Center for Communication & Civic Engagement

A Case of Mistaken Identity? Reporting Responsibility for Compromised Digital Records, 1995-2005

Philip N. Howard
University of Washington
pnhoward@u.washington.edu

Working Paper #6
2006

A Case of Mistaken Identity?
Reporting Responsibility for Compromised Digital Records, 1995-2005[1]

Kris Erickson
Philip N. Howard
University of Washington

Center for Communication and Civic Engagement
Working Paper # 2006-5

A Case of Mistaken Identity?
Reporting Responsibility for Compromised Digital Records, 1995-2005[2]

5/25/2006

Kris Erickson
Philip N. Howard
University of Washington

Abstract

We analyze over 215 incidents of compromised data between 1995 and 2005. All in all, some 1.76 billion records have been exposed, either through hacker intrusions or poor management. In the context of the United States, there have been 8 records compromised for every adult. Between 1995 and 2005, businesses were the primary sources of these incidents, but we find that the recent legislation in California to require notification of privacy violations has exposed educational institutions as among the least well equipped to protect the privacy of their students, staff, and faculty. Options for public policy oversight are discussed. However, recent legislative responses have favored market-based solutions instead of direct government regulation of electronic data.

I. INTRODUCTION

Recently, electronic personal records have become the subject of a great deal of public interest. Their ubiquity has spurred debates about the nature of our democratic society, the potential for electronic panopticism, and the erosion of personal privacy in an era of increased police surveillance. Attention has been leveled at the various aspects of data collection, data management (or mismanagement) and the potential for unwanted disclosure of private records through loss or theft. A series of high-profile cases culminating in the 2005 loss of more than 140,000 customer credit records by ChoicePoint has helped to generate further interest in the dangers associated with electronic personal data. So far, a considerable amount of blame has been directed at all parties involved: at the state, for being lackadaisical in regulating institutions and businesses that

deal with electronic records; at the private sector, which is accused of de-prioritizing personal privacy and information security; and finally at the end users themselves, who are enjoined by a variety of authorities and experts to take better care of managing their online identities in order to mitigate the risk of fraud.

As a society, how we assign responsibility will ultimately shape the responses that we collectively devise to manage the use of these electronic personal records. This chapter will explore how this responsibility is currently distributed, by examining legislation designed to manage the problem of compromised personal data. We will then compare the aims of this legislation with an analysis of reported incidents of data loss for the period of 1995-2005. A discrepancy between legislative responses to electronic data loss and the actual damages incurred would suggest that responsibility for maintaining the security of electronic personal records has been misplaced and should be re-examined.

II. U.S. Legislation To Secure Electronic Records

One of the features of information technology pointed out by legal scholars is that it consistently presents legislators with the challenge of regulating issues for which there are no readily apparent legal precedents. Lawmakers are frequently cast as lagging behind technological innovation, as they struggle to catch up with new forms of behavior enabled by rapidly evolving technology. Offline legal concepts such as private property and trespass often become problematic when applied to their online counterparts.

For example, Cavazos and Morin (1996) have argued that in the case of defamatory, libelous, and obscene speech, the law has struggled to adequately account for the nuances of computer mediated communication. Publishers and re-publishers of offline defamatory statements can be held liable, because it is expected that they possess considerable editorial control over their own published content. However, when publication moves into an online setting, the distribution of liability becomes less clear. Not all internet publishers maintain

strict editorial control, and some media outlets function more like “conduits” through which news is automatically updated. Other websites allow users to generate content, with limited moderation provided by the system administrator. In both of these cases, it becomes more difficult to assign responsibility for defamatory material.

The decentralized nature of computer networks poses other challenges for regulators. In cases involving obscenity, lawmakers in the United States have employed a method known as the “community standards test” to determine when published material can be considered obscene. Material is deemed to lie outside the protections afforded by the first amendment when it is found to be offensive to the norms and standards of the community in which it is located. While this method has functioned adequately in offline settings, it is less effective when individuals from diverse communities can transmit information to one another, often across state and national boundaries (Cavazos & Morin, 1996; Zook, 2003). Early applications of the community standards test to online publishers proved unworkable. In the case of *United States v Thomas* (6th Cir., 1996) a website operator located in California was tried in Tennessee for violating the obscenity laws in the jurisdiction where the material was accessed, rather than where the material was stored. This case is often cited as evidence that current legislation is anachronistic and lags behind the requirements of communication technologies that bypass traditional jurisdictional boundaries.

