



A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records, 1980-2006

Journal:	<i>Journal of Computer-Mediated Communication</i>
Manuscript ID:	draft
Manuscript Type:	Full-length Research Article
Keywords:	Hackers, Privacy, Data Repositories, News, Content Analysis



Review

V. FIGURES AND TABLES

Figure 1: Hacker and Organizational Culpability in Reported Incidents of Compromised Records, 1980-2006

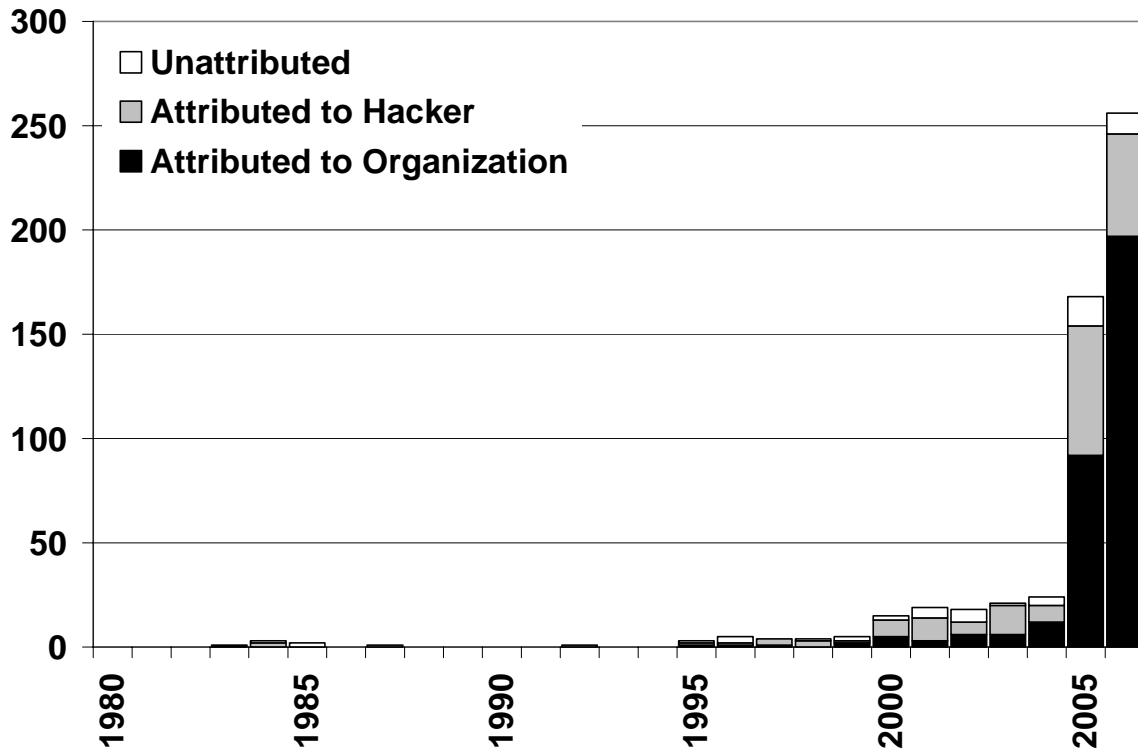


Table 1: Reported Incidents and Volume of Compromised Records by Sector, 1980-2006

	1980-1989				1990-1999				2000-2006				Total			
	Records		Incidents		Records		Incidents		Records		Incidents		Records		Incidents	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Commercial	90,000,002	96	3	43	53,369,339	100	16	73	1,708,156,069	96	190	36	1,851,525,740	96	209	38
Educational	0	0	0	0	0	0	0	0	8,121,234	0	166	32	8,121,234	0	166	30
Government	0	0	1	14	20	0	1	5	63,543,351	4	107	21	63,543,392	3	109	20
Medical	0	0	0	0	3,010	0	2	9	4,640,097	0	51	10	4,643,118	0	53	10
Military	4,190,000	4	3	43	461	0	3	14	90,601	0	7	1	4,281,129	0	13	2
Total	94,190,002	100	7	100	53,372,830	100	22	100	1,784,551,352	100	521	100	1,932,114,613	100	550	100

Note: A zero value in sectors with no incidents indicates that no records were compromised. A zero value in sectors with incidents indicates that the volume of compromised records was not reported.

Table 2: Reported Incidents and Volume of Compromised Records by Type of Breach, 1980-2006

	1980-1989				1990-1999				2000-2006				Total			
	Records		Incidents		Records		Incidents		Records		Incidents		Records		Incidents	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Administrative Error	0	0	0	0	0	0	0	0	33,281,120	2	18	3	33,281,120	2	18	3
Exposed Online	0	0	0	0	3,030	0	3	14	4,605,967	0	81	16	4,609,014	0	84	15
Insider Abuse or Theft	0	0	1	14	20	0	1	5	6,844,162	0	24	5	6,844,203	0	26	5
Missing or Stolen Hardware	0	0	0	0	20,000	0	1	5	44,397,886	2	198	38	44,417,892	2	199	36
Stolen – Hacked	90,000,002	96	3	43	33,430	0	10	45	1,659,391,166	93	159	31	1,749,424,795	91	172	31
Unspecified Breach	4,190,000	4	3	43	53,316,350	100	7	32	36,031,051	2	41	8	93,537,590	5	51	9
Total	94,190,002	100	7	100	53,372,830	100	22	100	1,784,551,352	100	521	100	1,932,114,613	100	550	100

Note: A zero value in a type of breach with no incidents indicates that no records were compromised. A zero value in sectors with incidents indicates that the volume of compromised records was not reported.

