The John Marshall Journal of Information Technology & Privacy Law

Volume 24
Issue 1 *Journal of Computer & Information Law - Fall 2005*
Article 3

Fall 2005

Do We Really Have No Place to Hide?, 24 J. Marshall J. Computer & Info. L. 57 (2005)

Matthew Hector

BOOK REVIEW

DO WE REALLY HAVE *NO PLACE TO HIDE?*

MATTHEW HECTOR†

"On the Internet, nobody knows you're a dog."

— The New Yorker[1]

Since the dawn of the Information Age, pundits and observers have often commented on how new technology may impact privacy. Some thought that the Internet provided increased anonymity, as the famous New Yorker cartoon quoted above indicates. Since 1993, however, observers have become increasingly aware that privacy is not as protected as they originally thought. They have provided scenarios that range from Orwellian nightmares to streamlined open societies. These visions have yet to come to fruition; however, what many of these observers have not mentioned is that private corporations have been collecting and compiling data about Americans for years in an attempt to learn more about consumers. While most of this took place outside the public eye, Robert O'Harrow, Jr., a writer for the Washington Post, has provided a sometimes frightening glimpse into the world of private data aggregators and their ties to State and Federal law enforcement in the September 12th world. His book, *No Place To Hide*,[2] sheds light on the previously shadowed world of those who know the most about Americans.

---

† Matthew Hector is a solo transactional attorney licensed in Illinois. He received his Bachelor of Arts from The University of Alabama, his Juris Doctor from The John Marshall Law School and is currently completing his LL.M. in Information Technology & Privacy Law at The John Marshall Law School. Mr. Hector would like to thank Robert O'Harrow, Jr. and Professor Leslie Reis for their assistance with this article.*See* Peter Steiner, Cartoon, *On the Internet, Nobody Knows You're a Dog,* 69 New Yorker 61, (July 5, 1993)(available at http://www.epatric.com/funstuff/dog/).

1. *See* Peter Steiner, Cartoon, *On the Internet, Nobody Knows You're a Dog,* 69The New Yorker, Vol. 69 No. 6120, (July 5, 1993)(available at http://www.epatric.com/funstuff/dog/).

2. Robert O'Harrow, Jr., *No Place To Hide* (Free Press 2005).

O'Harrow points out time and again the amount of data being stored, the speed with which private data aggregators like ChoicePoint and Acxiom can process that data, and the frighteningly detailed profiles they produce. His book also examines the ties between the private data aggregators and government investigators. In some anecdotes, these ties are highly effective in capturing criminals;, in others, they are the stuff of nightmares for those who feel the government should not pry into their lives. While the book attempts to show the positive and negative aspects of data aggregation, O'Harrow tends to give short shrift to the position of both private data aggregators and government law enforcement. This bias overshadows the central message of *No Place To Hide*: personal privacy is more limited than the average person thinks.

It is also worth noting that simply by informing people about the possible threats to their privacy, O'Harrow has taken a step towards what he considers an ultimate goal of informational privacy policy: allowing Americans to "make adult, refined decisions about how you are going to share your information."[3] *No Place To Hide* does a great job of establishing the state of informational privacy in the 21st Century. Setting the tone for the rest of the book, the introduction ends with an apt quote from President Dwight Eisenhower:

"In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military industrial complex. The potential for the disastrous rise of misplace power exists and will persist," Eisenhower said. "We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together."[4]

By providing readers with a detailed account of the development of the data aggregation industry and its ties with law enforcement, O'Harrow points out several areas of concern for the average American.

O'Harrow's first chapter, entitled "Six Weeks in August[5]," provides readers with a detailed account of the process by which the USA PATRIOT Act was drafted. He provides an interesting perspective by tracking the lives of Assistant Attorney General Viet Dinh, Jim Dempsey of the Center for Democracy and Technology, and Senator Patrick Leahy.[6]

---

3. WILL NEED CITE FOR THIS QUOTE TOWARDS THE END OF HIS TALK AT JMLS, DURING Q&ARobert O'Harrow, Jr., Lecture, *No Place To Hide*, (Chicago, Ill., Apr. 7, 2005) (copy of transcript on file with *The John Marshall Journal of Computer & Information Law*).