These jurisdictional conflicts become even more apparent in cases where lawmakers have attempted to regulate behavior across several legal jurisdictions, such as music piracy and online gambling. Faced with an overwhelming number of users, along with the relative anonymity provided by computer mediated communication, prosecutors in the United States have tended to focus efforts on website operators rather than on end users. The jurisdictional challenges posed by computer networks continue to hamper their efforts in this regard, however, since offending websites can be operated offshore in areas with less stringent regulation. The United States has pursued this strategy in regard to online

gambling, with limited success. Charges brought by New York State against 22 online gambling websites in 1999 yielded only one arrest, when the operator visited the country on vacation (Wilson, 2003).

An additional problem facing legislation aimed at controlling online behavior is its questionable effectiveness as a deterrent. The Computer Fraud and Abuse Act (CFAA) was passed in 1984 in response to growing political and media attention surrounding the dangers of computer crime. The Act criminalized unauthorized access on private computer systems, making it a felony offense when trespass leads to damages over a certain monetary threshold. The CFAA underwent major revisions in 1986 and 1996 and it was further strengthened by the passage of the USA Patriot Act in 2002. Overall, these revisions have served to make the act more broadly applicable to various kinds of computer crime, while also increasing the punitive response to these offenses. For example, the revisions in 2002 were tailored to make it easier to surpass the $5000 felony threshold. The threshold was waived in cases where computer systems involved are used for national security or law enforcement purposes. In cases not involving national security, the definition of "damage" was broadened to include costs relating to damage assessment and lost revenue during an interruption of service. The $5000 threshold is also cumulative over multiple machines if more than one system is involved in an attack[3]. Additionally, the maximum sentence for felony computer trespass was raised from 5 to ten years for first-time convictions, and from 10 to 20 years for repeat offenders (Skibell, 2003).

Given the relatively harsh penalties for computer trespass compared to other crimes where victims suffer personal physical harm, it is surprising that the CFAA has not been more effective as a deterrent. The apparent surge in computer-related offenses, including the theft of online personal records, suggests that the punitive nature of this legislation is not having the desired effect. Skibell argues that recent work from sociology supports the notion that not all computer crime is committed by self-interested or malicious criminals.

More legitimate computer hackers appear to be motivated by codes of conduct internal to their community and are therefore less likely to be deterred by legal sanctions (p.13). According to Jordan and Taylor (1998), these legitimate or "white-hat" computer hackers are motivated by a variety of concerns that make comparisons with other types of criminal behavior problematic.

> How often does a burglar leave behind an exact copy of the video recorder they have stolen? [...] What bank robbers ring up a bank to complain of lax security? The simple analogy of theft breaks down when it is examined and must be complicated to begin to make sense of what hackers do. (1998, p. 772).

In many cases, these authors argue, what hackers do is shaped by an ethical framework formed by a strong sense of imagined community. Many hackers are interested in the intellectual challenge and sense of mastery provided by computer networks, rather than monetary rewards that could be gained from accessing sensitive information. They seek to differentiate themselves from other computer criminals that use computer networks for destructive, rather than creative processes. If computer hackers derive a sense of identity from norms shared within their community, it is unlikely that punitive legislation will have a deterrent effect on their actions.

Arguably, the most significant threat posed by computer criminals does not come from this core group of "legitimate" hackers, but from individuals who make use of hacker techniques to invade systems for monetary gain. Since knowledge and tools developed by more experienced hackers can easily be obtained on the internet, the capability to penetrate insecure networks has propagated outside of the legitimate hacker community to other groups, ranging from inexperienced teenagers to international crime syndicates[4]. These individuals may feel protected from the law due to the relative anonymity of

CMC, or they may be located in jurisdictions where harsh criminal penalties for computer fraud do not apply.