RUNNING HEAD: A Case of Mistaken Identity?**A Case of Mistaken Identity?
News Accounts of Hacker, Consumer, and Organizational Responsibility for
Compromised Digital Records, 1980-2006****3/6/2007***Abstract*

The computer hacker is one of the most vilified figures in the digital era, but to what degree are organizations actually responsible for compromised personal records? To examine the role of organizational behavior in privacy violations, we analyze 589 incidents of compromised data between 1980 and 2006. In the United States, some 1.9 billion records have been exposed, either through poor management or hacker intrusions: about nine personal digital records compromised for every adult. There were more reported incidents in 2005 and 2006 than in the previous 25 years combined, and while businesses have long been the primary organizations hemorrhaging personal records, colleges and universities are increasingly implicated. Excluding a particularly large security breach at Acxiom, hackers account for the largest volume of compromised records, some 45 percent, while 27 percent of the volume is attributed to organizational mismanagement and 28 remains unattributed. But in terms of incidents, 9 percent were an unspecified type of breach, 31 percent of the incidents involved hackers, and 60 percent of the incidents involved organizational mismanagement: personally identifiable information accidentally placed online, missing equipment, lost backup tapes, or other administrative errors. Options for public policy oversight are discussed.

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. In early 2005, a series of high-profile cases culminating in the loss of more than 140,000 customer credit records by ChoicePoint helped generate significant public interest in the dangers associated with

1
2
3 digital records of personal information. Then that summer another 40,000 credit card
4 records appeared on the black market for personal data, and in the summer of 2006, the
5 Department of Veteran's Affairs admitted that some 18,000 personal records had been
6 compromised. Data security is never perfect, and credit card companies, universities and
7 government agencies cannot predict security lapses. But the growing number of news
8 stories about compromised personal records reveals a wide range of organizational
9 mismanagement and internal security breaches: lost hard drives and backup tapes,
10 employee theft, and other kinds of administrative errors.
11
12
13
14
15
16
17
18
19
20
21

22 So far, a considerable amount of blame has been directed at all parties involved:
23 at the state, for being lackadaisical in regulating institutions and businesses that deal with
24 electronic records; at the private sector, which is accused of de-prioritizing personal
25 privacy and information security; and finally at the end-users themselves, who are
26 enjoined by a variety of authorities and experts to take better care of managing their
27 online identities in order to mitigate the risk of fraud. A significant amount of the
28 information in these records concerns health and credit records, but such data is often
29 combined so that business, lobbyists, and politicians can generate a convincing electronic
30 portrait of an individual, thus effectively reconstituting their identity (Howard et al.,
31 2005). These stolen identities can also be used to fraudulently deceive government
32 agencies and credit institutions. The threat of electronic data theft also has serious
33 implications for societies that increasingly rely on the security of data networks for day-
34 to-day life. For example, as more of our political system becomes computerized, there is
35 a stronger possibility that electronic data could contain information about an individual's
36 political beliefs or voting records, which are now both easier to access and highly
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3 detailed (Howard, 2002, 2006). Yet most U.S. citizens report being uninterested in
4
5 learning how to better manage their personal data or in learning about the way
6
7 organizations mine for data (Fox, 2000; Milne & Culnan, 2004). Today, however, both
8
9 policy makers and computer software and hardware companies are aggressively in
10
11 enrolling individual consumers in the task of securing their own data against loss or theft.
12
13
14

15
16 At the center of these privacy breaches is often the hacker archetype. Corporate
17
18 and government leaders have reframed the meaning of computer hacking, using
19
20 intellectual property law, court challenges, and amicus briefs, from a character working
21
22 for freedom of access to technology and information to one that is deviant and criminal
23
24 (Nissenbaum, 2004). However, the actual role of hackers in the computer security sector
25
26 is considerably more complex. Many hackers not only enjoy technical challenges, but are
27
28 sometimes even enlisted by corporations and governments for their specific skills
29
30 (Samuelson, 2003; Universal City Studios, 2000). Even though the campaign against
31
32 hackers has successfully cast them as the primary culprits to blame for insecurity in
33
34 cyberspace, it is not clear that constructing this target for blame has improved the security
35
36 of personal digital records.
37
38
39

40
41 As a society, how we assign responsibility will ultimately shape the responses that
42
43 we collectively devise to manage the use of these electronic personal records. This
44
45 article explores how responsibility for protecting electronic data is currently attributed,
46
47 and examines legislation designed to manage the problem of compromised personal
48
49 records. We will then compare the aims of this legislation with an analysis of reported
50
51 incidents of data loss for the period of 1980-2006. A discrepancy between legislative
52
53 responses to electronic data loss and the actual damages incurred reveals that
54
55
56
57
58
59
60

1
2
3 responsibility for maintaining the security of electronic personal records has been
4
5 misplaced and should be re-examined. We conclude with a brief discussion of the
6
7 options for public policy oversight.
8
9

10 11 12 **II. U.S. LEGISLATION TO SECURE ELECTRONIC RECORDS**

13
14
15 Legal scholars often point out that new information technologies consistently present
16
17 legislators with the challenge of regulating issues for which there are no readily apparent
18
19 legal precedents. Lawmakers are frequently cast as lagging behind technological
20
21 innovation, as they struggle to catch up with new forms of behavior enabled by rapidly
22
23 evolving technology. Traditional legal concepts such as private property and trespass
24
25 often become problematic when applied in online contexts enabled by information and
26
27 communication technologies.
28
29
30

31
32 For example, Cavazos and Morin (1996) have argued that in the case of
33
34 defamatory, libelous, and obscene speech, the law has struggled to adequately account for
35
36 the nuances of computer mediated communication. Publishers and re-publishers of
37
38 offline defamatory statements can be held liable, because it is expected that they possess
39
40 considerable editorial control over their own published content. However, when
41
42 publication moves into an online setting, the distribution of liability becomes less clear.
43
44 Not all internet publishers maintain strict editorial control, and some media outlets
45
46 function more like “conduits” through which news is automatically updated. Other
47
48 websites allow users to generate content, with limited moderation provided by the system
49
50 administrator. In both of these cases, it becomes more difficult to assign responsibility
51
52 for defamatory material.
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

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 whether 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 and convicted in Tennessee for violating the obscenity laws in the jurisdiction where the material was accessed, rather than where the material was stored (“United States v. Thomas,” 1996). 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.