4. *See* O'Harrow, *supra* n. 2, at 9.

5. *Id.* at 11.

6. *Id.* at 10-12.

By following the lives of these men, O'Harrow defines the competing interests that were implicated in the drafting of the USA PATRIOT Act: "doing whatever was necessary to strengthen the government's legal hand against terrorists,"[7] "check[ing] the increasingly aggressive use of technology by law enforcement officials,"[8] and "striking the right balance" between security and privacy.[9] In the days after the September 11 attacks, the fear of Jack Dempsey and other civil libertarians was that we would see a return to the age of CONINTELPRO and revelations of the Church Report.[10] The Department of Justice, "saw a chance to turn back the clock," to the days before the Church Committee's report changed the face of domestic intelligence-gathering.[11] The tension between the civil libertarians and the Department of Justice is highlighted by Senator Leahy's efforts to strike a balance between the two sides.

O'Harrow's description of the events surrounding the drafting of the USA PATRIOT Act is also very enlightening. Most interesting is the description of the meeting between DOJ officials, Senate staffers and the privacy advocates. The representatives of the Department of Justice were upset to see their privacy-minded counterparts and initially refused to engage in a discussion with them, finally agreeing to simply read DOJ's suggestions and then leave.[12] Also interesting is his account of Senator Leahy's failed deal with former Attorney General John Ashcroft. Although Leahy had been under the impression that the Administration wanted to draft legislation that balanced security and privacy, he quickly found that many of his changes never made it past the initial drafting stages.[13] One example O'Harrow provides involves Section 215 of the USA PATRIOT Act, also colloquially known as the "library provision."[14] The book focuses, however, on the idea that Section 215 expanded law enforcement's power to obtain business records which had been expanded to, "in essence, any business."[15] This sets up one of the overarching themes of *No Place To Hide*: the unlikely marriage between pri-

7. *Id.* at 12.

8. *Id.*

9. *Id.* at 13.

10. *Id.* at 18 (describing the CIA surveillance of the U.S. Mail from 1953 to 1973, and CONINTELPRO, the FBI's domestic surveillance program that, "undermin[ed] the jobs of political activists, sen[t] anonymous letters to 'spouses of intelligence targets for the purposes of destroying their marriages,'" and specifically targeted to derail the "civil rights efforts" of Martin Luther King, Jr.).

11. *Id.* at 21.

12. *Id.* at 25.

13. *Id.* at 26-27.

14. *See* Deborah Zabarenko, *"Library Leader Questions Patriot Act,"* Reuters, available at http://www.boston.com/news/nation/washington/articles/2005/07/24/library_leader_questions_patriot_act/ (last visited accessed 10 Oct. 10ober, 2005).

15. *See* O'Harrow, *supra* n. 2, at 27.

vate data aggregators and law enforcement has some frightening implications.[16]

This specific example is not as dire as it may initially seem. While Section 215[17] does expand law enforcement's power to obtain business records by expanding the power to obtain records to "any tangible things," it also provides some protection for the civil liberties of U.S. citizens.[18] One of the most obvious protections, one that seems to defuse the concerns of librarians nationwide,[19] is that the powers granted to law enforcement pursuant to Section 215 cannot be used for investigations of U.S. citizens "conducted solely upon the basis of activities protected by the first amendment to the Constitution."[20] In this light, fears of law enforcement becoming the thought police are somewhat mollified. This sentence is awkward- not sure what you are trying to say – should it read "thought police" in quotes ? (ex- "the fear that law enforcement officials will become the "thought police" are somewhat mollified." Without further indication that a U.S. citizen is involved in terrorist activity, law enforcement cannot utilize its expanded powers to target someone based solely on choice of reading material. The potential for abuse remains, but it is worth noting that the power itself is no greater than that of criminal investigators who, via Rule 17(c) of the Federal Rules of Criminal Procedure, are empowered to simply subpoena "any books, papers, documents, data or other objects."[21] Moreover, given this section of the Federal Rules, criminal investigators have always been able to obtain business records, including library records via subpoena. It seems that this power to obtain library records has not been recently utilized by criminal investigators.[22]