While the CFAA aids in the prosecution of criminals who engage in electronic data theft and trespass, individual states have recently taken additional legal steps to regulate the management of electronic records. In 2003, the state of California introduced a new provision to the Information Practices Act, termed the "Notice of Security Breach". This addition to the California Civil Code obliges any business or agency that has been the victim of a security breach to notify any parties whose personal information may have been compromised. The California legislation defines "personal information" as an individual's full name, in combination with one of the following types of data:

> (1) Social security number.
> (2) Driver's license number or California Identification Card number.
> (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

The company or institution responsible for handling the compromised data must notify potential victims individually, unless the cost of notification exceeds a threshold amount of $250,000, or if the total number of individuals affected is greater than 500,000. In these cases, substitute notification can be made using a combination of e-mail notification and disclosure to major media outlets. Notification must be carried out "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement [...] or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." (California Civil Code 1798.29). Following California's footsteps, 22 additional States have enacted similar legislation as of 2005. For the most part, individual State legislatures have

maintained the spirit of the California provision, including the extension of liability to both businesses and agencies, as well as the notification threshold.

The aim of the "notification of breach" legislation is significantly different from the CFAA. By making corporations and institutions liable for damages potentially incurred by customers and clients, this legislation seeks to discipline offenders who engage in poor record-keeping practices. Both the indirect threat of future litigation and the potential for public embarrassment are intended to improve data security in both the public and private sector. Unlike the CFAA, however, this legislation does not directly address the issue of network security. It does not formalize standards or rules for information security, nor does it make businesses and institutions accountable for poor security practices that may make them vulnerable to attack. The legislation punishes businesses only for failing to notify the public, rather than for negligence in securing electronic records. Since adequately securing a computer network from intrusion is an expensive prospect, this legislation essentially lets businesses off the hook, by making them liable for damages only when they fail to notify affected individuals that their data has been compromised. Interestingly, by failing to assign responsibility for data loss to those agencies that manage electronic personal information, this legislation serves to shift that responsibility to the individual user, since it is he or she who must take steps to protect their identity once notified of a breach.

This sentiment is supported by the California Department of Consumer Affairs, which maintains a website devoted to online privacy protection. The agency has also distributed a flyer listing the "top 10 tips for identity theft prevention". This list enjoins consumers to take active steps to avoid becoming the victims of electronic fraud, by shredding personal documents, installing up-to-date computer virus and firewall software, and becoming vigilant about which sites they visit and how they use their credit cards. Consumers are also urged to take a more proactive role in monitoring their personal credit rating, in order to detect potential fraud. The Department of Consumer Affairs recommends that

individuals apply for free credit reports at least 3 times per year in order to prevent misuse of their electronic identity.

So far, the legal responses to electronic identity theft in the United States have sought to minimize the direct involvement by the state, instead relying on a partnership between the interests of private institutions and the consumers of those services. This strategy of government, whereby states seek to achieve policy outcomes through the discipline of market mechanisms, is consonant with what Nikolas Rose and other scholars have described as neoliberal governmentality (Burchell, 1996; Rose, 1999; Dean, 1999). Building on Foucault's original essay on governmentality (1978) this literature has explored strategies of government in Western liberal societies. These authors have argued that the mode of government in Western democracies has begun to shift from a welfarist conception of security, in which the state assumed the role of service provider "from the cradle to the grave" to one in which the state increasingly organizes itself around market principles of competitiveness and profit, and employs these market principles to guide political decision-making. During the Keynesian period from the end of the Second World War to the 1970s, Western liberal states in Europe and North America understood the provision of social welfare to be integral to the healthy functioning of social and economic processes. Since the 1970s and the period of sweeping market reforms broadly associated with the Reagan and Thatcher administrations, the focus has shifted away from the direct involvement of the state in social welfare to a system based on market relationships between producers and consumers. On one hand, this has been accompanied by a "roll-back" of state funded programs under the perceived pressure of budgetary constraints, and on the other hand, we have seen a roll-out of a variety of policy prescriptions to deal with ongoing and acute problems raised by a retreating state apparatus (Peck & Tickell, 2002). The language of service provision now seeks to implicate individual consumers of services such as health, welfare, and security as active agents in their own self-actualization. Graham Burchell refers to this process as

"responsibilization", the offloading of responsibility for social security onto active and self-motivated subjects:

> This involves "offering" individuals and collectivities active involvement in action to resolve the kind of issues hitherto held to be the responsibility of authorized governmental agencies. However, the price of this involvement is that they must assume active responsibility for these activities, both for carrying them out and, of course, for their outcomes (1996, p. 29).

