol 2001; Mayer-Schönberger 1997; Schwartz 2001), users increasingly take advantage of software and browser features that make it easier to view, delete and block Web cookies received from the sites they visit (McGann 2005; Mindlin 2006). Even in the absence of such privacy-protecting measures, cookies and IP addresses are linked only to a particular Web browser or computer, not necessarily a particular user. Neither the browser passing the cookie nor the Web server receiving it can know who is actually using the computer, or whether multiple users are using the same machine. Reliance on IP addresses and cookies might not provide necessary differentiation between users, limiting the extent of the "perfect recall" necessary for Google to deliver the most relevant results and advertising.

To overcome such limitations, Web site owners frequently urge users to register with the website and login when using the services (Ho 2005, p. 660-661; Tec-Ed 1999). When a user supplies a unique login identity to a Web server, that information, along with the current cookie ID, is stored in each log file record for that user's subsequent activity at the site. By tying aspects of the site's functionality to being logged in, the user is compelled to accept the Web cookie for that session. Even if the user deletes the cookie or changes her IP address at the end of the session, by logging in again at the next visit, a consistent record for the user in the server log can be maintained. Logging in with a unique user name similarly reduces the variability of multiple or shielded IP addresses. Further, any personally

identifiable information provided during the registration process, such as age, gender, zip code, or occupation, can be associated with the user's account and server log history, providing a more detailed profile of the user.

In early 2004, Google started experimenting with products and services that required users to register and login, including personalized search results, e-mail alerts when sites about a particular topic of interest are added to Google's index (Kopytoff 2004). Soon afterward, Google introduced products and services that required the creation of a Google Account, such as Gmail, Google Calendar, and the Reader service to organize news feeds. Other Google services can be partially used without a Google Account, but users are encouraged to create an account in order to maximize its benefits or access certain features. Examples include Google Video, with a Google Account required for certain premium content, and Book Search, in which a Google Account helps control access to copyright-protected text. When Google acquires external products and services with their own login protocols, migration to Google Accounts is typical, as the case with Blogger or Dodgeball. Internally developed products that previously utilized unique logins, such as Orkut, have also migrated to the universal Google Account.

Google's encouragement of the creation of Google Accounts, combined with its use of persistent Web cookies, provides the necessary architecture for the creation of detailed server logs of users' activities across Google's various products and services, ranging from the simplest of search queries to minute details of their personal lives. While the full extent of the data capturable by Google's infrastructure is difficult to estimate, Table 6.2 identifies some of the typical forms of personal information potentially stored within Google's servers.

**Table 6.2.** Sample of Personal Information Collected by Google's Suite of Products

| Product | Information Collected | Notes |
|---|---|---|
| *General Information Inquiries* | | |
| Web search | Web search queries<br>Results clicked | Search for own name, address, social security number, etc is common |
| Personalized Homepage | News preferences<br>Special interests<br>Zip code | |
| Alerts | News preferences<br>Special interests<br>E-mail address | Alerts for a user's own name (vanity search) are common |
| Image Search | Search queries<br>Results clicked | |

| Product | Information Collected | Notes |
|---|---|---|
| Video | Search queries<br>Videos watched/downloaded<br>Credit card information for purchased videos<br>E-mail details for shared videos | Google Video Player contains additional DRM technology to monitor off-site video usage |
| Book Search | Search queries<br>Results clicked<br>Pages read<br>Bookseller pages viewed | |
| *Academic Research* | | |
| Scholar | Search queries<br>Results clicked<br>Home library (Optional) | |
| *News and Political Information* | | |
| News | News search queries<br>Results clicked | |
| Reader | Feed subscriptions<br>Usage statistics | |
| Blog Search | Search queries<br>Results clicked | |
| *Communication and Social Networking* | | |
| Gmail | Text of email messages<br>E-mail searches performed<br>Email address or cellphone number (used for account creation) | |
| Groups | Search queries<br>User interests<br>Usage statistics<br>Profile information | Users are encouraged to create detailed profiles, including name, location, industry, homepage, etc |
| Talk | Contact list<br>Chat messages<br>Usage statistics | |
| Blogger | Weblog posts and comments<br>Profile information<br>Usage statistics | Users are encouraged to create detailed profiles, including name, location, gender, birthday, etc |
| Orkut | Profile information<br>Usage statistics<br>E-mail address and content of invitations | Users are encouraged to create detailed profiles, including name, location, gender, birthday, etc |

| Product | Information Collected | Notes |
|---|---|---|
| Dodgeball | Profile information<br>E-mail address<br>Location<br>Mobile phone information<br>Text messages sent | User location when messages sent are tracked by Google |
| *Personal Data Management* | | |
| Calendar | Profile information<br>Events<br>Usage statistics | |
| *Financial Data Management* | | |
| Finance | Financial quotes<br>Discussion group posts<br>Discussion group views<br>Portfolio (optional)<br>Profile information | Names and e-mails are displayed with discussion posts |
| *Consumer Activities* | | |
| Catalog Search | Product search queries<br>Results clicked | |
| Froogle | Product search queries<br>Results clicked<br>Sites visited<br>Shopping list | |
| Local / Maps | Search queries<br>Results clicked<br>Home location | Search queries might include geographic-specific information<br>Default location stored via Web cookie |
| *Computer File Management* | | |
| Desktop Search | Search queries<br>Computer file index (Optional) | Search queries visible to Google under certain circumstances<br>Desktop file index is stored on Google's services if using Search Across Computers |
| *Internet Browsing* | | |
| Bookmarks | Favorite websites<br>When visited | |
| Notebook | Notes and clippings<br>Sites annotated | |

| Product | Information Collected | Notes |
|---|---|---|
| Toolbar | Search queries<br>Websites visited | Use of some advanced features routes *all* browsing traffic through Google servers |
| Web Accelerator | Websites visited | *All* browsing traffic is routed through Google servers |

The result is a robust infrastructure arming Google with the ability to capture and aggregate a wide array of personal and intellectual information about its users, extending beyond just the keywords for which they search, but also including the news they read, the interests they have, the blogs they follow, the books they enjoy, the stocks in their portfolio, their schedule for the coming week, and perhaps the URL of every website they visit.

## 6.5 Discussion

It is easy to think of search engines like Google as one-way information interfaces: you enter a search term, and Google gives you millions of pages of information in return. You click on a link, and they direct you to a website, a helpful map, or a news report. But there is an important feedback loop; the interface is two-way. More than just the center of gravity of information seeking online, Google's information infrastructure also acts as a black hole, to continue the metaphor, using its gravitational forces to pull as much information about its users into its domain as possible. By monitoring and aggregating the results of every Web search performed, every image result clicked, every website bookmarked, or every page visited with the Toolbar, Google has created sophisticated infrastructure of dataveillance. The result is what John Battelle calls a "database of intentions":

> This information represents, in aggregate form, a place holder for the intentions of humankind - a massive database of desires, needs, wants, and likes that can be discovered, subpoenaed, archived, tracked, and exploited to all sorts of ends. Such a beast has never before existed in the history of culture, but is almost guaranteed to grow exponentially from this day forward. This artifact can tell us extraordinary things about who we are and what we want as a culture. (Battelle 2003)

While many of our day-to-day habits – such as using credit cards, ATMs, cell phones, or automated toll collection systems – leave countless "virtual footprints" of our activities, the panoptic gaze of Google's infrastructure of dataveillance tracks our search histories, e-mails, blog posts or general browsing habits, providing "an excellent source of insight into what someone is *thinking*, not just what that person is doing" (Hinman, 2005, p. 23).

The full effects of the panoptic gaze of Google's infrastructure of dataveillance are difficult to predict, but, like most infrastructures of dataveillance, the most obvious effects of Google's infrastructure relate to the exercising of disciplinary power, panoptic sorting, and the general invisibility of both its gaze and its power. Clive Norris warns that infrastructures of dataveillance are often used to "[render] visualization meaningful for the basis of disciplinary social control" (Norris 2002, p. 251). Instances of how users of Google's infrastructure were made visible for the exercise of disciplinary power include a court ordering Google to provide the complete contents of a user's Gmail account, including e-mail messages he thought were deleted (McCullagh 2006a) and the introduction of evidence that a suspected murderer performed a Google search for the words "neck snap break" (Cohen 2005). While Google appears to recognize, at least partially, the disciplinary threat of storing such robust records of its users activities when it announced it would move user data collected from its Chinese site outside of the country in order to prevent China's government from being able to access the data without Google's consent (McMillan 2006), the company recently agreed to comply with a Brazilian court order to release data on users of its Orkut social networking site to help Brazilian authorities investigate use of the site related to racism, pedophilia, and homophobia (Downie 2006). The possibility of Google providing search histories to government bodies for disciplinary action has reached new heights within the United States with the passage of the USA PATRIOT Act, greatly expanding the ability of law enforcement to access such records, while restricting the source of the records, such as Google, from disclosing any such request has even been made (see Battelle 2005, p. 197-204).

Google's infrastructure of dataveillance also spawns instances of "panoptic sorting" where users of Google are identified, assessed and classified "to coordinate and control their access to the goods and services that define life in the modern capitalist economy" (Gandy 1993, p. 15). Google, like most for-profit search engine providers, is financially motivated collect as much information as possible about each user: receiving personalized search results might contribute to a user's allegiance to a particular search engine service, increasing exposure to that site's advertising part-

ners as well as improving chances the user would use fee-based services. Similarly, search engines can charge higher advertising rates when ads are accurately placed before the eyes of users with relevant needs and interests (Hansell 2005). Through the panoptic gaze of its diverse suite of products, Google collects as much information as possible about an individual's behavior, and considers it to be potentially useful in the profiling and categorization of a user's potential economic value: recognizing that targeted advertising will be the "growth engine of Google for a very long time", Google CEO Eric Schmidt stressed the importance of collecting user information for economic gain, acknowledging that "Google knows a lot about the person surfing, especially if they have used personal search or logged into a service such as Gmail" (Miller 2006).