To address O'Harrow's main concern, the ability to access other business records, it is worth noting that most of this information has been freely given by consumers to third parties over the years. The Supreme Court has held that there is no reasonable expectation of privacy in records of this nature.[23] This seems rather logical, especially given the

16. *Id.* (commenting that due to the vast amount of data already aggregated into consumer profiles, increasing law enforcement's power to obtain those records gives it an unprecedented look into our private lives).

17. 50 U.S.C. §1861-1863 et. seq. (2001). .

18. 50 U.S.C. §1861(a)(1) (2001). .

19. *See* D. Zabarenko *supra* n. 13 (indicating that the president of the American Library Association fears that this "Kafkaesque" change to the existing law will "[erode] the presumed trust" between patron and librarian).

20. 50 U.S.C. §1861(a)(1). .

21. *See* Andrew C. McCarthy, *"Why Sections 214 and 215 Should Be Retained*, in " p.49, *Patriot Debates: Experts Debate The Patriot Act*, 49 (Stewart Baker & John Kavanagh, eds., . (American Bar Association Standing Comm. on Law and Natl. Sec. 2005).

22. *Id.* at 50.

23. *See Id.* at 49 (citing *Smith v. Maryland*, 442 U.S. 735, 744 (1979)).

scope of the dissemination of those records. As O'Harrow notes throughout *No Place To Hide*, private data aggregators have amassed and trade massive amounts of consumer data. The databases of Acxiom alone hold as much information as a "50,000 mile-high stack of King James Bibles."[24] At some point, consumers gave this information to a third party and lost their expectation of privacy in that information. While the reality of Section 215 may seem to defuse O'Harrow's fears, the question that begs asking is whether it is good public policy to allow our personal information to continue to be traded and collected like baseball cards. To this extent, *No Place To Hide* is extremely valuable as a tool to inform Americans so that future policy choices can be made with a more informed populace behind them. His ominous tone aside, O'Harrow does a good job of setting the stage for the rest of the book. By raising awareness of law enforcement's access to personal information and invoking the memory of its misconduct in the past, he highlights the impact of possible abuse of increased domestic spying power in the Information Age.

This treasure trove of personal information is perhaps the most disturbing and prominent theme in *No Place To Hide*. Most interesting is O'Harrow's account of the development of the data aggregation industry, and the extent to which it has already developed dossiers on Americans. As early as 1964, it was possible to buy lists of consumers organized by such categories as "a thousand women who had bought a 'bust developer' product."[25] For a bit more than fifteen dollars, it was possible to obtain a list of "the names and addresses of newlyweds, 500,000 in all."[26] Leading the industry, and using the existing computer technology to help process more data at a faster pace, the credit bureaus began building comprehensive databases on consumers.[27] Some of the bureaus' methods for collecting information may be surprising to some Americans. For instance, a large amount of unverified information was collected by private investigators going door-to-door and asking questions about consumers.[28] As technology developed, the consumer dossiers helped create specialized services that are now commonplace in our society,[29] including "instant credit, cheaper mortgages, a panoply of shopping options, and . . . detailed and accurate phone books."[30]

As O'Harrow aptly notes, the growing consumer profiles were generally available for a fee if one was determined to obtain them.[31] This ac-

24. *See* O'Harrow, *supra* n. 2, at 37.
25. *Id.* at 40.
26. *Id.*
27. *Id.* at 40-41.
28. *Id.* at 41.
29. *Id.* at 41.
30. *Id.*
31. *Id.*

tivity naturally raised the suspicions of civil libertarians who warned against a future where personal information became "an economically desirable commodity and a source of power."[32] As the power of microprocessors increased, several giants in data aggregation began to grow. By obtaining customer information from other companies, Acxiom and other aggregators build their databases while helping those companies learn "more about what makes their customers tick."[33] Acxiom and its peers deny that they are secretly collecting information and tout their ability to make their use of their data "entirely transparent to the consumer."[34]