Authors who have explored these societal shifts in the neoliberal governmentality literature have tended to focus on the material social struggles over welfare-state retrenchment, rather than on more abstract issues such as the legal regulation of cyberspace. However, the legal response that many states have adopted to deal with the problem of electronic records suggests that a governmentality analytic might be appropriate to studying legislation directed at cyberspace.

III. Analysis of Compromised Electronic Records, 1995-2005

Using Lexis-Nexis, we conducted a search of incidents of electronic data loss reported in major U.S. periodicals from 1995-2005. We used a snowball methodology to expand our analysis by including additional security breaches mentioned in the same article. Our method yielded 215 reported incidents, which were then cross-checked with additional sources to ensure accuracy.

Our list of reported incidents is limited to cases where one or more electronic personal records were compromised through negligence or theft. We acknowledge that there may be occasions where an end-user considers their data compromised when it is sold among third parties for marketing purposes without their informed consent. For this study, we only look at incidents of compromised records that are almost certainly illegal acts. For the purposes of this paper, we define electronic personal records as data containing privileged

information about any individual that cannot be readily obtained through other public means. Rather than become involved in the broader debate about the virtues and dangers of online anonymity, we have chosen to focus on data that is more sensitive than the information that we regularly volunteer in the course of surfing the web (such as one's name or IP address). We have focused on information that should reasonably only be known to the individual concerned, or be part of a confidentiality agreement (such as between a patient and a care provider). Electronic personal records therefore include individuals' personal credit histories, banking information such as credit card numbers or account numbers, medical records, social security numbers, grades, and criminal records. We focused only on incidents where compromised personal records were kept for a legitimate purpose by a company, institution, or government agency. Consequently, "phishing" or spoofing scams where victims are deceived into volunteering their own personal information are not included in our analysis. All of the incidents in our analysis deal with data that was maintained in electronic form, although in some cases compromised data was contained on a lost or stolen laptop computer.

Table 1: Reported Incidents and Volume of Compromised Records by Sector, 1995-2005

Sector	1995-1999, 27 Reports Records (Number)	(%)	2000-2004, 67 Reports Records (Number)	(%)	2005, 121 Reports Records (Number)	(%)	1995-2005, 215 Reports Reports (Number)	(%)
Commercial	53,401,189	100.0	1,646,016,716	99.9	49,462,297	88.0	1,748,880,202	99.5
Educational	10,000	0.0	1,487,111	0.1	1,751,108	3.1	3,248,219	0.2
Government	20	0.0	76,333	0.0	4,561,198	8.1	4,637,551	0.3
Medical	3,010	0.0	28,222	0.0	413,685	0.7	444,917	0.0
Military	461	0.0	13,600	0.0	33,001	0.1	47,062	0.0
Non-Profit	0	0.0	74	0.0	0	0.0	74	0.0
Total	53,414,680	100.0	1,647,622,056	100.0	56,221,289	100.0	1,757,258,025	100.0

Between 1995 and 2005, some 1.76 billion records were reported compromised by government agencies, firms, hospitals, and other kinds of organizations. In a sense, this number of lost records is larger than we might expect because a few

landmark incidents account for large portions of the total number of records compromised. The number of incidents—215 in all—may seem smaller than expected given the eleven year time frame of our search. Some articles report multiple incidents, and of course many incidents were covered by journalists on multiple occasions. There are an estimated 235 million adults living in the United States, so we can conservatively estimate that for every U.S. adult, 7 private records have been compromised during the 11-year period covered by this study.[5]

Table 1 shows the total number of reported incidents of compromised records between 1995-2005, along with the distribution of such incidents by sector. Over half of the incidents involved commercial actors, less than a third of the incidents involved colleges and universities, and the remainder involved government, hospitals, and the military. When the exceptional 2004 loss of 1.6 billion records by Axciom Corporation is removed, the commercial sector still accounted for approximately 148 million individual compromised records, more than thirty times that of the next-highest contributor, the government sector. The education sector accounted for a small percentage of the overall quantity of lost records, but accounted for nearly 30 percent of all reported incidents, suggesting that educational institutions suffer from a higher rate of data loss than might be anticipated. This could be explained by the fact that educational institutions generally maintain large electronic databases on current and past students, staff and faculty. However, medical institutions – which presumably also maintain large quantities of electronic data – reported a significantly lower number of incidents of data loss.