Perhaps the most potent aspect of the technological gaze of Google's infrastructure of dataveillance is its relative invisibility, indispensability, and apparent inescapability. The majority of Web searchers are not aware that search engines have the ability to actively track users' search behavior (Fallows 2005, p. 21; Kopytoff 2006), and as Google continues to expand its information infrastructure[4], it becomes arduous for everyday users to recognize the data collection threats of these services, and easier to take the design Google's infrastructure of dataveillance merely "at interface value" (Turkle 1995, p. 103). Greg Elmer warns of the dangers of such an environment where the collection of personal information is a prerequisite of participation inevitably entrenches power in the hands of the technology designers:

> Ultimately, what both requesting and requiring personal information highlight is the centrality of producing, updating, and deploying consumer *profiles* – simulations or pictures of consumer likes, dislikes, and behaviors that are automated within the process of consuming goods, services, or media and that increasingly anticipate our future needs and wants based on our aggregated past choices and behaviors. And although Foucault warns of the self-disciplinary model of punishment in panoptic surveillance, computer profiling, conversely, oscillates between seemingly rewarding participation and punishing attempts to elect not to divulge personal information. (Elmer 2004, p. 5-6)

This blurring of punishments and rewards – subtle requests and not so subtle commands for personal information – reoccurs in Google's information interface where the default settings and arrangement of services make

[4] Recent additions to Google's product suite include Web-based word processor and spreadsheet services, enterprise solutions for business use, online digital photo sharing, website authoring tools, an online database package, and the widely-popular video hosting website YouTube.

the collection of personal information automatic and difficult to resist, and many are willing to join "Planet Google" with only scant hesitation: "I don't know if I want all my personal information saved on this massive server in Mountain View, but it is so much of an improvement on how life was before, I can't help it" (Williams 2006). As with Bentham's panopticon, Google's infrastructure of dataveillance places its users under an almost invisible gaze, resulting in a kind of anticipatory conformity, whereby the divulgence of personal information become both routinized and internalized.

## 6.6 Conclusion

By amassing a tantalizing collection of, admittedly, innovative and useful tools, coupled with requiring the divulgence of personal information as a precondition for using many of its search-related products and services, Google has constructed an information-seeking environment whereby which individuals are continuously integrated into a larger infrastructure of dataveillance. Their quest for the perfect search engine has resulted in the emergence of a robust infrastructure of dataveillance that can quickly become the basis of disciplinary social control. Repeating Roger Clark's warning about the effects of dataveillance:

> [A] real impact of dataveillance is the reduction in the meaningfulness of individual actions, and hence in self- reliance and self- responsibility. Although this may be efficient and even fair, it involves a change in mankind's image of itself, and risks sullen acceptance by the masses and stultification of the independent spirit needed to meet the challenges of the future. …In general, mass dataveillance tends to subvert individualism and the meaningfulness of human decisions and actions. (Clarke 1988, p. 508)

Thus a Faustian bargain emerges with the quest for the perfect search engine: The perfect search engine promises breadth, depth, efficiency, and relevancy, but enables the widespread collection of personal and intellectual information in the name of its perfect recall. If left unchecked, potential cost of this bargain is nothing less than the "individualism and the meaningfulness of human decisions and actions."

What options exist for renegotiating our Faustian bargain with the perfect search engine? One avenue for changing the terms of the Faustian bargain is to enact laws to regulate the capture and use of personal information by Web search engines. A recent gathering of leading legal scholars and industry lawyers to discuss the possibility of regulating search en-

gines revealed, however, that viable and constitutional solutions are difficult to conceive, let alone agree upon.[5] Alternatively, the search engine industry could self-regulate, creating strict policies regarding the capture, aggregation, and use of personal data via their services. But as Chris Hoofnagle reminds us, "We now have ten years of experience with privacy self-regulation online, and the evidence points to a sustained failure of business to provide reasonable privacy protections" (2005, p. 1). Given search engine companies' economic interests in capturing user information for powering the perfect search engine, relying solely on self-regulation will likely be unsatisfying.

A third option is to affect the design of the technology itself. As Larry Lessig notes, "how a system is designed will affect the freedoms and control the system enables" (2001, p. 35), I argue that technological design is one of the *critical junctures* for society to re-negotiate its Faustian bargain with the perfect search engine in order to preserve a sense of "individualism and the meaningfulness of human decisions and actions." Potential design variables include whether default settings for new products or services automatically enroll users in data-collecting processes – or whether the process can be turned off. Or the extent to which different products should be interconnected: For example, if a user signs up to use Gmail, should the Personalized Search automatically be activated? Should the user automatically be logged in to other services? Ideally, new tools can be developed to give users access and control over the personal information collected: In the spirit of the Code of Fair Information Practices, a Google Data Privacy Center should be built to allow users to view all their personal data collected, make changes and deletions, restrict how it is used, and so on. Through such an intervention in the design of the perfect search engine, there is hope that our Faustian bargain can be re-negotiated to counter the disciplinary effects of its gaze.

## References

Agre P (2003) Your face is not a bar code: Arguments against automatic face recognition in public places. Available: http://polaris.gseis.ucla.edu/pagre/barcode.html via the Internet.

Andrews P (1999) The search for the perfect search engine. The Seattle Times E1

[5] See "Regulating Search: A Symposium on Search Engines, Law, and Public Policy" held in December 2005 at Yale Law School (http://islandia.law.yale.edu/isp/regulatingsearch.html).

Barbaro M, Zeller Jr T (2006) A Face Is Exposed for AOL Searcher No. 4417749. The New York Times A1

Battelle J (2003) The database of intentions. Searchblog. Available: http://battellemedia.com/archives/000063.php via the Internet.

Battelle J (2004) Perfect search. Searchblog. Available: http://battellemedia.com/archives/000878.php via the Internet.

Battelle J (2005) The search: How google and its rivals rewrote the rules of business and transformed our culture. Portfolio, New York

Battelle J (2006a) More on what google (and probably a lot of others) know. Searchblog. Available: http://battellemedia.com/archives/002283.php via the Internet.

Battelle J (2006b) What info does google keep? Searchblog. Available: http://battellemedia.com/archives/002272.php via the Internet.

Bennett C (1996) The public surveillance of personal data: A cross-national analysis. In: Lyon D, Zureik E, (eds) Computers, surveillance, and privacy. University of Minnesota Press, Minneapolis, pp. 237-259

Bennett C (2001) Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web. Ethics and Information Technology 3: 197-210

Bennett C et al. (2003) People and place: Patterns of individual identification within intelligent transport systems. In: Lyon D, (ed) Surveillance as social sorting: Privacy, risk, and digital discrimination. Routledge, London, pp. 153-175

Bentham J (1995) The panopticon writings. Verso, London ; New York

Bowker GC, Star SL (1999) Sorting things out: Classification and its consequences. MIT Press, Cambridge, MA

Brey P (2004) Ethical Aspects of Facial Recognition Systems in Public Places. Journal of Information Communication and Ethics in Society 2: 97-109

Brin S, Page L (1998) The Anatomy of a Large-Scale Hypertextual Web Search Engine. WWW7 / Computer Networks 30: 107-117

Clarke R (1988) Information Technology and Dataveillance. Communications of the ACM 37: 498-512

Clarke R (2001) Cookies. Available: http://www.anu.edu.au/people/Roger.Clarke/II/Cookies.html via the Internet.

Cohen A (2005) What Google Should Roll Out Next: A Privacy Upgrade. The New York Times A18

Cohen J (1996) A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace. Connecticut Law Review 28: 981-1039

Cohen J (2003) DRM and privacy. Communications of the ACM 46: 46-49

Diaz A (2005) Through the Google goggles: Sociopolitical bias in search engine design. Department of Communication B.A.:

Downie A (2006) Google carves a middle path on privacy. The Christian Science Monitor 1

Center EPI (1999) Internet privacy. Available: http://www.epic.org/privacy/internet/default.html via the Internet.

Elkin-Koren N (2001) Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing. University of Dayton Law Review 26: 180-209

Elmer G (2004) Profiling machines: Mapping the personal information economy. MIT Press, Cambridge, MA

Fallows D (2005) Search engine users: Internet searchers are confident, satisfied and trusting – but they are also unaware and naïve. Pew Internet & American Life Project. Available: http://www.pewinternet.org/pdfs/PIP_Searchengine_users.pdf via the Internet.

Ferguson C (2005) That's next for Google? Technology Review 108: 38-46

Foucault M (1971) The order of things: An archaeology of the human sciences. Vintage, New York

Foucault M (1977) Discipline and punish: The birth of the prison. Vintage Books, New York

Foucault M (1980) The eye of power. In: Gordon C, (ed) Power/knowledge: Selected interviews and other writings, 1972-1977. Pantheon, New York, pp. 146-165

Froomkin AM (2000) The Death of Privacy. Stanford Law Review 52: 1461-1543

Gandy O (1993) The panoptic sort: A political economy of personal information. Westview, Boulder, CO

Garfinkel S (2000) Database nation: The death of privacy in the 21st century. O'Reilly, Sebastopol, CA

Goldman E (2005) Deregulating Relevancy in Internet Trademark Law. Emory Law Journal 54:

Google (1999) Google receives $25 million in equity funding [press release]. Google Press Center. Available: http://www.google.com/press/pressrel/pressrelease1.html via the Internet.

Google (2005a) Company overview. Available: http://www.google.com/corporate/index.html via the Internet.

Google (2005b) Google privacy faq. Available: http://www.google.com/privacy_faq.html via the Internet.

Google (2005c) Google privacy policy. Available: http://www.google.com/privacypolicy.html via the Internet.

Google (2007) Our philosophy. Available: http://www.google.com/intl/en/corporate/tenthings.html via the Internet.

Gussow D (1999) In search of. St Petersburg Times Business: 13

Hafner K (2006) After subpoenas, Internet searches give some pause. The New York Times A1, A19

Hafner K, Richtel M (2006) Google resists U.S. subpoena of search data. The New York Times A1, C4

Hansell S (2005) Microsoft plans to sell search ads of its own. The New York Times C1, C8

Hansell S (2006) AOL Removes Search Data On Vast Group Of Web Users. The New York Times C4

Hargittai E (2002) Beyond logs and surveys: In-depth measures of people's web use skills. Journal of the American Society for Information Science and Technology 53: 1239-1244

Hinman L (2005) Esse est indicato in Google: Ethical and political issues in search engines. International Review of Information Ethics 3: 19-25

Ho SY (2005) An exploratory study of using a user remote tracker to examine web users' personality traits. Proceedings of the 7th international conference on Electronic commerce: 659-665

Hoofnagle C (2005) Privacy self regulation: A decade of disappointment. Electronic Privacy Information Center. Available: http://www.epic.org/reports/decadedisappoint.html via the Internet.

Horrigan J, Rainie L (2006) The internet's growing role in life's major moments. Pew Internet & American Life Project. Available: http://www.pewinternet.org/PPF/r/181/report_display.asp via the Internet.