41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

These jurisdictional conflicts become even more apparent in cases where lawmakers have attempted to regulate behavior across several legal jurisdictions, such as in the case of 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

1
2
3 offshore in areas with less stringent regulation. The United States has pursued this
4 strategy in regard to online gambling, with limited success. Charges brought by New
5 York State against 22 online gambling websites in 1999 yielded only one arrest, when the
6 operator visited the country on vacation (Wilson, 2003).
7
8
9
10
11

12
13 An additional problem facing legislation aimed at controlling online behavior is
14 its questionable effectiveness as a deterrent. The Computer Fraud and Abuse Act
15 (CFAA) was passed in 1984 in response to growing political and media attention
16 surrounding the dangers of computer crime. The act criminalized unauthorized access to
17 private computer systems, making it a felony offense when trespass leads to damages
18 over a certain monetary threshold. The CFAA underwent major revisions in 1986 and
19 1996, and it was further strengthened by the passage of the USA Patriot Act in 2002.
20 Overall, these revisions have served to make the act more broadly applicable to various
21 kinds of computer crime, while also increasing the punitive response to these offenses.
22
23
24
25
26
27
28
29
30
31
32
33

34 For example, the revisions in 2002 were tailored to make it easier to surpass the
35 \$5,000 felony threshold. The threshold was waived in cases where the computer systems
36 involved are used for national security or law enforcement purposes. In cases not
37 involving national security, the definition of “damage” was broadened to include costs
38 relating to damage assessment and lost revenue during an interruption of service. The
39 \$5,000 threshold is also cumulative over multiple machines if more than one system is
40 involved in an attack.¹ Additionally, the maximum sentence for felony computer trespass
41 was raised from 5 to 10 years for first-time convictions, and from 10 to 20 years for
42 repeat offenders (Skibell, 2003).
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Given the relatively harsh penalties for computer trespass compared with 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 not all computer crime is committed by self-interested or malicious criminals. The belief that all hackers are malicious is essentially a myth—many members of the computer hacker subculture do not condone destructive behavior and do not consider their activities to be particularly malicious. Criminals who make use of hacker techniques to access private data are rarely members of hacker communities, and often less sophisticated in their hacker skill-set (Skibell, 2002). 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. According to Jordan and Taylor, these legitimate computer hackers are motivated by a variety of concerns that make comparisons with other types of criminal behavior problematic (1998).

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).

1
2
3 These scholars argue that hacker projects are shaped by an ethical framework formed by
4 a strong sense of imagined community. Many hackers are interested in the intellectual
5 challenge and sense of mastery provided by computer networks, rather than monetary
6 rewards that could be gained from accessing sensitive information. They seek to
7 differentiate themselves from other computer criminals who use computer networks for
8 destructive, rather than creative processes.
9

10
11
12
13
14
15
16
17
18 Furthermore, in recent years the core hacker community has been somewhat
19 successful at contesting the malicious meaning attached to the term “hacker.” While the
20 press often continues to report hackers as those responsible for most forms of computer
21 crime, more legitimate hackers have worked hard to distance themselves from the
22 sensationalist definition used by the news media. Many of them divide their community
23 into “white hat” and “black hat” constituencies to help distinguish between those who use
24 their computer skills with malicious intent from those who do not. The term “cracker,”
25 which now denotes individuals who destroy rather than improve computer systems,
26 indicates a deliberate rhetorical strategy on the part of some hackers to bring nuanced
27 understanding of the different aspects of the computer hacking, particularly among
28 scholars interested in computer subcultures (Jordan & Taylor, 2004; Thomas, 2002). In
29 contrast, “gray hats” are those who publicly expose security flaws, without concern for
30 whether the act of exposure allows administrators to patch the flaw or allows others to
31 exploit the flaw. Moreover, mainstream computer security experts have co-opted the term
32 “blue hat” to further distinguish the community of skilled computer users who hack in the
33 service, and often employment, of Microsoft.
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Arguably, the most significant threat posed by computer criminals comes not from the core group of white, blue or grey hat 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.² These individuals may feel protected from the law due to the relative anonymity of computer-mediated communication 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

1
2
3 with any required security code, access code, or password that would permit
4
5 access to an individual's financial account.
6
7
8
9

10 The company or institution responsible for handling the compromised data must notify
11 potential victims individually, unless the cost of notification exceeds a threshold amount
12 of \$250,000, or if the total number of individuals affected is greater than 500,000. In
13 these cases, substitute notification can be made using a combination of e-mail notification
14 and disclosure to major media outlets. Notification must be carried out "in the most
15 expedient time possible and without unreasonable delay, consistent with the legitimate
16 needs of law enforcement [...] or any measures necessary to determine the scope of the
17 breach and restore the reasonable integrity of the data system" (California Civil Code
18 1798.29). Following California's footsteps, 22 additional states have enacted similar
19 legislation as of 2005. For the most part, individual state legislatures have maintained the
20 spirit of the California provision, including the extension of liability to both businesses
21 and agencies, as well as the notification threshold.
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38