Although data aggregators are cast as businesses bent on collecting consumer information without considering privacy issues, it is worth noting that a large amount of this data is willingly provided by the consumer. One example is the success that Condé Nast has had with its Preferred Subscriber Network. In 1998, subscribers to Condé Nast publications had the opportunity to fill out an eight-page survey. The survey, covering topics ranging from level of education to whether a subscriber suffered the heartbreak of halitosis, was widely successful in helping the publisher learn more about its subscribers.[35] O'Harrow maintains his cautionary tone by stating, "What few of [the subscribers] realize is how their responses become part of a vast and growing information market."[36] While the information collected by the Preferred Subscriber Network surveys is highly personal in nature, it is worth restating that subscribers freely provided this information and that once given, they cannot reasonably expect it to remain private. Ignoring his often ominous tone, readers of *No Place To Hide* would do well to realize what this means for the consumer: don't give anyone information you don't want shared.[37] Since the data aggregation industry has embraced computers and database technology, that statement bears even more weight – one of Acxiom's data products indexes "almost 200 million people living in 110 million households."[38]

One of the most frightening things about private databases is that they are at risk of being misused by would-be identity thieves. Searching Google News for "identity theft" or "stolen customer records" turns up thousands of articles on the subject. While it may seem that identity theft has been increasing lately, the increase in reports relates to a re-

32. *See iId.* (referencing Arthur R. Miller's text, *The Assault on Privacy*).

33. *Id.* at 43.

34. *Id.* at 52.

35. *Id.* at 53-55.

36. *Id.* at 54.

37. It is worth noting, however, that the Federal Trade Commission does, to some extent, enforce the privacy policies of web sites that collect personal information.

38. *See* O'Harrow, *supra* n. 2, at 61.

cently enacted California statute that requires businesses to notify customers when their data is stolen.[39] When it was announced that one of MasterCard's third-party processors suffered a security breach that put forty million customers at risk of fraud,[40] affected consumers knew to request a new account number. Companies like Acxiom are also at risk; when their security is breached, the complex dossiers they maintain are exposed to potential misuse. Acxiom suffered a breach in 2003 that resulted in the records of about twenty million consumers, a total cost of $3.2 million for the data aggregator.[41] As *No Place To Hide* indicates, sometimes the costs passed on to the consumer have a greater price.

Michael Berry's tale, a large portion of the book's third chapter, demonstrates the impact of losing one's personal information to someone with less than honest intentions. While attempting to consolidate some debt onto one credit card, he discovered that his identity had been used to open several credit accounts at various retailers, sometimes with clearly incorrect information.[42] As if ruined credit wasn't bad enough, a convicted murderer had assumed Berry's identity and killed again, leaving Berry as a suspect, at least in name.[43] Although the criminal was eventually caught, and Berry's credit reports were slowly repaired, he spent almost three years of his life trying to clear his credit and worrying that he would be arrested due to mistaken identity.[44] What is perhaps most disturbing is that Michael Berry is not alone. Given the size of some private databases, and the myriad of sources from which their data is compiled, it should be no surprise that identity theft is on the rise and the criminals often difficult to trace. The Commercial Crimes Division of the Los Angeles Police Department received one hundred calls a day regarding identity theft cases in 2003, but was only able to investigate a handful of those calls.[45] According to private research group Gartner, Inc., seven million Americans fell prey to identity thieves in 2002.[46]

According to O'Harrow, the weak link both in security and in repairing credit reports is the credit bureaus and data aggregators. By opening accounts when inaccurate information is provided,[47] using easy-to-find

39. *See* Jeanne Sahadi, *"ID data breaches: as rampant as it seems," CNN Money.com*, available at: http://money.cnn.com/2005/06/21/pf/breach_followup/index.htm?cnn=yes (last visitedaccessed Oct.ober 12, 2005).