Introna L, Nissenbaum H (2000) Shaping the Web: Why the Politics of Search Engines Matters. The Information Society 16: 169-185

Jansen BJ, Resnick M (2005) Examining Searcher Perceptions of and Interactions with Sponsored Results. Workshop on Sponsored Search Auctions at ACM Conference on Electronic Commerce

Jansen BJ et al. (2000) Real life, real users, and real needs: A study and analysis of user queries on the web. Information Processing and Management 36: 207-227

Kang J (1998) Information Privacy in Cyberspace Transactions. Stanford Law Review 50: 1193-1294

Kopytoff V (2004) Google tests souped-up Web searches. San Francisco Chronicle C3

Kopytoff V (2006) Most Web users say Google should keep data private. San Francisco Chronicle C3

Kristol D (2001) HTTP cookies: Standards, privacy, and politics. ACM Transactions on Internet Technology (TOIT) 1: 151-198

Kushmerick N (1998) The search engineers. The Irish Times 10

Lessig L (2001) The future of ideas: The fate of the commons in a connected world. Random House, New York

Levy S (2006) Searching for Searches. Newsweek 49

Lyon D (2001) Surveillance society: Monitoring everyday life. Open University Press, Philadelphia

Lyon D (2002) Editorial. Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix. Surveillance & Society 1: 1-7

Lyon D (2003b) Introduction. In: Lyon D, (ed) Surveillance as social sorting: Privacy, risk, and digital discrimination. Routledge, London, pp. 1-9

(2003a) Surveillance as social sorting: Privacy, risk, and digital discrimination. xi, 287 p

Lyon D, Zureik E (1996) Computers, surveillance, and privacy. University of Minnesota Press, Minneapolis

Maney K (2006) AOL's data sketch sometimes scary picture of personalities searching Net. USA Today 4B

Marable L (2003) False oracles: Consumer reaction to learning the truth about how search engines work: Results of an ethnographic study. Available: http://www.consumerwebwatch.org/news/searchengines/index.html via the Internet.

Mayer-Schönberger V (1997) The Internet and Privacy Legislation: Cookies for a Treat? West Virginia Journal of Law and Technology 1:

McCullagh D (2006b) Aol's disturbing glimpse into users' lives. CNET Newscom. Available: http://news.com.com/AOLs+disturbing+glimpse+into+users+lives/2100-1030_3-6103098.html?tag=st.num via the Internet.

McCullagh D (2006a) Police blotter: Judge orders gmail disclosure. Newscom. Available: http://news.com.com/Police%20blotter%20Judge%20orders%20Gmail%20disclosure/2100-1047_3-6050295.html via the Internet.

McGann R (2005) Study: Consumers delete cookies at surprising rate. ClickZ News. Available: http://www.clickz.com/news/article.php/3489636 via the Internet.

McMillan R (2006) Google moving search records out of china. InfoWorld. Available: http://www.infoworld.com/article/06/03/01/75996_030106HNgooglechina_1.html via the Internet.

McNamee R (2005) Google's desktop search. The New Normal. Available: http://thenewnormal.com/index.php/newnormal/googles_desktop_search/ via the Internet.

Miller M (2006) Google's schmidt clears the air. PCMagcom. Available: http://www.pcmag.com/article2/0,1895,1939257,00.asp via the Internet.

Mindlin A (2006) The Case of the Disappearing Cookies. The New York Times C5

Mintz H (2006) Feds after google data: Records sought in u.s. Quest to revive porn law. San Jose Mercury News. Available: http://www.siliconvalley.com/mld/siliconvalley/13657386.htm via the Internet.

Nagenborg M (2005) The ethics of search engines (Special issue). International Review of Information Ethics 3:

Nielsen//NetRatings (2007) Nielsen//netratings announces february u.s. Search share rankings. Available: http://www.nielsen-netratings.com/pr/pr_070320.pdf via the Internet.

Norris C (2002) From personal to digital: Cctv, the panopticon, and the technological mediation of suspicion and social control. In: Lyon D, (ed) Surveillance as social sorting. Routledge, London, pp. 249-281

Norris C, Armstrong G (1999) The maximum surveillance society: The rise of cctv. Berg, Oxford

Norvig P et al. (2006) The ethics and politics of search engines. Panel at Santa Clara University Markkula Center for Applied Ethics. Available: http://www.scu.edu/sts/Search-Engine-Event.cfm via the Internet. Accessed Panel discussion

Page L et al. (1998) The pagerank citation ranking: Bringing order to the web. Technical report

Pitkow J et al. (2002) Personalized search. Communications of the ACM 45: 50-55

Rainie L (November 2005) Search engine use shoots up in the past year and edges towards e–mail as the primary Internet application. Pew Internet and American Life Project

Ramasastry A (2005) Can we stop zabasearch -- and similar personal information search engines?: When data democratization verges on privacy invasion. FindLaw. Available: http://writ.news.findlaw.com/ramasastry/20050512.html via the Internet.

Regan P (1995) Legislating privacy: Technology, social values, and public policy. University of North Carolina Press, Chapel Hill

Regan P (2001) From Clipper to Carnivore: Balancing Privacy, Law Enforcement and Industry Interests. American Political Science Association

Schwartz J (2001) Giving the Web a Memory Costs Its Users Privacy. The New York Times A1

Solove D (2004) The digital person: Technology and privacy in the information age. New York University Press, New York

Stalder F, Lyon D (2003) Electronic identity cards and social classification. In: Lyon D, (ed) Surveillance as social sorting: Privacy, risk, and digital discrimination. Routledge, London, pp. 77-93

Staples WG (2000) Everyday surveillance: Vigilance and visibility in postmodern life. Rowman & Littlefield, Lanham, MD

Suchman L (1997) Do categories have politics? The language/action perspective reconsidered. In: Friedman B, (ed) Human values and the design of computer technology. Cambridge University Press, Cambridge, UK, pp. 91-105

Sullivan D (2006) Hitwise search engine ratings. SearchEngineWatch. Available: http://searchenginewatch.com/showPage.html?page=3099931 via the Internet.

Swidey N (2003) A nation of voyeurs: How the Internet search engine Google is changing what we can find out about one another - and raising questions about whether we should. The Boston Globe Sunday Magazine Magazine: 10

Tavani HT (2005) Search engines, personal information and the problem of privacy in public. International Review of Information Ethics 3: 39-45

Tec-Ed (1999) Assessing web site usability from server log files [white paper]. Available: www.teced.com/PDFs/whitepap.pdf via the Internet.

Teevan J et al. (2005) Personalizing search via automated analysis of interests and activities. Proceedings of the 28th annual international ACM SIGIR conference on Research and development in information retrieval 449-456

Turkle S (1995) Life on the screen: Identity in the age of the internet. Simon & Schuster, New York

Van Couvering E (2004) New media? The political economy of Internet search engines. Annual Conference of the International Association of Media & Communications Researchers, Porto Alegre, Brazil 7-14

Ventura HE et al. (2005) Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power. Critical Criminology 13: 55-70

Ward C (1998) Grocery store shopper cards save money but cost privacy. Houston Chronicle. Available:

http://www.chron.com/content/chronicle/business/98/05/03/grocerycards.1-1.html via the Internet.

Wikipedia contributors (2007) Ip address. Wikipedia, The Free Encyclopedia. Available: http://en.wikipedia.org/w/index.php?title=IP_address&oldid=123964420 via the Internet.

Williams A (2006) Planet Google Wants You. The New York Times 9.1

Wouters J (2004) Searching for disclosure: How search engines alert consumers to the presence of advertising in search results. Consumer Reports WebWatch. Available: http://www.consumerwebwatch.org/news/paidsearch/finalreport.pdf via the Internet.

Zetter K (2005) Tor torches online tracking. Wired News. Available: http://www.wired.com/news/privacy/0,1848,67542,00.html via the Internet.

Zimmer M (2005) Surveillance, privacy and the ethics of vehicle safety communication technologies. *Ethics and Information Technology* 7: 201-210

Zimmer M (2006) The value implications of the practice of paid search. *Bulletin of the American Society for Information Science and Technology*. *Bulletin of the American Society for Information Science and Technology*Available: http://www.asis.org/Bulletin/Dec-05/zimmer.html via the Internet.

# Beyond Media Hype: Empirical Analysis of Disclosed Privacy Breaches 2005-2006 and a DataSet/Database Foundation for Future Work

Ragib Hasan
rhasan@ncsa.uiuc.edu

William Yurcik
byurcik@ncsa.uiuc.edu

National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign (UIUC) Urbana, IL 61801.

## ABSTRACT

A welcome but unintended consequence of recent state disclosure laws in the U.S. (most notably California SB 1386), has been a continuous stream of privacy breaches reported in the mass media. In this paper, we provide empirical analysis of disclosed breaches for the period of 2005-2006 to better understand what is happening in aggregate (overall patterns and trends) beyond the often sensational individual cases reported in the media. By processing raw data from the best available sources, we have created an Internet-accessible database that can be queried for breach statistics and a data set that can be shared so that our analysis can be validated, as well as enable future analysis by other researchers. The statistical analysis we report here is a first step toward answering the important and complex questions of why privacy breaches are occurring and what may be the best practices to prevent and mitigate their effects. Policy formulation to address privacy breaches is already in process at the organization, state, and national levels largely driven by mass media coverage – it is our hope decision-makers take the empirical evidence we report here into consideration.

## Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and Protection*; H.3.4 [**Information Systems**]: Information Storage and Retrieval—*Systems and Software*; D.4.2 [**Software**]: Operating Systems—*Storage Management*

## Keywords

privacy breaches, breach disclosure laws, storage security

## 1. INTRODUCTION

What do these trios of organizations have in common?

1. Bank of America, Fidelity, and Bank of Bermuda
2. U.S. Departments of Agriculture, Treasury, and Veterans Affairs
3. Verizon, T-Mobile, and AOL
4. Ford, Boeing, and JetBlue
5. the Medical Centers of University of Washington, University of Pittsburgh, and Delta Blood Bank

These trios represent a wide range within five of the eight critical national infrastructures (in the U.S.) with disclosed privacy breaches that have been reported in the mass media between 2005-2006 [2, 3, 15]: (1) banking and finance, (2) government services, (3) telecommunications, (4) transportation, and (5) emergency services. [1] PrivacyRightsClearingHouse reports a total of 90 million records containing sensitive personal information have been compromised during this period [1].

Risks from releasing private information in a breach are twofold: (1) privacy risk and (2) identity theft fraud [14]. While the cost of personal information being revealed is specific to each individual and thus hard to quantify[2], the cost of identity theft *fraud* for individuals typically runs hundreds of dollars and several years to clear their name and the cost of identity theft *fraud* for organizations has been estimated to be in the tens of billions of dollars [5].

This is a new problem because third parties now control private data that used to be under an individual's direct control – data that used to be controlled exclusively by individuals physically within their own home – is now increasingly stored by third parties with Internet operations that may or may not invest in protecting private data [14]. For example, personal mail, finances, shopping behavior, and work/leisure activities that used to leave only physical traces that could

[1]PDD-63 identifies these eight critical infrastructures[8]. The critical infrastructures not represented in these trios are (6) electric power, (7) oil and gas, and (8) water.

