The John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 1 *Journal of Computer & Information Law - Fall 2000*

Article 9

Fall 2000

Database Nation: Does Information Technology of the 21st Century Pose a Daunting Threat to Personal Privacy in America, 19 J. Marshall J. Computer & Info. L. 197 (2000)

Robert S. Gurwin

Nicole D. Milos

BOOK REVIEW

DATABASE NATION — DOES INFORMATION TECHNOLOGY OF THE 21ST CENTURY POSE A DAUNTING THREAT TO PERSONAL PRIVACY IN AMERICA?

by ROBERT S. GURWIN†

Half a century ago, George Orwell's classic *1984* decried the loss of personal privacy to a totalitarian government which spied on its citizens, used video surveillance and controlled the media in order to maintain power.[1] Since the time Orwell's work was published, we have witnessed first hand as many of the purely fictitious technologies from *1984* have become frighteningly real. With each passing day, our capitalistic society fuels greater demand for gathering, exchanging, and selling of personal information.

Expressing grave concern for the demise of individual privacy rights, Simson Garfinkel, a frequent writer on computer themes and a weekly columnist for the Boston Globe has fired a warning shot by and through his recent work, *Database Nation: The Death of Privacy in the 21st Century.*[2] In his book, Garfinkel supposes a future where privacy has become a costly commodity. Individuals wishing to keep personal information from prying eyes are forced to take painstaking efforts to buy back their personal data or face the consequences of having it sold.

† Robert S. Gurwin, Attorney at Law, LL.M. in Information Technology, 2001, The John Marshall Law School; J.D., 1992, Case Western Reserve University School of Law; B.A., 1989, The University of Michigan. Mr. Gurwin would like to thank Leslie Ann Reis, Director of the John Marshall Law School Center for Information Technology and Privacy Law for her encouragement and guidance in preparing this article for publication.

1. George Orwell, *1984* (Signet Classic 1949).

2. Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly & Associates, Inc. 2000).

Indeed, *Database Nation* presents some very solid and compelling arguments to support legislative efforts regulating privacy in the United States. However, the author has painted a somewhat jaded picture of the technology and law at issue in attempt to bolster a sense of urgency to his cause. In fact, when examining a number of the specific concerns addressed by the author, it becomes blatantly apparent that there are already sufficient measures in place to protect the privacy of American citizens from many of these unwanted invasions of privacy and intrusions upon seclusion. Moreover, by exercising basic common sense and using appropriate discretion, Americans can often avoid many of the pitfalls that Garfinkel warns could potentially pierce their personal privacy.

In no way, however, does the author's very zealous battle cry detract from the book's extremely interesting historical account of the information age. Garfinkel provides a masterful layout of the political, social and technological forces that have made gathering, indexing and sale of personal information a potential Pandora's box that could, if left to its own devices, undermine any sense of individual privacy rights in this country. It is from this framework that the reader is able to fully understand the repercussions of freely unleashing personal data, which would clearly obliterate any sense of personal privacy. In this regard, Garfinkel's message is both valid and thought provoking since the continuing technological revolution mandates the adoption of appropriate social policy to balance individual privacy rights against the rapidly growing electronic exchange of information.

Garfinkel's chronology begins with several examples of what he calls "Privacy Under Attack."[3] Herein, the author exemplifies the loss of personal privacy, taken to the far extreme. He suggests a day when:

> Arriving late at work, you receive a polite email message from the company's timecard system; it knows when you showed up, and it gives you several options for making up the missed time. You can forgo lunch today, work an extra 45 minutes this evening, or take the 45 minutes out of your ever-dwindling vacation time. The choice is yours.[4]

Turning to the home front, the author explains that:

> [y]ou decide to go through yesterday's mail. There's a letter from the neighborhood hospital you visited last month. 'We're pleased that our emergency room could serve you in your time of need,' the letter begins. 'As you know, our fees (based on our agreement with your HMO) do not cover the cost of treatment. To make up the difference, a number of hospitals have started selling patient records to medical researchers and consumer marketing firms. Rather than mimic this distasteful behavior, we have decided to ask you to help us make up the

3. *Id.* at 1-12.
4. *Id.* at 2.