40. *See* Jeanne Sahadi, *"40m credit cards hacked," CNN Money.com*, available at: http://money.cnn.com/2005/06/17/news/master_card/index.htm?cnn=yes (last visitedaccessed Oct.ober 12, 2005).

41. *See* O'Harrow, *supra* n. 2, at 71-72.

42. *Id.* at 75-77.

43. *Id.* at 80-81.

44. *Id.* at 74-97.

45. *Id.* at 82-83.

46. *Id.* at 78.

47. *Id.* at 77.

tidbits of information as customer identifiers for phone transactions,[48] having inadequate data security,[49] and sometimes failing to fully correct mistakes on someone's credit report,[50] it certainly seems that the industry is guilty as charged. Although *No Place To Hide* shies away from making policy suggestions, it seems that the lackadaisical security policies of the keepers of consumer data are quickly becoming fertile ground for a new breed of lawsuit. One example is the lawsuit that Eileen Goldberg filed against ChoicePoint in February 2005.[51] The complaint alleges that since ChoicePoint compiles and sells consumer data for a profit, it owes a higher duty of care towards those whose data it compiles.[52] Identity thieves, posing as legitimate businesses, set up at least fifty accounts with ChoicePoint, giving them access to "Social Security numbers, credit histories and other personal information," all collected from consumers and aggregated by ChoicePoint.[53] This behavior continued for a year before ChoicePoint even realized what had happened.[54]

While ChoicePoint's negligent behavior is frightening, what is even more frightening is that it sells a virtual identity-check-in-a-box product called "Employee Background Check" at Sam's Club locations nationwide.[55] Although the product comes with release forms that must be signed by the subject of the identity check that are ostensibly audited by ChoicePoint, the company has never specified how or when these audits would occur.[56] If data aggregators are going to continue to sell consumer information, they must be held to a higher standard of care. Other lawsuits filed against data collectors have failed.[57] Courts have been hesitant to establish a duty of care owed by data aggregators to the individuals whose data they collect because those consumers are not customers of the data aggregators.[58] Despite this, as these companies continue to lose information to thieves and scammers, it seems that our legal system will be forced to address the issue, either via strong legisla-

48. *Id.* at 79-80.

49. *See* Sahadi, *supra* n. 40 (discussing a data security breach at Acxiom).

50. *See* O'Harrow, *supra* n. 2, at 97.

51. *See* Kim Zetter, *"California Woman Sues ChoicePoint," Wired News* (Feb. 24, 2005) available at http://www.wired.com/news/privacy/0,1848,66710,00.html?tw=WN_story_related (Feb. 24, 2005).(last visited October 12, 2005).

52. *Id.*

53. *Id.*

54. *Id.*

55. *See* O'Harrow, *supra* n. 2, at 135.

56. *Id.*

57. *See* Zetter *supra* n. 51 (indicating that previous negligence-based identity lawsuits have failed).

58. *See* Kim Zetter, *"ID Theft Victims Could Lose Twice," Wired News* (Feb. 23, 2005) available at http://www.wired.com/news/privacy/0,1848,66685,00.html (Feb. 23, 2005)(last visited October 12, 2005).

tion and stronger enforcement or via case precedents that indicate a duty of care to the subjects of their extensive databases.