[2]For example, the cost of making private medical information public is dependent on whether the person has a condition he or she wants to remain secret or not. Thus the cost to an individual for revealing private medical information may vary from zero to lifetime career earnings for medical conditions that, if exposed, could terminate a career.

be physically contained now leave Internet traces with third parties.

The only reason we know about most privacy breaches are new state laws mandating disclosure to affected parties of incidents that release private data due to security compromise. In the past, organizations did not notify affected parties when their private data was compromised, leaving them at risk for identity theft fraud often only to find out when it was too late. New state disclosure laws allow individuals to take proactive steps to safeguard their identities after a compromise has occurred – thus returning control of private data back to individuals.

Disclosure laws have done much more than giving individuals notice, they have also improved protection by providing metrics upon which to measure security where no metrics existed before. However, since there are typically no public disclosure requirements in state laws and disclosure laws have not been actively enforced, reporting in the mass media has been spotty and focused on the sensational rather than insightful analysis.

The goal of this paper is to provide both comprehensive and in-depth analysis of privacy breaches beyond mass media reports by processing raw data from a combination of best available sources for patterns and emerging trends. In previous work, we framed a storage security threat model which organized potential attacks into categories along multiple dimensions [11]. In this work, we seek to understand the risks from potential attacks by analyzing the mechanisms, frequency, and impact of privacy breaches from empirical data. While past experience may or may not be indicative of future attacks, understanding vulnerabilities that are being exploited in the current environment is an important starting point for future improvement. Future attacks are unpredictable, but known risks can be measured to serve as a foundation for looking ahead. Due diligence dictates that security investment to mitigate risks should be based on evidence; otherwise it will expose the organization to continuing privacy breaches and liability from shareholder/customer/third-party lawsuits [12].

The remainder of this paper is organized as follows: Section 2 introduces the current privacy disclosure laws in the U.S. (at the time of publication). Section 3 provides details about the best available data sources we use in this investigation. Section 4 presents statistical processing results (in multiple dimensions) describing the source data along with analysis. Section 5 provides a brief overview of related work. We end with a summary and future work in Section 6.

## 2. PRIVACY BREACH DISCLOSURE LAWS

In the U.S., 28 states have enacted privacy breach laws (at time of publication), see Table 2 at the end of the paper. These state laws are similar but may have different requirements for notice trigger, timing, content, and recipients [13]. While other federal laws[3] also require reporting of storage security status of different various forms, these federal laws are focused on compliance with financial requirements for companies and non-profit organizations to federal regulators. In contrast, when private information is compromised, privacy breach state laws typically require only direct notification between the third party organization with the compromise and each affected individual without involvement from federal/state regulators or any level of law enforcement. Private information is defined to be any of the following: social security numbers, drivers license number, bank account numbers, credit/debit card numbers, as well as any other personal identifying information.

While the compromise of any individual identity has the potential for fraud, it should be noted that experience indicates only a percentage of compromised private data will be involved in identity theft fraud. For example, criminal investigators have found only 800 cases of fraud among the 163,000 identities exposed by the ChoicePoint privacy breach in 2004 (less than 0.5%) [9]. Nearly all breach disclosure laws provide an exemption if the personal data was encrypted at the time of the compromise [13].

## 3. DATA SOURCES

Privacy breach disclosure laws are currently established only in the United States and are not enacted in every state. However, even in the growing number of states that have such laws, disclosure reporting is only required between the organization and the affected parties (employees, customers, etc.) and there is no requirement for public reporting. As a result, there is no comprehensive data source on privacy breaches although there are several lists of breach incidents actively maintained on websites [1, 3].

Potential costs to an organization for a privacy breach reported in the mass media includes damage to reputation, loss of current/future customers, liability from other state's laws, and possible lawsuits from shareholders/customers. In the privacy breaches that have been disclosed, many were reported in the mass media first before being disclosed; thus leading one to infer that many privacy breaches required to be disclosed by law are not being disclosed unless forced to do so.[4]

No organization has been sued for not disclosing a privacy breach they were required by law to disclose. However, several organizations (particularly ChoicePoint) have been sued for negligence by parties affected by privacy breaches that were disclosed. This provides an additional economic incentive not to disclose privacy breaches.

Since there is not a standard format for disclosures, information that would be valuable for analysis is reported inconsistently and often not reported at all. In this paper, we have attempted to provide the best available view of disclosed privacy breaches by merging data from the two leading sources of privacy breaches: PrivacyRights.org [1] and Attrition.org [2]. The time period of analysis is between January 1, 2005 and June 5, 2006.[5] PrivacyRights.org has 182 privacy breach

[3]Federal laws relevant to reporting storage security status include: Sarbanes-Oxley, Gramm-Leach-Bliley, and HIPAA. For example, within Sarbanes-Oxley Law of 2002, Section 404 requires companies to document the effectiveness of internal controls/procedures and Section 409 requires real-time disclosure of information that changes the financial condition or operation of the company [4].

[4]For example, ChoicePoint first disclosed its 2005 breach only to California residents which had the first disclosure law in the nation and later disclosed to residents in other states and the District of Columbia, as new state laws were enacted.

[5]For final publication we intend to extend this period to June

incidents for this period. For each report, this data source provides date of the incident, organization name, type of breach, and number of records lost. Attrition.org has information on 183 privacy breach incidents for this same period. For each entry, it lists the following information: date, organization name, type of business, specific information about the business, type of data, specific nature of data, whether a third party was involved in data handling and loss, total records lost, and a reference to the notification or news item related to the breach.

We have manually merged these two lists into a single data set containing 219 breach reports for the time period and then manually entered this data set into a database system. This database containing disclosed privacy breaches 2005-2006 upon which our analysis is based is available for query via the Internet at the following URL: *url blinded for WESII'06 peer review*. To our knowledge, this is the most comprehensive data set on disclosed privacy breaches and its availability will both validate the results we report in this paper as well as enable future work by other researchers.

# 4. ANALYSIS

In this section, we analyze the data obtained from the two data source, and represent the data in various graphical formats in order to communicate the essence of the data set we have assembled. Unless otherwise noted, all values are rounded to the nearest integer.

Table 1 shows an overview of the nature of the data we analyzed. It shows the mean, median, standard deviation, confidence interval, and high / low values for the number of breach incidents and total records lost per month and per incident, during the chosen time interval.

It is interesting to see the large standard deviations from Table 1. This is because the data set contains two breach incidents which were vastly larger than the others, making the record size statistics highly skewed. The difference between the average values and the high values for record sizes reflects this, resulting in the large standard deviation.

## 4.1 Type of Organizations

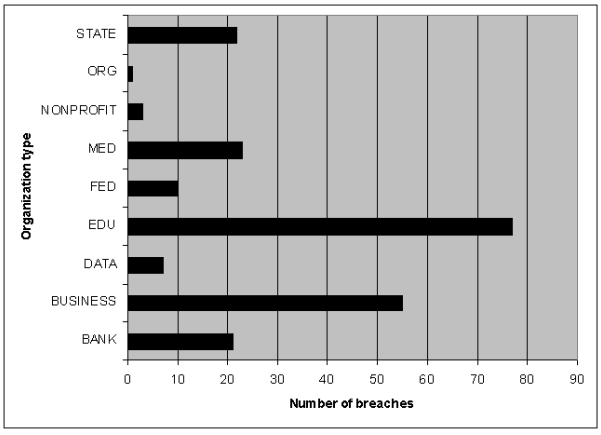



**Figure 1: Reported privacy breach incidents by organization.**

30, 2006 to have exactly 1.5 years of data for comparison.

| Disclosure Statistics (3 significant digits) | Frequency of disclosures per month | Record Size per month | Record Size per incident |
|---|---|---|---|
| Mean | 12.11 | 5.74M | 589K |
| Standard deviation | 5.68 | 14.9M | 3.8M |
| 95% Confidence Interval around Mean | 9.48 – 14.74 | 0 – 12.6M | 26.6K – 1.15M |
| Median | 12 | 913K | 20K |
| High | 21 | 57.8M | 40M |
| Low | 2 | 42K | 13 |

**Table 1: Overview of statistical information.**

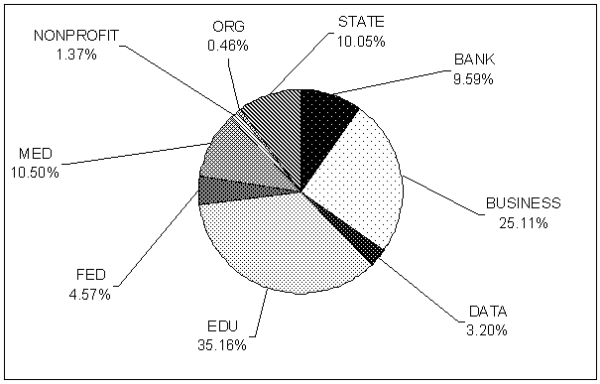



**Figure 2: Breakdown of privacy breach incidents by organization.**

Fig. 1 and 2 show that educational institutions constituted the largest portion of reported security breaches. Out of 219 reported cases, we find that 35% of the cases were reported from educational institutions. Businesses accounted for 25% of reports, followed by Medical organizations (11%) , State organizations (10%), and banks (10%). Now, the large number of incidents from educational institutions can be explained in two ways: either the security considerations for records are not strict, or educational institutions are more likely to report breach incidents, even in absence of laws mandating breach reporting.

In Fig.4, we show the percentage of total records lost for each type of organization. While Fig. 1 shows that educational institutions reported the most breaches, they account for only 2% of total records lost. The largest number of records lost were from business institutions (35%), followed by federal agencies (30%).