The table reveals the steep climb in reported incidents since California's legislation took effect. In the five year period between 1995 we found 28 incidents of compromised digital records. This number more than doubled in the five year period between 2000 and 2004. In the year 2005 alone, there were three times as many reported incidents as compared with the earliest 1995-1999 period. Interestingly, the mandatory reporting legislation seems to have

exposed educational institutions as a major source of leakage of private data. In the ten year period from 1995 to 2004, corporations were the primary source of compromised data. But in 2005, the majority of incident reports were generated by universities and colleges. These kinds of organizations may have been the least equipped to protect the data of their students, staff and faculty. However, over time private firms consistently hemorrhage the greatest volume of records.

Several factors might explain the pattern of increasing incidents and volume of compromised data over time. First, there is the possibility that the results are skewed due to the relative quantity of new, fresh news stories devoted to this issue, with older reports simply disappearing from the record as they become obsolete and are deleted. If this were the case, we would expect to see a gradually decaying pattern with greater number of reported cases in 2005 than in 2004, 2003, and so on. The dramatic difference in reported incidents between 2004 and 2005 suggests that this effect does not adequately explain our observations. A second possibility is that increased media attention in 2005 lead to a relative over-reporting of incidents, compared with previous years. Literature on media responses to perceived crises or "moral panics" would suggest that a similar effect commonly accompanies issues that are granted a disproportionate amount of public attention, such as with the case of the mugging scare in Great Britain in the 1970s or the crackdown on the rave subculture in the 1990s (Hall et. al 1978; Critchter, 2003). While it is unlikely that media outlets have exaggerated the amount of electronic personal record loss, it is possible that in previous years a certain number of events went unreported in the media due to lack of awareness or interest in the issue. A third possibility is that there were a greater number of reported incidents of data loss in 2005, because institutions are maintaining and losing a larger quantity of electronic data, and because a changing legislative environment in many states is obliging institutions to publicly report events that may have gone unreported in previous years.

It is likely that a combination of factors explain our observations. The Notification of Breach legislation that requires the prompt reporting of lost records in California came into effect in 2003, however the legislation was not widely adopted and implemented by other states until 2004/2005, which might help to explain the dramatic increase in reported cases. The Notification of Breach legislation in California, like many other states, requires notification when a resident of the State of California has been a victim of data loss, regardless of where the offending institution resides. Therefore, institutions located in states without Notification of Breach laws, such as Oregon, are still required to report cases to victims who live in states that have enacted this type of legislation, such as New York. The nature and complexity of institutional databases means that in many cases, compromised databases are likely to contain information about residents who are protected by notification of breach legislation, thus increasing the total number of reported cases.

For the majority of incidents, the news article reports some information about how the records were compromised. A closer reading of each of the incidents, however, reveals that most incidents are actually a combination of mismanagement, criminal intent, and occasionally, bad luck. Hackers are often blamed, but occasionally the hacker is known to be an insider, such as a student or employee. Moreover, company public relations experts often posit that personal records were only "exposed" when they cannot tell that the records have been specifically copied by intruders.

Table 2: Reported Incidents by Type of Breach, 1995-2005

	1995-1999 %	2000-2004 %	2005 %	1995-2005 %
Stolen - Hacker	52	52	36	43
Unspecified Breach	30	27	10	18
Exposed Online	11	9	14	12
Missing or Stolen Hardware	4	1	24	14
Insider Abuse or Theft	4	7	10	8
Administrative Error	0	3	6	4
Total	100	100	100	100

Table 3: Reported Incidents by Type of Sector, 1995-2005

	1995-1999 %	2000-2004 %	2005 %	1995-2005 %
Commercial	74	69	34	50
Educational	4	12	46	30
Government	4	4	11	8
Medical	7	9	7	8
Military	11	4	2	4
Total	100	100	100	100

Table 2 reveals that the legislation has also seemed to have the effect of forcing the reporting organizations to reveal more detail about the ways these private records get compromised. In the ten years between 1995 and 2004, the bulk of incident reports had paltry details, with most incidents described as an unspecified breach or as the result of hackers. However, by 2005, the majority—some 46 percent—of incidents were revealed to involve different kinds of organizational culpability. Sometimes management accidentally exposed private records online, administrative error resulted in leaked data, or employees were caught using the data for activities not related to the business of the organization. By 2005, a fifth of the incidents took the form of missing or stolen hardware. On some occasions, staff simply misplaced backup tapes, while on others, computer equipment such as laptops were stolen.[6]