It is ironic that data aggregators like ChoicePoint and Acxiom have farmed their services out to law enforcement, especially since ChoicePoint was unable to verify the identity of its "customers," allowing identity thieves to buy consumer information.[59] Although it does not draw this correlation, *No Place To Hide* spends significant time discussing the relationship between data aggregators and law enforcement. In the wake of the September 11, 2001 terrorist attacks on New York City and Washington, D.C., data aggregators realized that they could use their vast collections of consumer information to assist law enforcement in catching criminals and preventing further terrorist attacks.[60] This assistance was also worth a hefty sum in government contracts awarded to the aggregators.[61]

The power of consumer databases and profiling technology is both shocking and amazing. One example is Seisint's product, The Matrix. During the D.C. Sniper shootings of 2002, law enforcement was scrambling to capture the shooters with little luck. Hank Asher and other Seisint executives were frustrated that D.C.-area law enforcement had been unwilling to send data to Matrix.[62] However, after lobbying the FBI to produce information and after another victim was killed, law enforcement provided a wealth of information to Matrix.[63] When combined with the power of the Matrix profiling system, Seisint predicted that it would take a week at most to find the shooters.[64] On October 23, law enforcement claimed that it had a suspect.[65] After running the suspect through Matrix, the technicians at Seisint felt that it wasn't the right person.[66] Starting with a database of over 21,000 John Williamses, Matrix narrowed down the field based on law enforcement input until a man from Tacoma, Washington had been singled out.[67] As it turned out, this was the John Williams who, along with John Lee Malvo, had been responsible for the killings in the D.C. area; by October 24, 2002, the pair had been captured.[68]

Despite this criminal-catching potential, outcry from lobbyists and

59. *Id.*
60. *See* O'Harrow, *supra* n. 2, at 56-57, 98-100, 152.
61. *Id.*
62. *Id.* at 118.
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.* at 118-19.
67. *Id.* at 119.
68. *Id.*

privacy groups ultimately killed Matrix's adoption by law enforcement.[69] The main concern of the privacy lobby was that allowing law enforcement access to consumer databases would ultimately be an end-run around the evidence-gathering restrictions of the Fourth Amendment.[70] John Poindexter, of the failed Total Information Awareness project, also had misgivings about Matrix, largely based on the background of Hank Asher, founder of Seisint.[71] O'Harrow spends a considerable amount of time discussing Asher's past, describing him as a drug-smuggler and indicating that he may have had ties to the plan to assassinate Daniel Ortega, the former Nicaraguan President.[72] While these characterizations may be newsworthy, and do cause one to question whether a "rogue fellow"[73] should have access to so much consumer information, let alone access to Federal law enforcement, it detracts from the concerns of the privacy lobby. What is most frightening about the collusion between the data aggregators and law enforcement is that the ability to profile is increased exponentially. While the information is already technically public, having been freely given to private companies by consumers, allowing law enforcement to use the databases to profile suspects seems like bad policy, even if it is Constitutionally acceptable. The ACLU took issue with this approach, describing it as "replacing an unpopular Big Brother initiative with a lot of Little Brothers."[74] As opposed to spending several pages focusing on Hank Asher's possibly shady background, *No Place To Hide* should have focused on the arguments both for and against systems like Matrix.

This is not to say that O'Harrow completely ignores the potential problems of the trend of data aggregator and law enforcement cooperation. One example is the fact that no matter how amazingly sophisticated, consumer databases are only as accurate as the information they are provided and sometimes they just produce false positive results. O'Harrow points to DBT's list-cleansing efforts that excluded many Florida voters from the polls in November 2000.[75] Due to flawed information and very little double-checking by election officials, a large number of Florida voters were inappropriately barred from voting due to false-positives for felony convictions.[76] Whether this gave George W. Bush the

69. *Id.* at 122-23.

70. *Id.* at 123.

71. *Id.*

72. *Id.* at 111, 112.

73. Robert O'Harrow, Jr., Lecture, *No Place To Hide*, (Chicago, Ill., Apr. 7, 2005) (copy of transcript on file with *The John Marshall Journal of Computer & Information Law*).'NEED CITE FROM LECTURE TRANSCRIPT

74. *See* O'Harrow, *supra* n. 2, at 123.

75. *Id.* at 125-29.