## 4.2 Type of Data

Fig. 5 shows the types of data items lost through breaches. We categorized the type of records into the following cate-

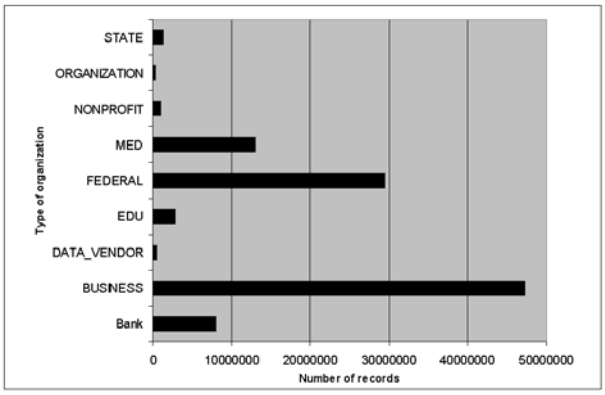



**Figure 3: Reported privacy records lost by organizations.**

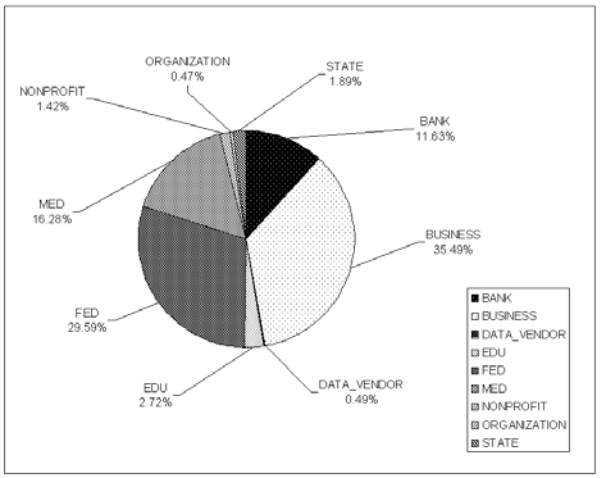



**Figure 4: Reported privacy records lost by organization.**

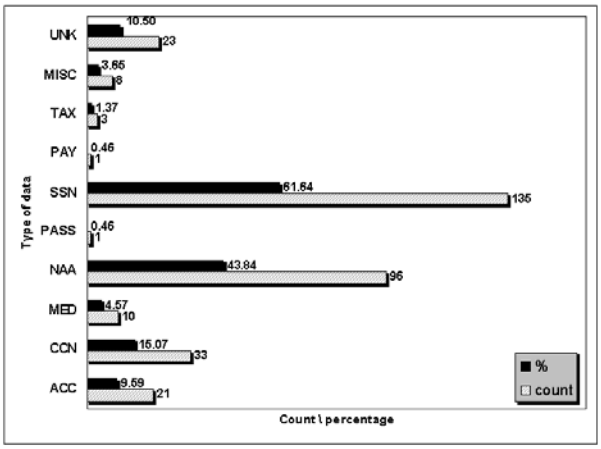



**Figure 5: Reported Breaches by Data Type.**

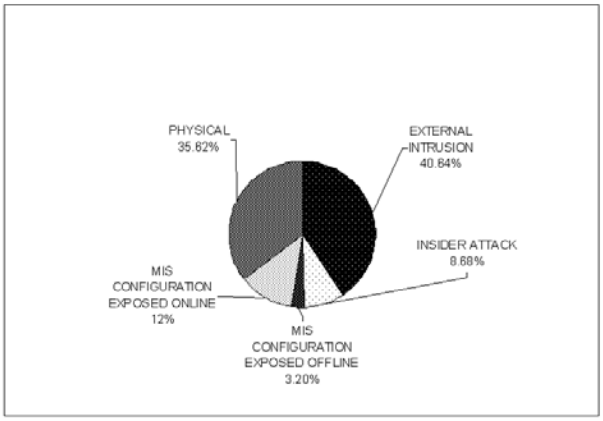



**Figure 6: Type of breaches.**

gories: social security numbers (SSN), names and addresses (NAA), credit card numbers (CCN), medical records (MED), account information (ACC), tax information (TAX), passwords (PASS), miscellaneous data (MISC), and unknown records (UNK).

From the figure, we can see that, social security numbers were by far the most common data stolen or lost. In 135 out of the 219 reported breaches (62%), SSN's were lost or stolen. This is understandable as social security numbers can be used effectively in various identity theft activities. The next most common type is name/address information, which amounted to 96 entries (44%). followed by credit card numbers, 15%, unknown record types, 11%, and account numbers 10%. Note that in many cases, more than one data types were among the lost/stolen records.

## 4.3 Type of breach

Fig. 6 shows the breakdown of different types of breaches. It shows that, 41% of the attacks occurred via external intrusion, implying a system breach or other type of malicious attack by external entities. The next most common type of breach was physical attack, covering 36% of total breaches. By this, we imply cases where loss or theft of media (tapes, hard drives, portable drives) or hardware (laptops, computers) occurred. Interestingly, many of these physical losses were due to loss or theft of laptops or backup tapes, often from cars or employee residences. These could perhaps be easily prevented via strict security policies regarding transfer of data to laptops, not allowing data to be taken to employee residences, and mandatory encryption of all types of data in transit. Data breach due to mis-configuration covered 12% of total breaches; these are cases where the data records were inadvertently exposed on the web or via email. Insider attacks by malicious insiders constitute 9% of the attacks, while accidental data loss via offline methods (e.g. SSN printed on mail labels) was the least of all – covering only 3% of total breaches.

## 4.4 Times of breach

Here, Fig. 7 shows the breakdown of number of reported breaches per month. Interestingly, the number of breaches per month shows a periodicity – with a peak attained in June 2005 followed by a fall in October 2005, before peaking again in February / March 2006. While there is no clear explanation for this, a possibility is the lapse in security during the

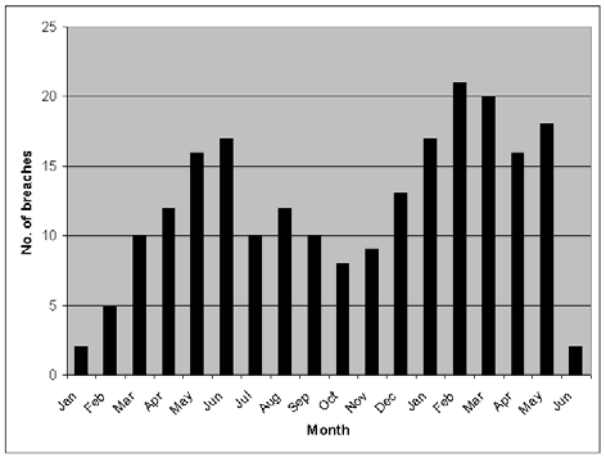



**Figure 7: Breach incidents per month (Jan 2005-Jun 2006.**

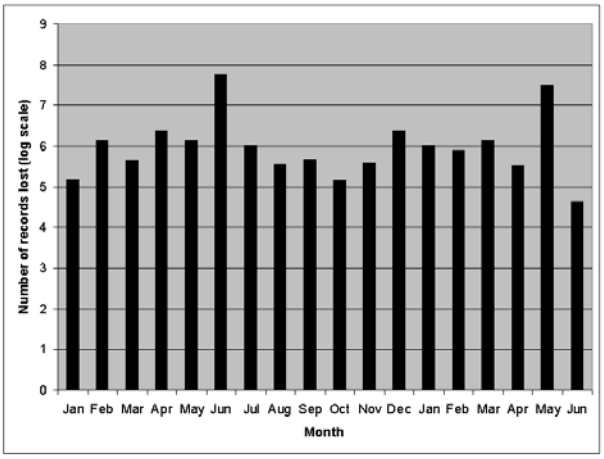



**Figure 9: Number of records lost per month (log scale), Jan 2005-Jun 2006.**

end of the financial year.

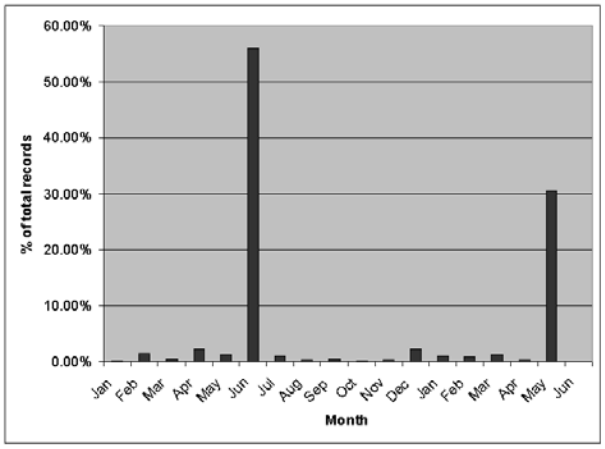



**Figure 8: Percentage of records lost per month (Jan 2005-Jun 2006.**

Fig. 8 shows the percentage of number of records affected per month. The figure shows two spikes - one in June 2005, and the other in May 2006. The former refers to a breach of CardSystems, resulting in loss of 40 million credit card records. The latter is the recent breach of social security numbers and other information of the U.S. Department of Veterans Affairs. Fig. 9 shows corresponding spikes in average number of records lost per month on a log scale so months with non-spike events are more visible. It also shows that the average number of records/month is approximately $10^6$.

## 4.5 Breach Sizes

The appendix of this paper has four scatter diagrams to better understand sizes. Fig. 10 is a scatter diagram of record size lost by date and shows peak events in early summer and a continuous clustering at mid-levels throughout the year.

Fig. 12 is a scatter diagram of record size lost by breach type and clearly shows physical breaches have a higher tendency than external breaches. Inside attacks are widely distributed while offline/online exposure are sparsely clustered at mid-levels.

Fig. 11 is a scatter diagram of distribution of different categories of data types throughout the time period.

Fig. 13 is a scatter diagram of record size lost per organization type and clearly shows education and businesses similarly clustered with more events than other organizations although businesses has some high volume events with no counterparts in educational organizations.

## 4.6 Case Study Across Organizational Types

The appendix of this paper has four sets of figures to compare different characteristics of privacy breaches across the top four different organization types in terms of number of breaches: (1) educational, (2) businesses, (3) banks, and (4) medical institutions.

Figs. 14-17 show reported breaches over the period of study – while reported breaches for banks and medical institutions are relatively constant in volume, the reported breaches for education and businesses is more cyclical reflecting the nature of their operations.

Figs. 18-21 show reported records lost per month – businesses peak to lose the most records while education has a steady level on non-peak records lost (note Y-axis is not the same between education and business).

Figs. 22-25 show reported breaches by breach type – while banks and medical institutions are dominated by physical breaches, businesses are relatively balanced between physical and external intrusions, and education is dominated by external intrusions.

Figs. 26-29 show reported breaches per data type – while education and banks are dominated by SSN breaches, businesses are dominated by credit card breaches, and medical institutions are dominated by miscellaneous medical identifiers. It must be noted that the data type in this category is not mutually exclusive, multiple data types can be lost in a single breach. The breach data type may be the closest distinguishing characteristic for types of different organiza-

tions.

## 5. RELATED WORK

We are aware of only three related efforts to analyze privacy security breaches. First, in [15] the authors summarize selected privacy security incidents reported in the press since 2000. At present [15] is limited in its analysis due to the small set of incidents and biased sampling but the authors state the report will be updated regularly so time will show the value of this work.