39 The aim of the "notification of breach" legislation is significantly different from
40 that of the CFAA. By making corporations and institutions liable for damages potentially
41 incurred by customers and clients, this legislation to some extent seeks to discipline
42 offenders who engage in poor record-keeping practices. Both the indirect threat of future
43 litigation and the potential for public embarrassment are intended to improve data
44 security in both the public and private sector. Unlike the CFAA, however, this legislation
45 does not directly address the issue of network security. It does not formalize standards or
46 rules for information security, nor does it make businesses and institutions accountable
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3 for poor security practices that may make them vulnerable to attack. The legislation
4 punishes businesses only for failing to notify the public, rather than for negligence in
5 securing electronic records. Since adequately securing a computer network from
6 intrusion is an expensive prospect, this legislation essentially lets businesses off the hook,
7 by making them liable for damages only when they fail to notify affected individuals that
8 their data have been compromised. Interestingly, by failing to assign responsibility for
9 data loss to those agencies that manage electronic personal information, this legislation
10 serves in part to shift that responsibility to the individual user, since it is he or she who
11 must take steps to protect their identity once notified of a breach.
12
13
14
15
16
17
18
19
20
21
22
23

24 This sentiment is supported by the California Department of Consumer Affairs,
25 which maintains a website devoted to online privacy protection. The agency has also
26 distributed a flyer listing the “top 10 tips for identity theft prevention.” This list enjoins
27 consumers to take active steps to avoid becoming the victims of electronic fraud, by
28 shredding personal documents, installing up-to-date computer virus and firewall
29 software, and becoming vigilant about which sites they visit and how they use their credit
30 cards. Consumers are also urged to take a more proactive role in monitoring their
31 personal credit rating, in order to detect potential fraud. The Department of Consumer
32 Affairs recommends that individuals apply for free credit reports at least 3 times per year
33 in order to prevent misuse of their electronic identity.
34
35
36
37
38
39
40
41
42
43
44
45
46
47

48 So far, the legal responses to electronic identity theft in the United States have
49 sought to minimize the direct involvement by the state, instead relying on a partnership
50 between the interests of private institutions and the consumers of those services. The two
51 major forms of legislation governing the security of computer records in the United
52
53
54
55
56
57
58
59
60

1
2
3 States – the CFAA and the California Notification of Breach laws – closely resemble
4
5 offline governmental strategies that seek to place responsibility on individual consumer-
6
7 citizens while disciplining those who do not adequately protect themselves (Burchell,
8
9 1996; Peck & Tickell, 2002). Moreover, the reticence of public agencies in the United
10
11 States to draft legislation that would directly influence the terrain of data security is
12
13 consistent with the overall trend of regulatory devolution, a shift that began before the
14
15 information sector occupied such a primary position in the national economy.
16
17
18
19

20
21 The legislative choices that policymakers in the United States have made to
22
23 combat the problem of data insecurity have been shaped by the tenet that governments
24
25 should interfere only minimally with markets. Thus, legislative initiatives have eroded
26
27 public policy oversight of corporate behavior. In the arena of data security for private
28
29 information, this erosion has meant de-emphasizing the role of government and public
30
31 policy oversight in data security, encouraging industry self-regulation among the firms
32
33 benefiting in the retention of personal data, and increasing individual responsibility for
34
35 managing our personal data.
36
37
38
39
40

41 **III. ANALYSIS OF COMPROMISED ELECTRONIC RECORDS, 1980-2006**

42
43 We conducted a search of incidents of electronic data loss reported in major U.S. news
44
45 media from 1980 to 2006. These included print publications with national circulation
46
47 such as the *New York Times*, the *L.A. Times*, and *USA Today*, along with major broadcast
48
49 news media. Because some news reports contained references to more than one incident,
50
51 we employed a snowball methodology to expand our analysis by including additional
52
53 security breaches mentioned in the same article. Duplicate entries were eliminated by
54
55
56
57
58
59
60

1
2
3 comparing news stories on the basis of organizations involved, dates, and other incident
4 details. In cases where papers reported different quantities of lost records, we chose the
5 most conservative report. We also consulted lists of electronic data breaches compiled by
6 third party computer security advisories, such as the Identity Theft Resource Center
7 (www.idtheftcenter.org) and Attrition.org. Our method yielded 589 incidents, 550 of
8 which were successfully cross-checked with LexisNexis and Proquest to ensure accuracy,
9 and 39 of which we discarded for involving citizens of other countries or for being
10 unverifiable in major news media reports.³
11
12
13
14
15
16
17
18
19
20
21

22 There are interesting advantages and disadvantages to using printed news sources
23 to construct the history of computer hacking and breached private records. As stated
24 above, the mainstream media often equate hackers with any crime involving a computer
25 and use the misnomer “hacker” without a nuanced understanding of the history of more
26 legitimate computer hacking. We continue to use the term in this analysis because it is
27 the most commonly used term in media reports where an intruder was deemed
28 responsible for compromised data. While criminal records would certainly provide details
29 about the prevalence of malicious intrusions, such records are extremely difficult to
30 collect nation-wide. Moreover, a survey of incidents composed through criminal records
31 would significantly *over-sample* incidents where an individual hacker was at fault, and
32 significantly *under-sample* incidents where an organization was culpable but not deemed
33 criminally negligent. Over the decade, journalists would not have discovered all
34 incidents, and even though current California law requires that a person whose data had
35 been compromised be so informed, such a breach is not necessarily noted in news
36 archives. However, journalists do their best to report the facts, and in the absence of a
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3 public agency that might maintain comprehensive incident records on privacy violations,
4
5 news accounts provide a good accessible resource.
6
7