> difference. We are recommending a tax-deductible contribution of $275 to help defray the cost of your visit.'[5]

Garfinkel's examples are purposefully designed to make the reader uncomfortable and for good reason. Although employers routinely utilize current technology to track employees' time, the thought of receiving an electronic spanking from the computer for showing up late is both degrading and demoralizing. Far worse, however, is the thought of health care providers selling patient records to researchers or marketers. Generally, people expect that information about our health and medical treatment is entirely personal in nature and should never be commercially compromised. This premise has even been codified into law, as in Illinois where there is a specific right of each patient to privacy and confidentiality in health care.[6] The state statute provides that:

> Each physician, health care provider, health services corporation and insurance company shall refrain from disclosing the nature or details of services provided to patients except that such information may be disclosed to the patient, the party making treatment decisions if the patient is incapable of making decisions regarding the health services provided, those parties directly involved with providing treatment to the patient or processing the payment for that treatment, those parties responsible for peer review, utilization review and quality assurance, and those parties required to be notified under the Abused and Neglected Child Reporting Act [325 ILCS §§ 5/1 et seq.], the Illinois Sexually Transmitted Diseases Control Act [410 ILCS §§ 325/1 et seq.] or where otherwise authorized or required by law. This right may be waived in writing by the patient or the patient's guardian, but a physician or other health care provider *may not* condition the provision of services on the patient's or guardian's agreement to sign such a waiver. (Emphasis added.)[7]

While posed for effect, lawmakers concerned about protecting patient privacy have contemplated Garfinkel's scenario. Therefore, the very activity of which the author warns has already been legislatively precluded.[8]

Yet the author attempts to scare the public continue well into the next chapter wherein he attacks the practices of Equifax, Experian and Trans Union Corporations, our nations three primary credit-reporting agencies.[9] Garfinkel tells the tale of "Steve and Nancy Ross, who did a lot of traveling in the early 1980s and paid for it with a ruined credit

---

5. *Id.* at 1.

6. *Public Health Prevention and Protection Medical Patient Rights Act,* 410 ILCS § 50/3(d) (1998).

7. *Id.*

8. *Id.; see also e.g.* Cal.Civ. Code §§ 56.05(d), 56.10 (West 1997 & Supp. 1998); Minn. Stat. § 144.335, 3a(a) (1996).

9. *Garfinkel, supra* n. 2, at 24.

report, courtesy of the Internal Revenue Service."[10] The couple had allegedly made certain estimated quarterly Federal income tax payments that were never properly credited due to the fact that they temporarily resided away from their home in New Jersey and payments they had mailed were routed, instead, to an IRS service center in California. Due to this mix-up, the IRS placed a 10,000 dollar lien against the couple's home in New Jersey, which became part of their credit report as maintained by Equifax, Experian (then known as TRW) and Trans Union. This negative information caused the couple to endure incredible difficulties ranging from their local bank canceling their credit card to being unable to secure any other type of charge or loan privileges.

Ultimately, the Ross family cleared up the misapplied tax payments with the Internal Revenue Service, which then cleared the lien it had erroneously filed. According to the author, however, when Mr. Ross contacted TRW to remove the erroneous entry, the following exchange took place:

> 'I called up TRW first,' says Steve Ross. 'They said 'no problem, send a copy of the letter [from IRS] and an explanation, and we will put that with your credit report.'[sic]' I said, 'Aren't you going to expunge the record?' They said 'No.' They don't do that. When you have an unfavorable note in your credit report, they don't take it out; they just put your explanation with it.[11]

By simply accepting this as proper application of the law, the Ross family went through seven years of being unable to use credit because they allowed the negative information, albeit false, to remain as part of their credit report.

In reality, the Federal Fair Credit Reporting Act ("FCRA") clearly provides for the removal of inaccurate information from a consumer's credit report, such as the tax lien at issue in the Ross case.[12] Specifically, the FCRA provides that when a consumer has requested a dispute investigation, "The consumer reporting agency shall promptly provide to the person who provided the information in dispute all relevant information regarding the dispute that is received by the agency from the consumer. . ."; and if "an item of the information is found to be inaccurate or incomplete or cannot be verified, the consumer reporting agency shall promptly delete that item of information from the consumer's file or modify that item of information, as appropriate, based on the results of the reinvestigation."[13] (Emphasis added). Pursuant to the provisions of the FCRA, Mr. Ross should have enforced his right to have the erroneous tax lien information deleted from his credit report and could have considered

10. *Id.* at 25-26.
11. *Id.* at 27.
12. 15 U.S.C. § 1681(h) (1994).
13. *Id.*

filing a civil suit against any reporting agency that failed to do so for violation of the FCRA. Once again, the author has posed an alarming situation for which a clear legal remedy already exists. In cases concerning credit data, courts of law are becoming increasingly sympathetic to the consumer who has been harmed due to falsely maintained and reported data and are sending a message to the nation's credit agencies to clean up their acts.[14]