In [15], it is claimed that *almost half of the security breaches occurred at institutions of higher education.* Fig.2 shows that, considering the number of breach incidents, educational institutions indeed are the most vulnerable to privacy breaches (with 35% of total breaches). However, this does not take into account the number of total records affected. Fig. 4 shows the fraction of total affected records to be the highest in case of business entities (35%), while educational institutions account for only 3%. This is because, typically, the number of records lost from an educational institutions is not as high as that from business entities. [15] also claims that, *In 2005, a stolen computer (desktop, laptop, or hard drive) was the cause of the security breach 20% of the time.* Our analysis in Fig. 6 shows that 36% of breaches were due to such thefts which is a consistent although not exact result.

Second, from the State Government of California, [6] recommends best practices for organizations responsible for protecting personal information including making breach notifications to individuals. In addition to recommendations, [6] also includes lessons learned from studying breach notifications in California.[6] It makes several claims based on experience of being the first state to have enacted a privacy breach disclosure law in 2003. The report suggests more precautions should be taken to prevent physical losses, the most prevalent form of privacy breach (53%) in California. As shown in Fig. 6, the nationwide average for physical privacy breach is 36%. Next, the report claims that in California, loss of social security numbers are the most common type of data breach at 85%). Fig. 5 shows the nationwide figure we report is 61.64%, distantly followed by credit card numbers (15%), name and address (10%), and account information (10%). Thus our results are similar to both findings from the State of California.

Third, [7] studies the impact of privacy breaches on stock market valuation. The events used in [7] are limited to those affecting publicly traded firms and include different types of security incidents not limited to privacy breach disclosures.[7] While firms are an important part, they are still only part of the overall security breach picture. By excluding non-profit organizations (e.g. universities, hospitals, etc) and government agencies, and focusing on many different types of security events (not just privacy breaches), the data analysis in [7] cannot be compared directly to our work which focuses exclusively on privacy breaches across all organizations.

[6]Of course this analysis is limited to the unique environment within the State of California although many/most of the businesses in question with privacy breach disclosures have national presence.

[7]the [7] source data includes websites, mailing lists, news feeds, and blogs and was not made publicly available.

## 6. SUMMARY

There is in progress a multi-level response to the privacy breaches reported in the mass media. At the national level, the U.S. Office of Management and Budget has issued recent security directives that all Federal agencies encrypt classified/sensitive data on a laptop (or other handheld device), implement two-factor authentication for all remote data access, require remote or wireless users to re-authenticate after 30 minutes of inactivity, and the reporting of privacy breaches within one hour.[10] At the State level, U.S. states are either enacting a new law where there was no law previously or amending current laws with a variety of special requirements. Lastly organizations are now labeling data and protecting it with security solutions increasingly similar to classified environments.

While personal data on networked devices will always be subject to some risk, with investment the level of risk can be managed. This work is only a start to preventing and mitigating privacy breaches by analyzing and thus better understanding the demonstrated risks in the current environment January 2005 – June 2006. Recommending the type and level security solutions should have direct relationship to potential threats (threat modeling), probability of event occurrence (empirical event data analysis), potential event impact (empirical event data analysis) along with the tradeoffs and risk posture unique to different organizational environments. To do otherwise invites disaster in that chosen security solutions may not match the actual threats resulting in wasted investment, performance degradation, service denial, civil/criminal liability, and continued data compromise. We have carefully restrained ourselves from recommending security solutions since that is a next study to build upon this empirical event analysis.

## Acknowledgments

We acknowledge special insights on privacy breaches from (in alphabetical order): Arshad Noor (StrongAuth, Inc.), Umash Prasad (State of California Criminal Justice Statistics Center - Special Requests Unit) and Prof. Marianne Winslett (UIUC). We anticipate the constructive criticism of anonymous WESII'06 reviewers which we plan to incorporate to improve this paper.

## 7. REFERENCES

[1] A chronology of data breaches reported since the choicepoint incident (list). *Privacy Rights Clearinghouse* http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[2] Dataloss mailing list. *Attrition.org* http://attrition.org/security/dataloss.html.

[3] Entities that suffered large personal data incidents (list). *Attrition.org* http://attrition.org/errata/dataloss.

[4] Sarbanes-Oxley Act of 2002. *U.S. Securities and Exchange Commission*, http://www.sarbanes-oxley-forum.com.

[5] 2006 identity fraud survey report. *Better Business Bureau/Javelin National Survey*, http://www.javelinstrategy.com/research, 2006.

[6] Recommended practices on notice of security breach involving personal information. *State of California*

*Department of Consumer Affairs/Office of Privacy Protection*, April 2006.

[7] A. Acquisti, A. Friedman, and R. Telang. Is there a cost to privacy breaches? an event study. In *Workshop on the Economics of Information Security (WEIS)*, 2006.

[8] W. J. Clinton. Presidential Decision Directive/NSC-63 (PDD-63). May 22, 1998.

[9] C. Conkey. Identity theft: Shielding yourself. July 14, 2006.

[10] L. Greenemeier. After a lucky break with va laptop, feds tighten up. *InformationWeek*, July 3, 2006.

[11] R. Hasan, S. Myagmar, A. J. Lee, and W. Yurcik. Toward a threat model for storage systems. In *ACM International Workshop on Storage Security and Survivability (StorageSS)*, pages 94–102, 2005.

[12] M. Hines. Data losses may spark lawsuits. In *eWeek*, June 12, 2006.

[13] P. Mueller. How to survive data breach laws. *Network Computing*, June 8, 2006.

[14] B. Schneier. Risks of third-party data. *Communications of the ACM*, May 2005.

[15] R. Tehan. Personal Data Security Breaches: Context and Incident Summaries. In *Congressional Research Service Report for Congress*, December 16, 2005.