8 Our list of reported incidents is limited to cases where one or more electronic
9
10 personal records were compromised through negligence or theft. We acknowledge that
11
12 there may be occasions where end-users consider their personal information
13
14 compromised when the data are sold among third parties for marketing purposes without
15
16 their informed consent. For this study, we look only at incidents of compromised records
17
18 that are almost certainly illegal or negligent acts. For the purposes of this paper, we
19
20 define electronic personal records as data containing privileged information about an
21
22 individual that cannot be readily obtained through other public means. Rather than
23
24 become involved in the broader debate about the virtues and dangers of online
25
26 anonymity, we have chosen to focus only on data that are more sensitive than the
27
28 information that we regularly volunteer in the course of surfing the web (such as one's
29
30 name or IP address). We define "personal data" to be information that should reasonably
31
32 be known only to the individual concerned or be held by an organization under the terms
33
34 of a confidentiality agreement (such as between a patient and a care provider). Electronic
35
36 personal records therefore could include individuals' personal credit histories, banking
37
38 information such as credit card numbers or account numbers, medical records, social
39
40 security numbers, and grades earned at school. We focused only on incidents where
41
42 compromised personal records were kept for a legitimate purpose by a company,
43
44 institution, or government agency. Consequently, "phishing" or spoofing scams where
45
46 victims are deceived into volunteering their own personal information are not included in
47
48 our analysis. All of the incidents in our analysis deal with data that were maintained in
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3 electronic form, although in some cases compromised data were contained on a lost or
4
5
6 stolen laptop computer.
7

8 Between 1980 and 2006, some 1.9 billion records were reported compromised by
9
10 government agencies, firms, hospitals, universities and the military. This is the sum of
11
12 compromised records from 529 cases in which some estimate of the volume of lost
13
14 records was offered, though in 60 of these incidents the impact of the security breach was
15
16 unknown. In a sense, this number of lost records is larger than we might expect because
17
18 a few landmark incidents account for large portions of the total number of records
19
20 compromised. On the other hand, the number of confirmed incidents—550 in all—may
21
22 seem smaller than expected given the 26-year time frame of our search. Some articles
23
24 report multiple incidents, and of course many incidents were covered by journalists on
25
26 multiple occasions. In 2004, the Census Bureau estimated that there were 217 million
27
28 adults living in the United States. We can conservatively estimate that for every U.S.
29
30 adult, in the aggregate, nine private records have been compromised. Unfortunately we
31
32 cannot know how many of these compromised private records have actually been used
33
34 for identity theft, or how many were sold to marketing companies.
35
36
37
38
39
40
41
42
43

44 TABLE 1 ABOUT HERE: Reported Incidents and Volume of Compromised Records by
45
46 Sector, 1980-2006
47
48
49

50 Table 1 reveals the number of reported incidents and volume of compromised
51
52 records between 1980 and 2006, along with their distribution by sector. The majority of
53
54 incidents involved commercial actors, less than a third of the incidents involved colleges
55
56
57
58
59
60

1
2
3 and universities, and the remainder involved government, hospitals, and the military.
4
5
6 When the exceptional loss of 1.6 billion personal records by Acxiom Corporation is
7
8 removed, the commercial sector still accounted for approximately 252 million individual
9
10 compromised records, four times that of the next-highest contributor, the government
11
12 sector.⁴ The education sector accounted for a small percentage of the overall quantity of
13
14 lost records, but accounted for 30 percent of all reported incidents, suggesting that
15
16 educational institutions suffer from a higher rate of computer insecurity than might be
17
18 anticipated. This could be explained by the fact that colleges and universities generally
19
20 maintain large electronic databases on current and past students, staff, faculty, and
21
22 alumni, and have an organizational culture geared towards information sharing.
23
24
25 However, medical institutions—which presumably also maintain large quantities of
26
27 electronic data—reported a significantly lower number of incidents of data loss. These
28
29 differences may be the result of strong privacy legislation in the arena of medical
30
31 information, but comparatively weak privacy legislation in the arena of educational and
32
33 commercial information.
34
35
36
37

38
39 Although the Table 1 has aggregated twenty six year's worth of incidents, the
40
41 bulk of the reports occur in 2005 and 2006, after legislation in California, Washington,
42
43 and other states took effect. There were three times as many incidents in the period
44
45 between 2005 and 2006 as there were in the previous 25 years. Interestingly, the
46
47 mandatory reporting legislation seems to have exposed educational institutions as a major
48
49 source of leakage of private data. In total, 38 percent of the incidents involved
50
51 commercial firms, but specifically in 2005 and 2006, 35 percent of the incidents involved
52
53
54
55
56
57
58
59
60

1
2
3 educational institutions. These kinds of organizations may have been the least equipped
4
5
6 to protect the data of their students, staff, faculty and alumni.
7

8 For the majority of incidents, the news article reports some information about
9
10 how the records were compromised. A closer reading of each of the incidents, however,
11
12 reveals that most incidents involve different combinations of mismanagement, criminal
13
14 intent, and, occasionally, bad luck. The hacker label is often used, even when the theft is
15
16 perpetrated by an insider, such as a student or employee. Moreover, company public
17
18 relations experts often posit that personal records were only “exposed,” not
19
20 compromised, when employees post private records to a website or loose a laptop and the
21
22 company cannot be sure that anyone has taken specific advantage of the security breach.
23
24
25
26
27
28

29 TABLE 2 ABOUT HERE: Reported Incidents and Volume of Compromised Records by
30 Type of Breach, 1980-2006
31
32
33
34

35 Table 2 reveals that the legislation has also seemed to have the effect of forcing
36
37 the reporting organizations to reveal more detail about the ways these private records get
38
39 compromised. In the early reports, most incidents were described as an unspecified
40
41 breach or as the general result of hacker activity. However, for the period between 2000
42
43 and 2006, 31 percent of the incidents were about a breach caused by a hacker, 8 percent
44
45 of the incidents involve an unspecified breach, and 61 percent of the incidents involved
46
47 different kinds of organizational culpability. For example, sometimes management
48
49 accidentally exposed private records online, administrative error resulted in leaked data,
50
51 or employees were caught using the data for activities not related to the work of the
52
53
54
55
56
57
58
59
60

1
2
3 organization. On some occasions, staff simply misplaced backup tapes, while on others,
4
5 computer equipment such as laptops were stolen.⁵
6
7