Table 3 reveals the important trends in incidents of compromised records by sector. Over the decade of this survey, half the incidents of compromised records involved corporate actors losing or exposing data. But even though the private businesses lose the largest volume of private records, the proportion of newspaper reports identifying a business has actually diminished over time. Surprisingly, colleges and universities have become the most often reported target organization. Over time, incidents involving military targets have declined.

IV. CONCLUSION

Of course, we should expect organizations to do due diligence and safeguard the digital records holding personal information from attack by malicious intruders. But often organizations are both the unwilling and unwitting victims of a hacker intrusion. Through this study of reported incidents of compromised data, we found that well over a third of the attacks over the last decade have been from malicious hackers, many with criminal intent. Surprisingly, the proportion of incident reports involving a hacker is about the same as the proportion of incidents involving organizational action or inaction. While 42 percent of the incidents involve a hacker, 38 percent of the incidents involve missing or stolen hardware, insider abuse or theft, administrative error and accidentally exposing data online. Just under a fifth of the incidents reports give too little information about the breach to determine the cause—either organizations or individual hackers might be to blame for some of these incidents. Organizations probably can be blamed for the management practices that result in administrative errors, lost backup tapes, and openly exposed data online. Even though an organization can be the victim of theft by its employees, we might still expect organizations to develop suitable safeguards to ensure the safety of client, customer, or member data.

Legislators at the federal and state level have adopted two main strategies to address the problem of electronic record management. On one hand, they have directly targeted those individuals (computer hackers) whose actions potentially threaten the security of private electronic data. The CFAA has been repeatedly strengthened in response to a perception that electronic data theft represents a material and growing concern. The fact that punishments for digital trespass now surpass those for many other more violent forms of crime such as assault and rape suggest that federal legislators consider computer crime to constitute a serious threat to security in this country. However, our data suggest

that malicious intrusion makes up only a portion of all reported cases, and that other factors, including poor management practices by institutions themselves, also contribute to the problem.

The second strategy employed by regulators might be thought of as an indirect or "disciplinary" strategy. Notification of Breach legislation obliges institutions that manage electronic data to report any loss of that data to the individuals concerned. While this directly addresses the problem of consumer protection by empowering individuals to protect themselves in case of lost or stolen data, it has likely been intended to produce secondary effects. Companies and institutions, wary of both the negative publicity and the financial costs generated by an incident of data loss, are encouraged to adopt more responsible network administration practices. Similarly, end-users are urged to weigh both the risk of doing business electronically and the costs associated with taking action once they are notified of a potential breach. The practice of using a risk/reward calculus to achieve policy objectives through legislation has been termed governing "in the shadow of the law" by some authors working in the critical legal studies and governmentality literature (Mnookin & Kornhauser, 1979; Rose, 1999).

One potential problem with this strategy is that the risks and rewards will be unequally distributed among various individual, state and corporate actors. While a large corporation might possess the resources and technical skill necessary to encrypt data, secure networks, or hire external auditors, other institutions in the private or public sector may not find the risk of potential record loss worth the expenditure necessary to secure that data. Governing through market discipline is likely to result in a wide spectrum of responses from differentially situated actors.

While the current market-based approach may not be ideal, there are a number of disincentives to adopting more direct legislation to regulate electronic personal records. Some of the less popular alternatives include setting stricter standards for information management, levying fines against institutions that

violate information security standards, or mandating the encryption of all computerized personal data. However, the introduction of legislation to directly regulate institutions that handle electronic information would certainly be controversial. A wide variety of agencies, companies, and organizations manage personal records on a daily basis. This complexity would hinder the imposition of standardized practices such as encryption protocols. Corporations would likely balk at the prospect of having to pay fines or introduce expensive security measures, and accuse the government of heavy-handed interference. Others might argue that the imperatives of free-market capitalism demand that the government refrain from adopting punitive legislation, in order to maximize the competitiveness of American business. The scale and scope of electronic record loss over the past decade would suggest, however, that the state has a more direct role to play in protecting personal information. Electronically-stored data might very well be weightless, but it is a weight that may be too heavy for private interests and consumers alone to bear.