Scare tactics aside, Garfinkel provides a fascinating account of the many different facets of information technology being used to gather and disseminate data. For example, the author devotes an entire chapter to the data that is collected in the ordinary course of life.[15] This includes the electronic bread crumbs that are thrown whenever we use an automated teller machine to withdraw some cash, shop using a credit or debit card, pick up the telephone and place a call, drive on a toll road, or bring a vehicle across the U.S./Canadian border.[16]

Another chapter, entitled "A View From Above," traces the history of satellite surveillance technology beginning with Cold War-Era devices used to spy on the former Soviet Union up through modern day units that currently orbit the earth taking a perpetual video of life on planet earth.[17]

The author notes how satellite surveillance violates no law or treaty since things that happen outdoors, in public, are public by definition.[18] However, Garfinkel uses this chapter of the book to offer a very frank discussion of the political implications resulting from deployment of commercial spy satellites.[19] Launched in 1986 by the French government, SPOT 1 (a French acronym for *Satellite Pour l'Observation de la Terre* – satellite for observation of the earth) was the first satellite that sold its captured images for commercial purposes.[20] The SPOT 1 just happened to be passing over the Ukraine when the Chernobyl nuclear power plant was burning out of control and approaching nuclear meltdown. In its usual fashion, the Soviet government had tried to keep this disaster from making world headlines, but the SPOT satellite pictures portrayed the horrid truth and severity of the situation.[21] According to Garfinkel, the French government has acted very responsibly when weighing the com-

14. *See e.g., Cushman v. Trans Union Corp.*, 115 F.3d 220 (3rd Cir. 1997); *Guimond v. Trans Union Credit Info. Co.*, 45 F.3d 1329 (9th Cir. 1994); *O'Connor v. Trans Union Corp.*, 1999 WL 773504 (E.D. Pa. 1999).

15. Garfinkel, *supra* n. 2, at 69-93.

16. *Id.* at 69.

17. *Id.* at 93-125.

18. *See id.* at p. 97.

19. *Id.*

20. *Id.* at 97.

21. *Id.* at 98.

mercial use of its satellite against issues of international security. For example, during the Persian Gulf War, the French refused to allow the sale of any satellite photographs to the news media that could have revealed information about troop movements in the battle areas.[22] On the other hand, the author points out how photographs were made available to the United States military in order to document the results of Serbian ethnic cleansing in Kosovo which, in turn, helped rally public support for NATO's bombing of Serbia.[23]

Working from the surveillance cameras that orbit the earth's atmosphere to the security cameras outside many buildings and parking lots, Garfinkel draws a nice balancing line to establish the reality that there is, in fact, a time and place for the use of these technologies. He acknowledges that security cameras protect the public by curtailing terrorist activities and have assisted law enforcement in solving crimes such as bank robbery, auto theft and the like. The author concludes this section on a humorous note pointing out how surveillance technology enabled he and his wife to find out what their cats do while left alone all day at home.[24]

Moving forward, the author launches an examination of market data and the increasing ability of companies to custom tailor their advertising to those most likely to have an interest in their products and services. Garfinkel cites to the very popular grocery store loyalty card programs which enable a supermarket to know exactly which products each customer purchases, how often these items are purchased, and even whether it takes a 10-cent or a 50-cent incentive coupon to persuade the customer to buy a particular item.[25]

But the author is quick to point out the privacy implications when customers voluntarily reveal such a wealth of information about their buying habits. In one case, a supermarket faced with a lawsuit by one of its customers, who had slipped and fallen on store property, threatened to use the fact that the customer was a frequent purchaser of alcohol to damage his reputation to the court.[26]

Moreover, Garfinkel expresses a very strong distaste for direct marketing firms and the marketing practices of large companies that take great liberties with their customer's personally identifiable information without seeking consent. The author mentions CVS Pharmacy and Giant Foods Pharmacy by name, as both firms sold their customer's pre-

22. *Id.* at 102.

23. *Id.* at 98.

24. *Id.* at 109 (explaining how the author and his wife set up a Web cam on their personal computer in order to watch the activities of their pet cats).

25. *Id.* at 98.