76. *Id.*

advantage in the 2000 elections aside, O'Harrow echoes a point made by Chris Hoofnagle, an attorney for the Electronic Privacy Information Center: "By outsourcing the collection of records, the government doesn't have to ensure the data is accurate, or have any provisions to correct it in the same way it would under the Privacy Act."[77] Hoofnagle characterizes this behavior as "sidestepping the laws intended to protect individuals from government intrusion."[78]

This point is reinforced by O'Harrow's descriptions of developing technologies like face-recognition software and other biometric identification systems. Although he does recognize that face recognition and other biometric technologies may help victims of identity theft like Michael Berry,[79] he quickly turns back to his cautionary tone stating, "The use of biometric identifiers shifts an enormous amount of power into the hands of those who control the equipment . . . what about when government turns to those records to satisfy it obsession for security?"[80] O'Harrow likens this to the "Panopticon," a theoretical prison, the design of which makes prisoners feel constantly watched.[81] While this could be the end-result of a society in which the government makes heavy use of surveillance cameras, Americans who live in urban areas are already being watched more than they know. For instance, the NYC Surveillance Camera project has lists and maps of the location of all security cameras in Manhattan.[82] The City of Chicago has similarly dense cameras in the downtown Loop area,[83] and the City of Chicago Police Department has deployed surveillance cameras controllable by police via squad car laptop.[84] Adding face-recognition technology to these existing systems, and linking private and governmental camera systems to a common database would certainly put individuals in public places under closer scrutiny; however, one has never had an expectation of privacy in public places. If these technologies cannot reach into the homes of Americans, it seems unlikely that our society will become as extreme as Bentham's Panopticon. Certainly, building databases of biometric information would require the same work-around as systems like the Matrix, such that private aggregators would need to index the data and then sell it to

77. *Id.* at 137.

78. *Id.* at 138.

79. *Id.* at 167.

80. *Id.* at 169-70.

81. *Id.* at 170.

82. *See NYC Surveillance Camera Project Maps,* available at: http://www.mediaeater.com/cameras/locations.html (last visitedaccessed Nov.ember 1, 2005).

83. *See Surveillance Cameras in Chicago, "Chicago, IL,"* available at: http://www.notbored.org/chicago-SCP.html (last visitedaccessed Nov.ember 1, 2005).

84. *See* Andrew Buchanan, *"On Chicago Streets, Cameras Are Watching," The Christian Science Monitor* (July 30, 2003) available at: http://www.csmonitor.com/2003/0730/p01s02-usgn.html (July 30, 2003).(last visited November 1, 2005).

the government. Even then, if done at the request of law enforcement, it would raise questions as to whether the activity was protected by the Privacy Act of 1974. As the technology stands right now, it is highly unlikely that face recognition and biometrics will be the invasive nightmare that O'Harrow warns against any time soon.[85]

On the whole, *No Place To Hide* is valuable because it serves to inform Americans about the extent to which their personal information is being used both by private companies and law enforcement. The amount of personal information available to data aggregators and government is staggering. The current capabilities of consumer databases are fascinatingly frightening and they are only increasing. Nascent technologies like biometrics could enable a much more pervasive surveillance culture. These statements are true, but they are not set in stone. State legislatures are the most likely place for privacy to regain a foothold in the American legal system. California has already passed legislation to help its citizens shore up their informational privacy. The California Civil Code requires that collectors of consumer data inform those potentially affected by a breach of security.[86] The result is that consumers nationwide are made aware of these security breaches, creating a trickle-up effect that can help individuals protect their privacy.

This effect, in turn, increases individual awareness of privacy issues. As more Americans become aware of the threats to their privacy, States will be forced to address the concerns of their citizens. Additionally, stalled Federal legislation like the Notification of Risk to Personal Data Act may receive a second look from Congress.[87] Citizens must be informed enough about the risks to their privacy to be concerned and demand protection. *No Place To Hide* meets this need, and its ominous tone certainly drives the message home. Although all is not yet lost, O'Harrow establishes the threats to privacy and provides Americans with many valid reasons to be concerned.

---

85. *See* O'Harrow, *supra* n. 2, at 181.
86. CA Civ. Code §1798.29 (2001).
87. *See* Zetter, *supra* n. 58.