V. REFERENCES

United States v. Kevin Mitnick, 145 F.3d 1342 (9th Cir. 1998) *available at* 1998 WL255343.

Burchell, Graham (1996). "Liberal Government and Techniques of the Self." *Foucault and Political Reason: Liberalism. Neoliberalism, and Rationalities of Government*.

Barry, Osbourne & Rose (eds.) Chicago: University of Chicago Press.

Cavazos, EA, Morin, D (1996). A new legal paradigm from cyberspace? The effect of the information age on the law. *Technology in Society*, vol. 18, no. 3, pp. 357-371.

Critcher, Chas (2003). *Moral Panics and the Media*. Buckingham & Philidelphia: Open University Press.

Dean, Mitchell (1999). *Governmentality: power and rule in modern society*. London; Thousand Oaks, CA: Sage Publications.

Foucault, Michel (1978). Governmentality. In Burchell, Gordon, and Miller, eds. *The Foucault effect: studies in governmentality*. Chicago: University of Chicago Press.

Hall, Stuart et. al (1978). *Policing the Crisis: Mugging, the State, and Law and Order*. New York: Holmes & Meier.

Jordan, Tim and Taylor, Paul (1998). A Sociology of Hackers. *The Sociological Review.*

Larner, Wendy (2000). Neo-liberalism: Policy, Ideology, Governmentality. Studies in Political Economy 63, 5-25.

Lessig, Lawrence (1999). Code and other laws of cyberspace**.** Selected chapters. New York: Basic Books. Selected Chapters.

Mitchell, Katharyne (2004). *Crossing the neoliberal line: Pacific rim migration and the metropolis*. Philadelphia: Temple University Press.

Mnookin, Robert & Kornhauser, Lewis (1979). Bargaining in the Shadow of the Law. Yale Law Journal, 88, 950-968.

Peck, Jamie (2004). Geography and public policy: constructions of neoliberalism. *Progress in Human Geography*, *28(3),* 392-405.

Peck, Jamie & Tickell, Adam (2002). Neoliberalizing Space. *Antipode*

Rose, Nikolas (1999). *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.

Skibell, Reid (2003). Cybercrimes & Misdemeanors: a Reevaluation of the Computer Fraud and Abuse Act. *Berkeley Technology Law Journal*, 18.

Thomas, Douglas (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.

Wilson, Mark (2003). "Chips bits and the Law: an economic geography of Internet gambling" *Environment and Planning A* 35, pp. 1245-1260.

Zook, M. (2003). "Underground globalization: mapping the space of flows of the internet adult industry" *Environment and Planning A* 35, pp. 1261-1286.

VI. ENDNOTES

[1] For their advice on early drafts of this project the authors are grateful to Dr. Katherine Mitchell, and members the local Seattle hacker community. Please direct correspondence to Kris Erickson, University of Washington Geography Department, Box 353550**,** Seattle, WA, 98195 or by email at kriseric@u.washington.edu.

[2] For their advice on early drafts of this project the authors are grateful to Dr. Katherine Mitchell, and members the local Seattle hacker community. Please direct correspondence to Kris Erickson, University of Washington Geography Department, Box 353550**,** Seattle, WA, 98195 or by email at kriseric@u.washington.edu.

[3] In practice, the monetary felony threshold has proved somewhat meaningless, since the value of computer code compromised during intrusion is often quoted well in excess of $5000. In the case of *United States v Mitnick* (9th. Cir. 1998), Sun Microsystems claimed $80 million in damages related to the cost of research and development of the source code that Mitnick copied during his intrusion.

[4] Many of the cases of theft that we identified were reportedly carried out by individuals working outside of the United States. For example, the 2001 theft of customer account information from Bloomberg Financial was carried out by a Kazak citizen named Oleg Zezov, who threatened to expose the information unless the company paid him $250,000.

[5] Although we were searching for incidents reported in U.S. newspapers, involving U.S. organizations and U.S. adults, our search also revealed 4 million records compromised overseas. These were included.

[6] We believe it is more likely that computer equipment is stolen for personal use or resale value, rather than for the data that thieves might suspect is on the hard drives of the equipment they steal.