8 A single incident, involving 1.6 billion compromised records at Axiom, accounts
9
10 for a large portion of the volume of records lost in the period 2000-2006.⁶ If this event is
11
12 removed from this period, then 32 percent of the compromised volume and 30 percent of
13
14 the incidents are related to hackers, 48 percent of the compromised volume and 62
15
16 percent of the incidents involve organizational behavior, and 20 percent of the
17
18 compromised volume and 8 percent of the incidents remain unattributed. If this event is
19
20 removed from the volume of compromised records for the whole study period—between
21
22 1980 and 2006—then 45 percent of the total volume of compromised records related to
23
24 hackers, 27 percent of the volume was attributed to the organization, and 28 percent
25
26 remained unattributed. If this event is removed from the total number of incidents for the
27
28 whole study period, then 31 percent of the incidents involved hackers, 60 percent
29
30 involved organizational management, and 9 percent remain unattributed. Regardless of
31
32 how the data is broken down, hackers never account for even half of the incidents or the
33
34 volume of compromised records.
35
36
37
38
39
40
41
42

43
44 **FIGURE 1 ABOUT HERE: Hacker and Organizational Culpability in Reported Incidents**
45
46 **of Compromised Records, 1980-2006**
47
48
49

50
51 If we distinguish the reported incidents that clearly identify a hacker from those
52
53 concerning some other form of breach, the organizational role in these privacy violations
54
55 moves into sharp relief. Figure 1 separates the count of stories in which a hacker was
56
57
58
59
60

1
2
3 clearly identified as the culprit, from those stories where the cause of the breach was
4
5 unspecified, and from those stories where the cause of the breach was related to
6
7 organizational action or inaction. In this later category, we consider organizational
8
9 behavior to include four types of security breach: accidental exposure of personal
10
11 records online, insider abuse or theft, missing or stolen hardware, or other administrative
12
13 error. First, it is noticeable that as more states require organizations to report
14
15 compromised digital records, the overall volume of annual news stories on the topic
16
17 increases significantly. In fact, there were more reported incidents in 2005 and 2006 than
18
19 in the previous 25 years combined. We found 126 incidents of compromised records
20
21 between 1980 and 2004, and 424 incidents between 2005 and 2006. Just summing the
22
23 incidents from 2005 and 2006, when mandatory reporting legislation was in place in
24
25 many states, we find that 68 percent of the stories concern data that were accidentally
26
27 placed online or exposed through administrative errors, stolen equipment, or other
28
29 security breaches such as employee loss of equipment or backup tapes.
30
31
32
33
34
35

36
37 Several factors might explain the pattern of increasing incidents and volume of
38
39 compromised data over time. First, there is the possibility that the results are skewed due
40
41 to the relative growth of new, fresh news stories devoted to this issue, and the loss of
42
43 older stories that disappeared from news archives as time passed. Perhaps there have
44
45 always been hundreds of incidents every year, but only in recent years has the severity of
46
47 the problem been reported in the news. If this were the case, we would expect to see a
48
49 gradually decaying pattern with greater number of reported cases in 2006 than in 2005,
50
51 2004, and so on. However, the dramatic difference in reported incidents between later
52
53 years and early years suggests that this effect does not adequately explain our
54
55
56
57
58
59
60

1
2
3 observations. A second possibility is that increased media attention or sensational
4 reporting in 2005 and 2006 lead to a relative over-reporting of incidents, compared with
5 previous years. Literature on media responses to perceived crises or “moral panics”
6 would suggest that a similar effect commonly accompanies issues that are granted a
7 disproportionate amount of public attention, such as with the case of the mugging scare in
8 Great Britain in the 1970s or the crackdown on the rave subculture in the 1990s (Cricher,
9 2003; Hall et al., 1978). While it is unlikely that media outlets have exaggerated the
10 amount of electronic personal record loss, it is possible that in previous years a certain
11 number of events went unreported in the media due to lack of awareness or interest in the
12 issue of identity theft. A third possibility is that there were a greater number of reported
13 incidents of data loss in 2005 and 2006, because institutions are maintaining and losing a
14 larger quantity of electronic data, and because a changing legislative environment in
15 many states is obliging institutions to report events publicly that may have gone
16 unreported in previous years. The fourth possibility, and the most plausible one, is that
17 mandatory reporting legislation has exposed both the severity of the problem and the
18 common circumstances of organizational mismanagement.
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40

41 It is likely that a combination of factors explain our observations. The
42 Notification of Breach legislation that requires the prompt reporting of lost records in
43 California came into effect in 2003; however, the legislation was not widely adopted and
44 implemented by other states until 2005, which might help to explain the dramatic
45 increase in reported cases. The Notification of Breach legislation in California, as many
46 other states, requires notification when a state resident has been a victim of data loss,
47 regardless of where the offending institution resides. Therefore, institutions located in
48
49
50
51
52
53
54
55
56
57
58
59
60

1
2
3 states without Notification of Breach laws, such as Oregon, are still required to report
4 cases to victims who live in states that have enacted this type of legislation, such as New
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

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 many 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.

IV. CONCLUSION

Surveying news reports of incidents of compromised personal records helps us to understand the diverse situations in which electronic personal records are stolen, lost, or mismanaged. More important, it allows us to separate incidents in which personal records have been compromised by outside hackers from incidents in which breaches were the result of an organizational lapse. Of course, we should expect organizations to perform 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 malicious hacker. Through this study of reported incidents of compromised data, we found that two-fifths of the incidents over the last quarter century involve malicious hackers with criminal intent. Surprisingly, however, the proportion of incident reports involving hackers is smaller than the proportion of incidents involving organizational action or inaction. While 31 percent of the incidents reported clearly identify a hacker as the culprit, 60 percent of the incidents involve missing or stolen hardware, insider abuse or theft, administrative error, or accidentally exposing data online. The remainder of news stories record too little information about the breach to

1
2
3 determine the cause—either organizations or individual hackers might be to blame for
4
5
6 some of these incidents.