26. *Id.* at 159; *see also Rivera v. Vons Co.*, <http://www.lasurperiorcourt.org/CivilRegister/register.asp?divCode=CV&Case=BC155495> (L.A. Sup. Ct. Mar. 9, 1999).

scription drug information to a marketing firm. The drugstores claimed they were doing so only to send out mailings to remind customers to refill their prescriptions. However, a newspaper investigative journalist revealed that, in fact, the profiles were also being used for targeted marketing and were being shared with other pharmaceutical manufacturers.[27] Along these same lines, Garfinkel discusses lawsuits filed against U.S. News and World Report by a disgruntled subscriber whose name and address were leased to other magazines for solicitation purposes.[28]

In defense of the author's charges, the Direct Marketing Association ("DMA") has long maintained a system of opt-out wherein consumers who do not wish to receive solicitation mailings can send a card to the DMA asking to be removed from the marketing lists.[29] In theory, the unwanted mail is then supposed to cease.[30] However, this system to opt-out is fatally flawed as Garfinkel points out these numerous holes in the system:

Many consumers don't know that opt-out lists exist or even how to exercise their ability to opt-out;

Every time a consumer moves, it is necessary to re-register to continue opting out of direct market mailings;

Registration for opt-out expires every five years, requiring consumers to continually re-register;

Companies sending bulk mailings are not legally required to use the lists so many simply do not.[31]

Ultimately, Garfinkel advocates the use of existing laws in this arena to fight back against direct marketers and urges adoption of additional laws protecting consumers from the unwanted sales pitches.

Existing laws affording protection include the 1991 Federal Telephone Consumer Protection Act, which prohibits telemarketers from faxing advertisements without the permission of the machine's owner.[32] More importantly, this law criminalizes the use of automatic dialing units that make calls to consumers and play pre-recorded telemarketing messages.[33] States have enacted similar laws such as the Illinois Automatic Telephone Dialers Act that, in essence, parallels the Federal statute.[34] Likewise, the Illinois Telephone Solicitations Act limits the hours

27. Garfinkel, *supra* n. 2, at 173.

28. *Id.* at 178-79; *See generally Avrahami v. U.S. News and World Report, Inc.*, 1996 Va. Cir. LEXIS 518.

29. Garfinkel, *supra* n. 2, at 169.

30. *Id.*

31. *Id.* at 169.

32. 47 U.S.C.S § 227 (2000).

33. *Id.*

34. 815 ILCS § 305/5.

during which telemarketing calls can be placed and requires that the marketer immediately identify his or her name, the name of the business or organization being represented and the purpose of the call.[35]

Further aiding consumers is section 310.4 of the Federal Trade Commission's Telemarketing rule, paralleled by state statutes which mandate: "if the person called requests to be taken off the contact list of the business or organization, the operator must refrain from calling that person again and take all necessary steps to have that person's name and telephone number removed from the contact records so that the person will not be contacted again."[36]

Concluding this section, Garfinkel makes a number of constructive and feasible suggestions to expand existing privacy protection laws in this area. His first proposition is to require direct mailings to carry an indexing code number on the address label which consumers would be able to use in order to request their names be deleted from mailing lists.[37] The second recommendation is what has been known as an "asterisk law" wherein consumers may have their telephone numbers added, at no-charge, to a national registry of numbers that telemarketers are legally precluded from calling.[38] Telemarketers calling a number on the asterisk list would be fined $10,000 for each violation as a very stiff incentive to keep unwanted telemarketing calls from being placed. Although both of these ideas also operate on an opt-out basis, they certainly afford consumers greater ability to eliminate unwanted solicitations by either mail or telephone and could prove to be an effective plan to strengthen rights of privacy in the information age.

In evaluating the state of privacy in the 21st century, Simson Garfinkel asks his readers to focus on three key elements that he believes will ensure an America where some semblance of privacy exists. First, he stresses the need to rethink consent, pointing to the blanket authorizations that the public mindlessly signs each day.[39] By doing so, Garfinkel argues that consent in this country has turned into an absolute joke and has become meaningless. The author appropriately states that "[c]onsent is a great idea, in practice, but the laws that govern consent need to be rewritten to limit what kinds of agreements can be made with consumers. Consent should be more of a two-way street, with the organizations that are demanding consent making the terms and conditions

35. 815 ILCS § 413/15.

36. *Id.*

37. Garfinkel, *supra* n. 2, at 169-73.

38. *Id.* at 174.