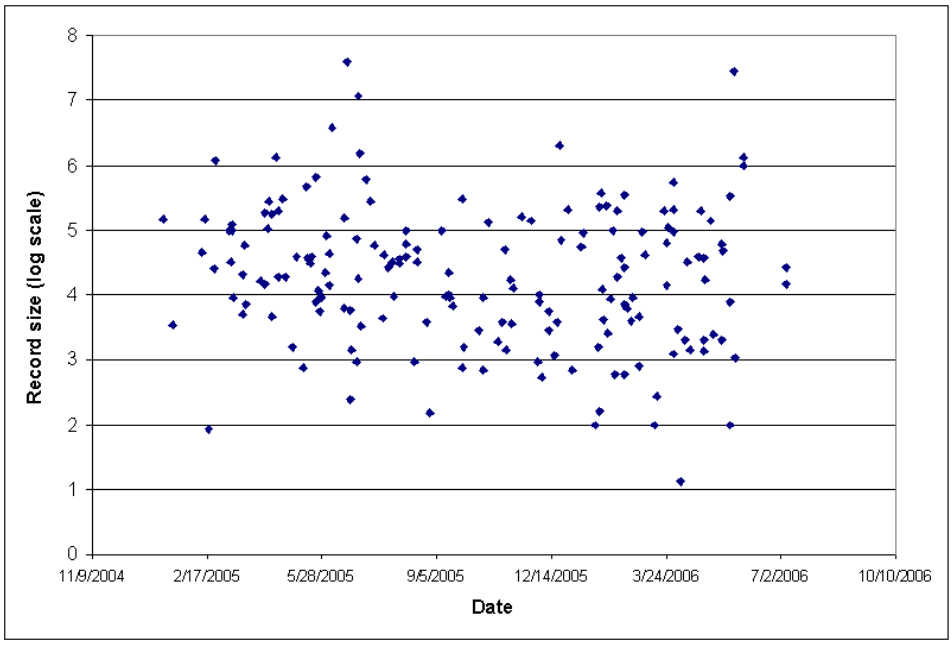



**Figure 10: Scatter diagram for number of records lost by date.**

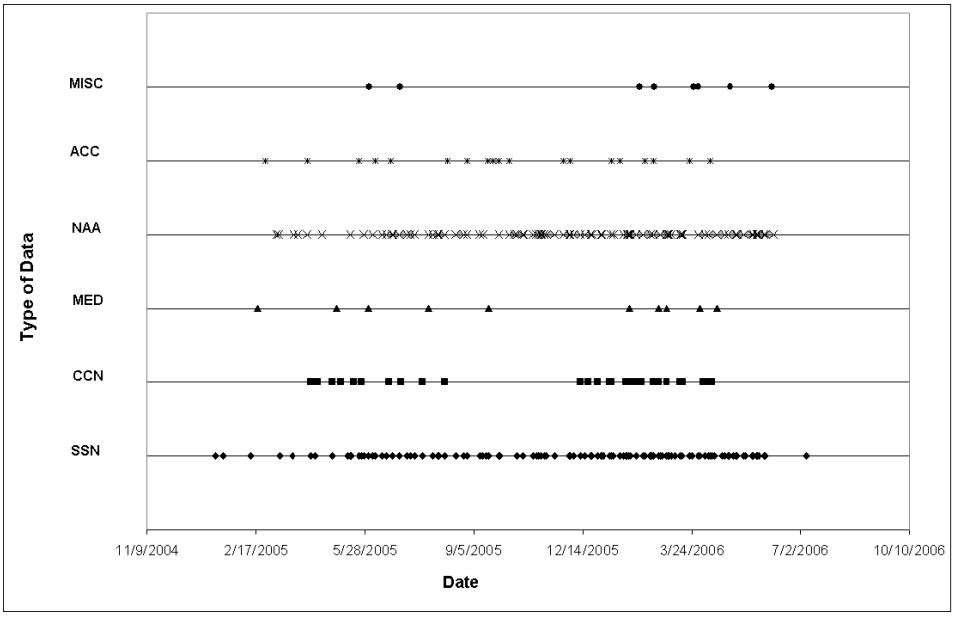



**Figure 11: Scatter diagram for data types lost by date.**

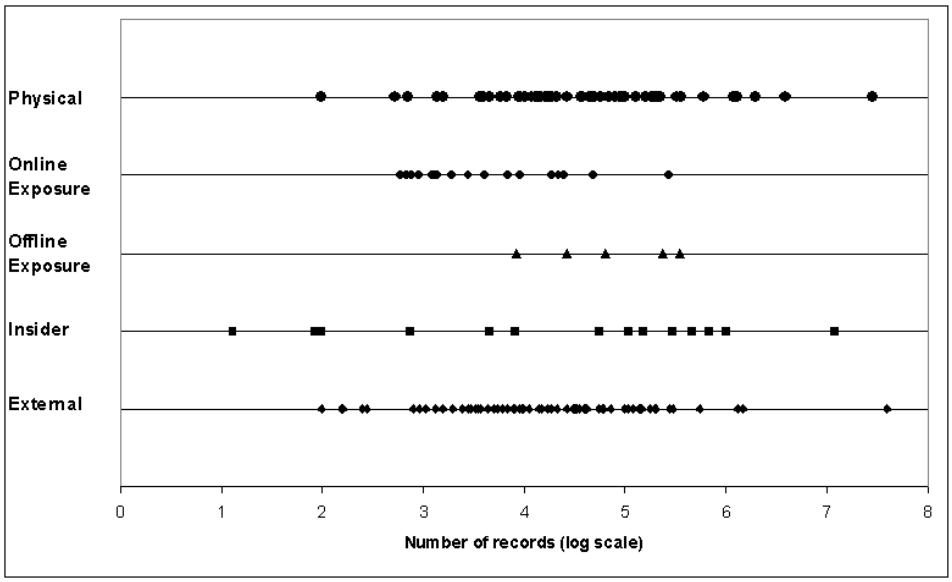



**Figure 12: Scatter diagram for number of records lost by breach types.**

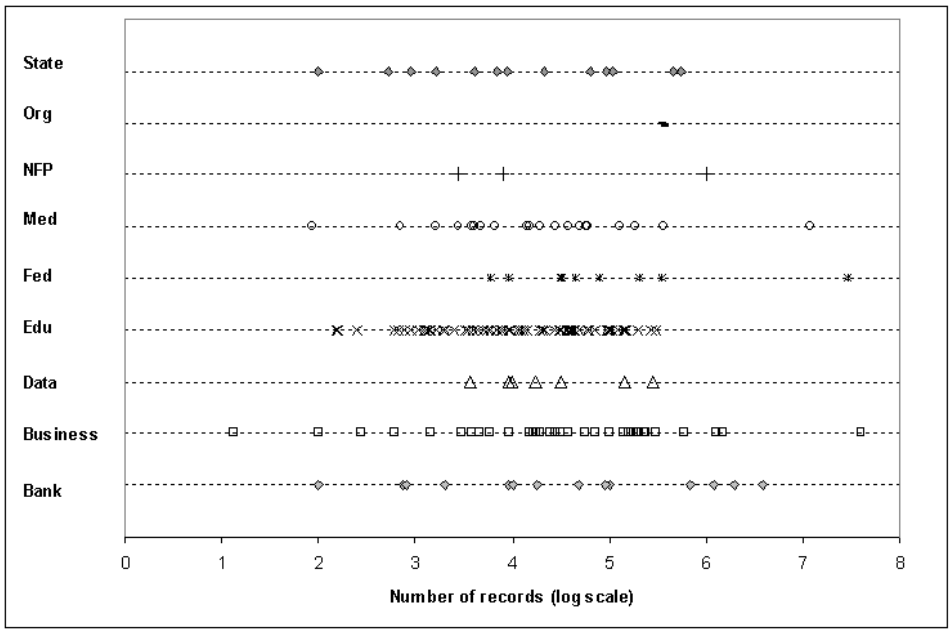



**Figure 13: Scatter diagram for number of records lost by organization type.**

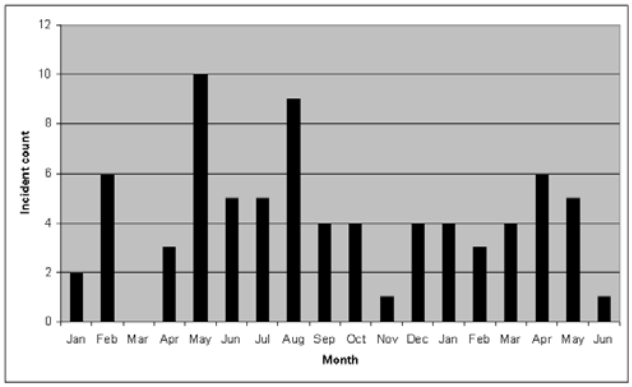



**Figure 14: Reported breaches per month: Educational institutions.**

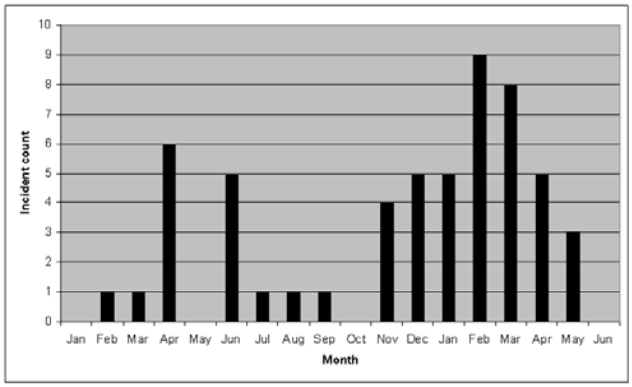



**Figure 15: Reported breaches per month: business institutions**

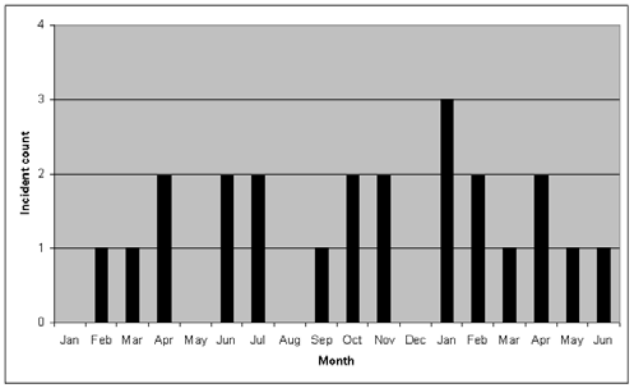



**Figure 16: Reported breaches per month: banks**

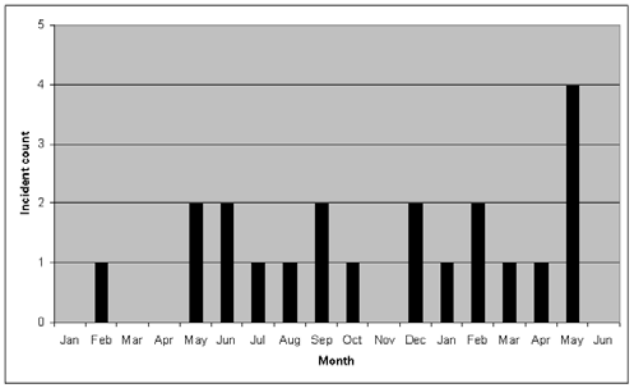



**Figure 17: Reported breaches per month: medical institutions**

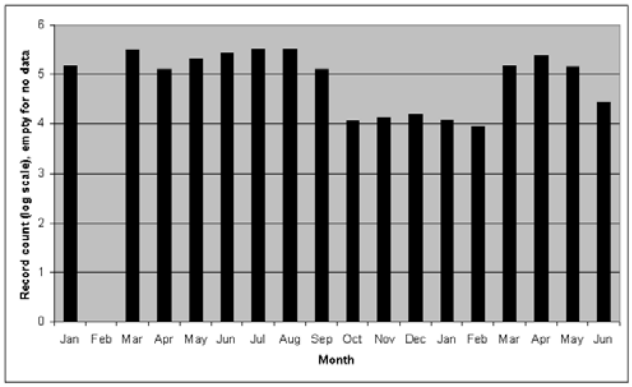



**Figure 18: Reported records lost per month: Educational institutions.**

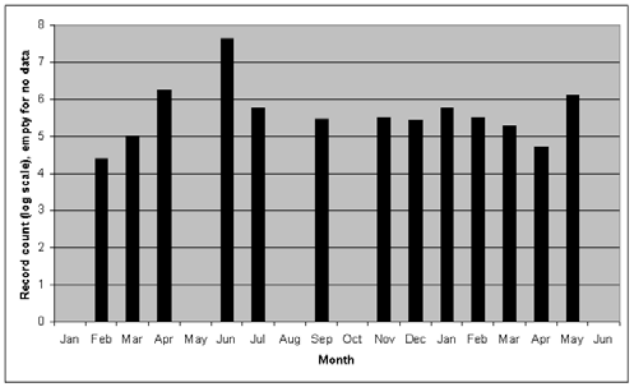



**Figure 19: Reported records lost per month: business institutions**

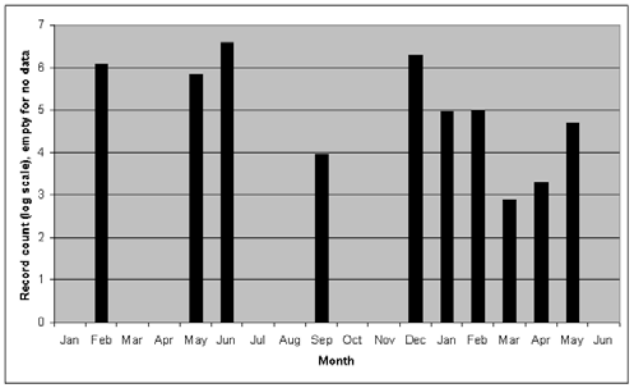



**Figure 20: Reported records lost per month: banks**

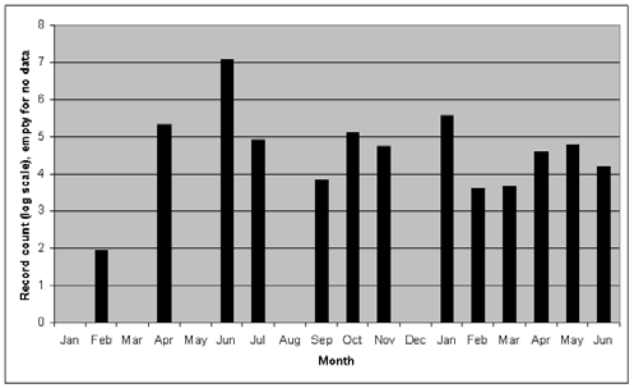



**Figure 21: Reported records lost per month: medical institutions**

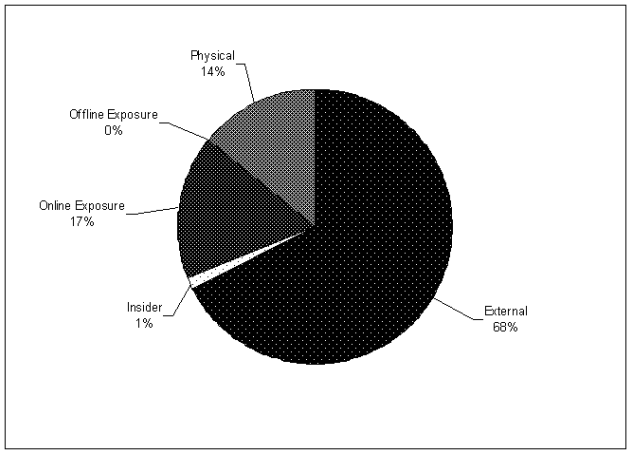



**Figure 22: Reported breaches by breach type: educational institutions.**

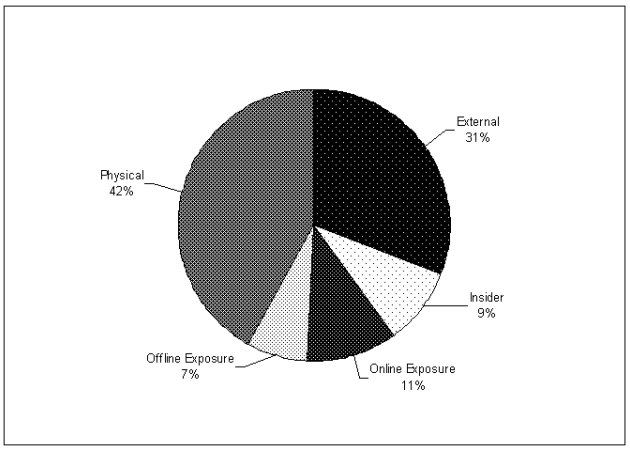



**Figure 23: Reported breaches by breach type: business institutions**

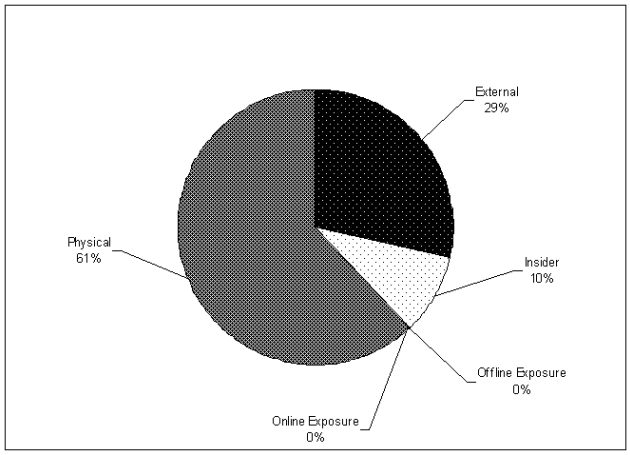



**Figure 24: Reported breaches by breach type: banks**

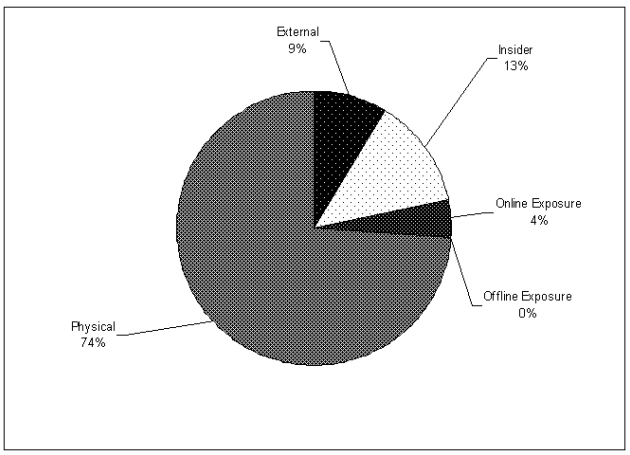



**Figure 25: Reported breaches by breach type: medical institutions**

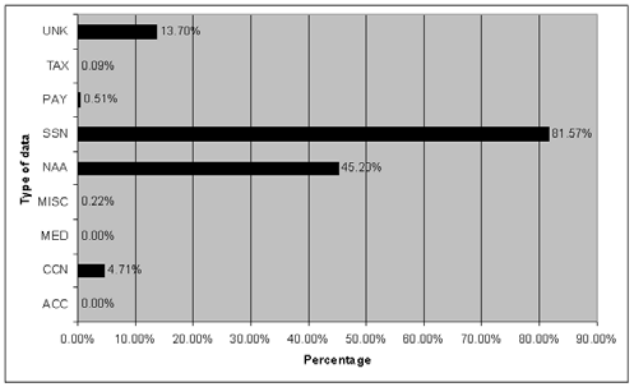



**Figure 26: Reported breaches by data type: Educational institutions.**

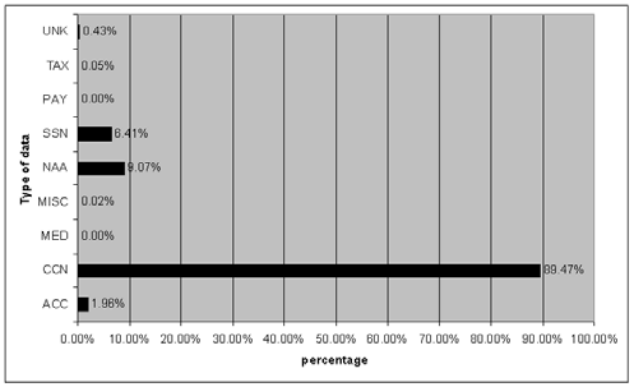



**Figure 27: Reported breaches by data type: business institutions**

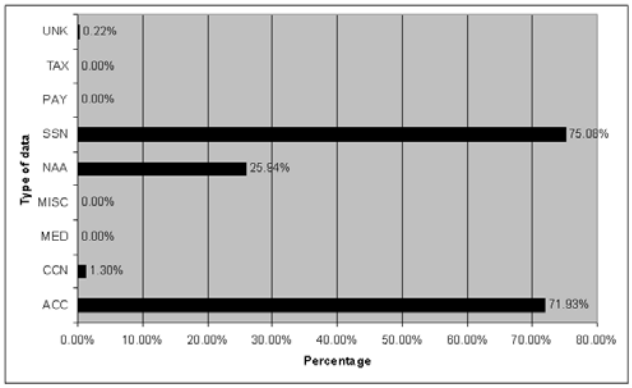



**Figure 28: Reported breaches by data type: banks**

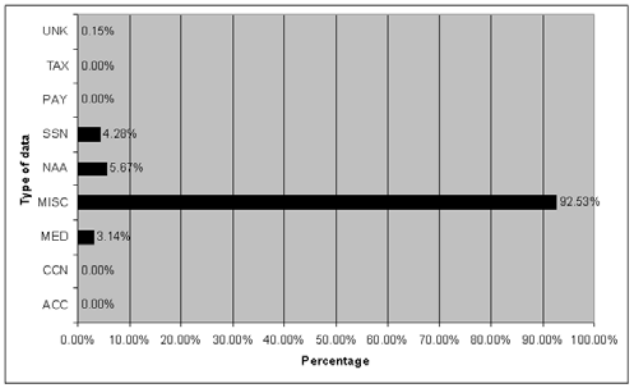



**Figure 29: Reported breaches by data type: medical institutions**

| States | Start Date | State Law | Responsible Party | Likelihood of Harm Threshold | Best Practices Required |
|---|---|---|---|---|---|
| (1) California | 07/01/03 | SB 1386 | entities conducting business, separate section for state agencies | no | yes |
| (2) Arkansas | 03/31/05 | SB 1167 | entities conducting business | yes | yes |
| (3) Georgia | 05/06/05 | SB 230 | data brokers only, excludes state agencies | no | no |
| (4) North Dakota | 06/01/05 | SB 2251 | entities conducting business | no | no |
| (5) Delaware | 06/28/05 | HB 116 | entities conducting business | no | no |
| (6) Florida | 07/01/05 | HB 481 | entities conducting business | yes | no |