7
8 Organizations probably can be blamed for the management practices that result in
9
10 administrative errors, lost backup tapes, or data exposed online. And even though an
11
12 organization can be the victim of theft by its employees, we might still expect
13
14 organizations to develop suitable safeguards to ensure the safety of client, customer, or
15
16 member data. Even using the news media's expansive definition of hacker as a basis for
17
18 coding stories, we find that a large portion of the security breaches in the United States
19
20 are due to various forms of organizational malfeasance.
21
22
23

24
25 One important outcome of the legislation is improved information about the types
26
27 of security breaches. Many of the news stories between 1980 and 2004 report paltry
28
29 details, with sources being off the record and vague estimates of the severity of the
30
31 security breach. Since mandatory reporting legislation in many states, most news
32
33 coverage provides more substantive details. In 2006, only 10 of the 257 news stories
34
35 were unable to make some attribution of responsibility for a security breach.
36
37
38

39
40 Legislators at the federal and state level have adopted two main strategies to
41
42 address the problem of electronic record management. On one hand, they have directly
43
44 targeted those individuals (computer hackers) whose actions potentially threaten the
45
46 security of private electronic data. The CFAA has been repeatedly strengthened in
47
48 response to a perception that electronic data theft represents a material and growing
49
50 concern. The fact that punishments for digital trespass now surpass those for many other
51
52 more violent forms of crime suggests that federal legislators consider computer crime to
53
54 constitute a serious threat to our personal and collective security. However, our data
55
56
57
58
59
60

1
2
3 suggest that malicious intrusion by hackers makes up only a portion of all reported cases,
4
5 while other factors, including poor management practices by organization themselves,
6
7 contribute more to the problem.
8
9

10 The second strategy employed by regulators might be thought of as an indirect or
11
12 “disciplinary” strategy. Notification of Breach legislation obliges institutions that
13
14 manage electronic data to report any loss of that data to the individuals concerned. While
15
16 this directly addresses the problem of consumer protection by empowering individuals to
17
18 protect themselves in case of lost or stolen data, it has probably been intended to produce
19
20 secondary effects. Companies and institutions, wary of both the negative publicity and
21
22 the financial costs generated by an incident of data loss, are encouraged to adopt more
23
24 responsible network administration practices. Similarly, end-users are urged to weigh
25
26 both the risk of doing business electronically and the costs associated with taking action
27
28 once they are notified of a potential breach. The practice of using a risk/reward calculus
29
30 to achieve policy objectives through legislation has been termed governing “in the
31
32 shadow of the law” by some authors working in the critical legal studies and
33
34 governmentality literature (Mnookin & Kornhauser, 1979; Rose, 1999).
35
36
37
38
39

40 One potential problem with this strategy is that the risks and rewards will be
41
42 unequally distributed among various individual, state, and corporate actors. While a
43
44 large corporation might possess the resources and technical skill necessary to encrypt
45
46 data, secure networks, or hire external auditors, other institutions in the private or public
47
48 sector may not find the risk of potential record loss worth the expenditure necessary to
49
50 secure that data. Governing through this type of market discipline is likely to result in a
51
52 wide spectrum of responses from differentially situated actors.
53
54
55
56
57
58
59
60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

There are a number of alternatives open to lawmakers and policy advisors that could materially strengthen the security of electronic personal records in this country. Alternatives include setting stricter standards for information management, levying fines against institutions that violate information security standards, and 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 probably 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, especially in order to maximize competitiveness. Identity theft can have a significant impact on individuals whose identity is stolen, and can taint the reputation of the organization that was compromised. But in the incidents studied here, the security breach is often with commercial firms, and increasingly educational institutions, rather than individuals.

Although computer hacking has been widely reframed as a criminal activity and has received increasingly harsh punishments, the legal response has obfuscated the responsibility of commercial, educational, government, medical and military organizations for data security. The scale and scope of electronic record loss over the past decade would suggest that organizational self-regulation or self-monitoring is failing to keep our personal records secure and that the state has a more direct role to play in

1
2
3 protecting personal information. State-level initiatives have helped expose the problem
4
5 by making it possible to collect better data on the types of security breaches that are
6
7 occurring, and to make some judgments about who is responsible for the breaches. If
8
9 public policy can be used to create incentives for organizations to better manage
10
11 personally identifiable information and punish organizations for mismanagement, such
12
13 initiative would probably have to come at the state level. Electronically stored data might
14
15 very well be weightless, but the organizations that retain personally identifiable
16
17 information must shoulder more of the heavy burden for keeping such data secure.
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