39. *Id.* at 264. For example, people often sign forms for medical providers and insurance companies authorizing an unconditional release of their personal information for an indefinite period of time. *Id.*

exceedingly clear. Blanket, perpetual consent should be outlawed.[40]

Second, Garfinkel stresses the importance of computer security, urging that both the makers and users of this technology must not overlook or side step the issue. As an example, the author cites the booming cellular telephone industry in the 1980s, which from the start was an inherently insecure network wherein any person with a radio scanner could listen in on cellular conversations.[41] Instead of developing a mobile telephone system where eavesdropping was not possible, the manufacturers lobbied Congress to enact laws to make it illegal to listen in on cellular conversations. The author's point about such backward logic is completely valid and should be considered in developing privacy policy in the future.

Finally, Garfinkel urges that the United States should resurrect the Office of Technology Assessment ("OTA"). Created in October 1972 and signed into law by President Richard Nixon, the OTA was directed to serve the following objectives:

Identify existing or probable impacts of technology or technological programs;

Where possible, ascertain cause-and-effect relationships;

Identify alternative technological methods of implementing specific programs;

Identify alternative programs for achieving requisite goals;

Make estimates and comparisons of the impacts of alternative methods and programs;

Present findings of completed analyses to the appropriate legislative authorities;

Identify areas where additional research or data collection is required to provide adequate support for the assessments and estimates described in paragraphs 1-5 of this subsection;

Undertake such additional associated activities as the appropriate authorities specified under subsection (d) may direct.[42]

While the OTA did not have any power to make laws or regulations, it published reports on topics that Congress asked it to study. According to Garfinkel, of the 741 reports that the OTA prepared before it was killed in 1995,[43] 175 dealt with privacy issues. Specifically, the author notes:

> The OTA's 1988 report 'Electronic Record Systems and Individual Privacy' looked directly at many of the databank issues discussed in Chapter 2 of this book, and drew the parallel between privacy and com-

40. *Id.*

41. *Id.*

42. *Id.* at 265.

43. The newly elected Republican majority of Congress eliminated the OTA in 1995.

> puter security. The OTA looked at issues of worker monitoring, as in its 1987 report 'The Electronic Supervisor: New Technology, New Tensions.' Likewise, the OTA considered at length the tradeoffs between law enforcement and civil liberties, especially in the context of wiretapping, database surveillance, and remote surveillance systems. . . It is a tragedy that the people of the United States allowed their elected representatives to kill the OTA. Any serious privacy agenda for the twenty-first century should include re-creation of this national treasure.[44]

Such an agency remains plausible since it does not run contrary to the Clinton Administration's consistent policy on technology and e-commerce matters.[45] The Clinton Administration openly endorsed the concept of industry self regulation, rather than government imposed legislation, so as to avoid any undue restrictions on electronic commerce. Announcing his policy, President Clinton stated that "for electronic commerce to flourish, the private sector must lead" and directed executive agencies to refrain from imposing unnecessary regulations where effective industry self-regulation measures are in place.[46] Since the OTA did not legislate or regulate in any manner, but rather served in an advisory capacity to the Congress, such an agency could play a vital role in helping to shape the future balance between technology and privacy rights in America.

Database Nation is an important work because it reminds Americans to stop and think about the value of their personal data, and moreover, to remember that it should not be taken for granted. By demonstrating the extent to which personal information is being gathered, indexed and sold, Garfinkel attempts to educate so that, in turn, the public can elect representatives through the democratic process who will strike the appropriate balance between technology and privacy in shaping the future of our country. For its role in furthering this process, *Database Nation* will likely hold ongoing literary merit for its detailed and candid account of the technology versus privacy dichotomy that exists as we enter the 21st century.

---

44. Garfinkel, *supra* n. 2, at 266.

45. Elizabeth Weise, *Privacy is Peter Swire's domain: Behind the scenes, he's president's go-to guy,* U.S.A. Today <http://www.usatoday.com/life/cyber/tech/cti036.htm> (June 7, 2000) (recognizing the importance of privacy issues, President Clinton appointed Ohio State University law professor Peter Swire to serve as his Chief Counselor for Privacy in the Executive Office of the President at the Office of Management and Budget. Swire, the first person to hold the position, served in an advisory capacity, much like the role served by the former Office of Technology Assessment). In addition, Swire acted as a national voice on privacy issues. *Id.*

46. President William J. Clinton, Vice President Albert Gore, *A Framework for Global Electronic Commerce* (July 1, 1997) <http://www.iitf.nist.gov/eleccomm/ecomm.htm> (accessed Nov. 15, 2000).