| (6) Tennessee | 07/01/05 | HB 2170 | "information holder" including people, business, or state agency | yes | no |
| (8) Washington | 07/24/05 | SB 6043 | any person or business, plus state agencies | yes | no |
| (9) Texas | 09/01/05 | SB 122 | a person that conducts business | no | yes |
| (10) Nevada | 12/01/05 | SB 347 | data collectors, including all entities and state agencies | yes | yes |
| (10) North Carolina | 12/01/05 | SB 1048 | any person or state agency | no | no |
| (12) New York | 12/08/05 | SB 5827 | any person or business | no | no |
| (13) Connecticut | 01/01/06 | SB 650 | any person that conducts business | yes | no |
| (13) Illinois | 01/01/06 | HB 1633 | data collectors, including all entities and state agencies | no | no |
| (13) Louisiana | 01/01/06 | SB 205 | any person or agency | yes | no |
| (13) Minnesota | 01/01/06 | HF 2121 | entities conducting business, section for state agencies | no | no |
| (13) New Jersey | 01/01/06 | A4001 | a business or public entity | yes | yes |
| (18) Maine | 01/31/06 | LD 1671 | data brokers only, excludes state agencies | no | no |
| (19) Ohio | 02/15/06 | HB 104 | any person or state agency | yes | no |
| (20) Montana | 03/01/06 | HB 732 | entities conducting business, plus special requirements for insurers | yes | yes |
| (20) Rhode Island | 03/01/06 | HB 6191 | any state agency or person, including all businesses] | yes | yes |
| (22) Wisconsin | 03/31/06 | SB 164 | entities conducting business | no | no |
| (23) Oklahoma | 06/08/06 | HB 2357 | only state entities | no | no |
| (24) Indiana | 06/30/06 | 503 | person or government agency | no | no |
| (24) Pennsylvania | 06/30/06 | SB 712 | any entity | yes | no |
| (26) Idaho | 07/01/06 | 28-51-104 | entities conducting business | yes | no |
| (27) Nebraska | 07/13/06 | LB 876 | entities conducting business | yes | no |
| (28) Colorado | 09/01/06 | 6-1-7161a | entities conducting business | yes | no |
| (29) Arizona | 12/31/06 | SB 1338 | entities conducting business | yes | yes |
| (30) Hawaii | 01/01/07 | SB 2290 | entities conducting business | no | no |
| (30) Kansas | 01/01/07 | SB 196 | entities conducting business | yes | no |
| (30) New Hampshire | 01/01/07 | HB 1660 | entities conducting business | yes | no |
| (30) Utah | 01/01/07 | SB 69 | entities conducting business | yes | no |
| (30) Vermont | 01/01/07 | SB 284 | entities conducting business | no | no |

**Table 2: Summary of State Laws for Privacy Breach Disclosures adapted from: (1) "State Laws Governing Security Breach Notification", Crowell Moring LLP, 01/25/06. http://www.crowell.com/; (2) "Security Breach Notice Legislation: Effective Dates, and Security Breach Notification Chart," Perkins Cole Attorneys Al Gidari, Barry Reingold, and Matt Staples; and (3) "Notice of Security Breach State Laws," Consumer Union, June 27, 2006.**