VI. REFERENCES

- Burchell, G. (1996). Liberal Government and Techniques of the Self. In Barry, Osbourne & Rose (Eds.), *Foucault and Political Reason: Liberalism, Neoliberalism, and Rationalities of Government*. Chicago: University of Chicago Press.
- Cavazos, E. A., & Morin, D. (1996). A New Legal Paradigm from Cyberspace? The Effect of the Information Age on the Law. *Technology in Society*, 18(3), 357-371.
- Critcher, C. (2003). *Moral Panics and the Media*. Buckingham, UK Open University Press.
- Dean, M. (1999). *Governmentality: Power and Rule in Modern Society*. London: Sage
- Foucault, M. (1991). Governmentality. In *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press.
- Fox, S. (2000). *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*. Washington, DC: Pew Internet and American Life Project.
- Hall, S., Critcher, C., Jefferson, T., Clarke, J., & Robert, B. (1978). *Policing the Crisis: Mugging, the State, and Law and Order*. New York: Palgrave Macmillan.
- Howard, P. N. (2002). Network Ethnography and the Hypermedia Organization: New Media, New Organizations, New Methods. *New Media & Society*, 4(4), 550-574.
- Howard, P. N. (2006). *New Media Campaigns and the Managed Citizen*. New York: Cambridge University Press.
- Howard, P. N., Carr, J., & Milstein, T. J. (2005). Digital Technology and the Market for Political Surveillance. *Surveillance and Society*, 3(1).
- Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. *The Sociological Review*, 46(4), 757-781.
- Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* New York: Routledge.
- Milne, G. R., & Culnan, M. J. (2004). Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing*, 18(3), 15-29.
- Mnookin, R., & Kornhauser, L. (1979). Bargaining in the Shadow of the Law. *Yale Law Journal*, 88, 950-968.
- Nissenbaum, H. (2004). Hackers and the Contested Ontology of Cyberspace. *New Media & Society*, 6(2), 195-217.
- Peck, J., & Tickell, A. (2002). Neoliberalizing Space. *Anitpode*, 34(3), 380-404.
- Rose, N. (1999). *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.
- Samuelson, P. (2003). Digital Rights Management (and, or, vs.) the Law. *Communications of the ACM*, 46(4), 41-45.
- Skibell, R. (2002). The Myth of the Computer Hacker. *Information, Communication and Society*, 5(3), 336-356.
- Skibell, R. (2003). Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act. *Berkeley Technology Law Journal*, 18(3), 909-944.
- Thomas, D. (2002). *Hacker Culture*. Minneapolis: University of Minnesota Press.
- United States v. Kevin Mitnick, 145 F.3d 1342 (9th Circuit 1998).

1
2
3 United States v. Thomas, 74 F. 3d 701 (6th Circuit 1996).
4 Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294 320 (Federal Superior
5 Court 2000).
6
7 Wilson, M. (2003). Chips, Bits and the Law: An Economic Geography of Internet
8 Gambling. *Environment and Planning A*, 35(7), 1245-1260.
9
10 Zook, M. (2003). Underground Globalization: Mapping the Space of Flows of the
11 Internet Adult Industry. *Environment and Planning A*, 35(7), 1261-1286.
12
13
14
15
16

17 VI. ENDNOTES

18
19
20 ¹ In practice, the monetary felony threshold has proved somewhat meaningless, since the value of computer
21 code compromised during intrusion is often quoted well in excess of \$5000. In the case of *United States v*
22 *Mitnick* (9th Cir. 1998), Sun Microsystems claimed \$80 million in damages related to the cost of research
23 and development of the source code that Mitnick copied during his intrusion. ("United States v. Kevin
24 Mitnick," 1998)

25 ² In our survey, some incidents involving U.S.-based organizations or U.S. citizens were reportedly carried
26 out by individuals working outside the United States. For example, the 2001 theft of customer account
27 information from Bloomberg Financial was carried out by a Kazak citizen named Oleg Zevov, who
28 threatened to expose the information unless the company paid him \$250,000.

29 ³ We retained incidents that had been reported in multiple sources, even if no exact number of
30 compromised records was reported. To be conservative, we recorded these incidents as having 0
31 compromised records. In news stories where it was only reported that "hundreds" or "thousands" of
32 personal records were compromised, we recorded 100 or 1,000 compromised records.

33 ⁴ The records lost by Axiom Corporation consisted of credit card numbers, purchasing histories, and
34 marital status of individuals.

35 ⁵ We believe it is more likely that computer equipment is stolen for personal use or resale value, rather than
36 for the data that thieves might suspect is on the hard drives of the equipment they steal.

37 ⁶ This single case is illustrative of the challenge of compiling and comparing incidents of compromised
38 personal records. For example, the Axiom incident involved an employee of Snipermail.com, who
39 removed 8.2 gigabytes of personal data in 137 separate incidents between April 2002 and August 2003. To
40 be consistent with our sampling, we record this as a single incident occurring in 2004 because the news
41 coverage and his arrest did not occur until 2004. Axiom, the company that was entrusted with personal
42 records, and even justice officials commenting on the case, describe the culprit as a hacker. However, there
43 was actually a client relationship between the two firms, and Snipermail.com staff legitimately had the
44 correct password to upload data to Axiom servers. Someone at the Snipermail.com firm guessed that the
45 same password might also be used to download data, though they were not legitimately allowed to do so.
46 Some might argue that this is an example of a poor security choice of Axiom's, not an example of an
47 ingenious technical exploitation by a rogue outsider with a hacker's skills. However, the majority of cases
48 we label as "insider abuse" involve employees. The culprit in this case did legitimately have some insider
49 information about Axiom's security. To be conservative, and since we are interested in how the news
50 media frames issues of data security, we label this incident thus: we code it as involving data stolen by a
51 hacker because that was the language used in news coverage; we do not code it as insider abuse because the
52 culprit was not an employee.
53
54
55

56 VII. ABOUT THE AUTHORS

57
58
59
60

1
2
3
4
5 Kris Erickson is a doctoral candidate in Geography at the University of Washington,
6 where he studies the role of computer subcultures in the regulation of cyberspace. His
7 dissertation research on the hacker community explores the rise of the computer security
8 profession and its implications for global Internet governance. Address: Department of
9 Geography, 408 Smith Hall, Box 353550, University of Washington, Seattle,
10 Washington, 98195.
11

12
13 Philip N. Howard is an assistant professor in the Communication Department at the
14 University of Washington. His book *New Media Campaigns and the Managed Citizen*
15 (New York: Cambridge University Press, 2006) is about the role of information
16 technology in campaign strategy and political culture. He has published a co-edited
17 collection with Steve Jones entitled *Society Online: The Internet In Context* (Thousand
18 Oaks, CA: Sage, 2003). Currently, he directs the World Information Access Project
19 (www.wiareport.org). Address: Department of Communication, 141 Communications
20 Building, Box 353740, University of Washington, Seattle, Washington, 98195.
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60