Wisconsin Lawyer

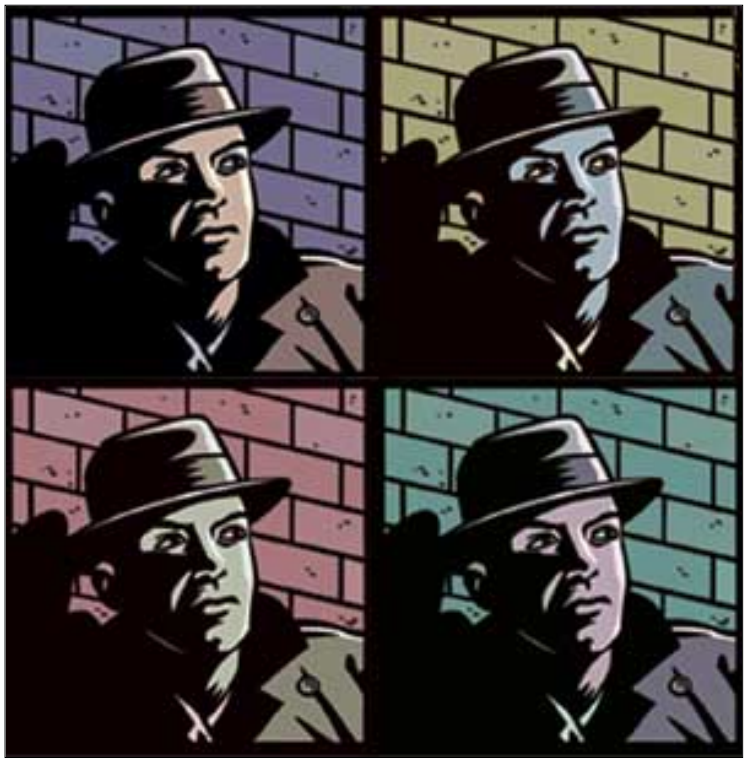
Make a Selection

Vol. 74, No. 2, February 2001

Carnivores, Cyber Spies and the Law

While it is difficult to stay informed about new technologies and laws that enhance privacy or permit its invasion, the matter is substantially important to all attorneys and their clients. Information is a key element in the practice of law, the conduct of business, and the functioning of democracy. Attorneys need to know how to get and protect information.

by Michael K. McChrystal, William C. Gleisner III, & Michael J. Kuborn



Protecting data is critical to the development of the wondrous economic and social potential of cyberspace.[1] Stated simply, online privacy and online security[2] are necessary conditions for a thriving electronic world. Threats to privacy arise with almost every new development in information technology. As detailed in previous Wisconsin Lawyer articles, cyberspace poses a growing host of privacy issues.[3] New technologies are coming online for increasingly sophisticated "Web tracking"[4] of individual Web users;[5] for expanded forms of "cyber spying" by employers, parents, and spouses;[6] and for highly sophisticated government surveillance systems.[7]

Widespread concern is expressed about online privacy invasions,[8] but the use of technical and legal protections against those invasions is sporadic at best.[9] With the rapid changes that have been occurring, it is difficult even to stay informed about new technologies and laws that enhance privacy or permit it to be invaded. This is a matter of substantial importance to all attorneys. Information is a key element in the practice of law, the conduct of business, and the functioning of democracy. Attorneys need to know how to get and how to protect information. Along with many clients, attorneys are themselves in the information business.

This article surveys three emerging technologies and the risks they pose to data privacy and security: online criminal investigation tools, private "cyber spying" programs, and online public records.

Carnivore and Other Criminal Investigation Tools

Cops chase robbers, and robbers are doing more of their dirty work in cyberspace. Online criminal investigation and surveillance technologies are intended to enhance online security, but public security often involves infringements of individual privacy. This recognition is, of course, the cornerstone of Fourth Amendment protections, particularly since the pivotal decision in Katz v.

United States[10] began defining those protections in terms of what is reasonably viewed as private.

"Carnivore," a recent technology developed by federal law enforcement agencies, has been the subject of a great deal of attention in the popular press.[11] The Carnivore system's very methodology makes an important point about the way in which technological innovations threaten privacy interests.

For some time, law enforcement agencies have been allowed to record a telephone subscriber's outgoing telephone numbers (using pen registers) and incoming telephone numbers (using trap and trace devices) without a probable cause showing.[12] Carnivore originally was designed to perform similar functions in an email context.[13] According to recent testimony before Congress, however, markedly different principles are involved:

"Carnivore operates by monitoring all traffic on the network link where it is installed. In theory, Carnivore examines traffic and only stores data appropriate to the order under which it operates - i.e., data relating to the target of an order, or even narrower information pertaining to pen register or trap and trace orders. Does Carnivore only reveal the information that is legally entitled under a particular wiretap or pen register order? Since Carnivore operates openly on a network link, it has the potential to capture the traffic of customers who are not the subjects of an order. It also has the potential to capture the content of communications even when a pen register order would limit collection to addressing information."[14]

The decision in United States Telecom Association v. Federal Communications Commission describes some of the efforts of federal law enforcement agencies to keep pace with new information technology.[15] The story begins with the Electronic Communications Privacy Act of 1986 (ECPA), under which law enforcement agencies are required to meet a much lower standard for retrieving incoming and outgoing telephone number information than they are required to meet for intercepting the content of telephone calls.[16] Simply put, whom you talk to on the telephone is less protected than what you say.

In response to advances in communication technology, Congress enacted the Communications Assistance for Law Enforcement Act of 1994 (CALEA) "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing, and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services."[17] The point of CALEA was to update the government's ability to monitor and investigate possibly unlawful conduct. CALEA did not expressly cover "information services" such as email and Internet access.[18]

Following two years of proceedings and extensive negotiations with the FBI, the Telecommunications Industry Association (TIA), an accredited standard-setting body, adopted technical standards pursuant to CALEA and published them as Interim Standard/Trial Use Standard J-STD025 (the "J-Standard"). Unlike CALEA, the J-Standard included procedures for dealing with "data packet" traffic, or email. Serious concerns were voiced regarding the technical feasibility of separating call content (requiring a Title III wiretap warrant) from call-identifying information (requiring only a pen register order) in the email context.

The FCC denied challenges to the adoption of this new standard, but it did order the industry group "to study CALEA solutions for (data packet) technology and report to the Commission in one year on steps that can be taken, including particular amendments to [the J-Standard], that will better address privacy concerns."[19] The court upheld the FCC's action in this regard, but emphasized that "nothing

in the Commission's treatment of packet-mode data requires carriers to turn over call content to law enforcement agencies absent lawful authorization."[20] Thus, adoption of the standards did not mandate actions in excess of Congressional authority and denied further review of the challenges to data packet standards.[21]

The bottom line is that a proper legal solution to the question of intercepting email information must await the technological ability to examine only email addressing information without scrutinizing the content of the email. Until that ability exists, the higher wiretap standard ought to apply.[22] The Carnivore controversy involves this very point, with the question being whether this technology has, in fact, arrived.

While sometimes the law must wait until the technology is available, often the technology has arrived and the law remains mired in the past. Consider this testimony before the Congress:

"Remarkably, the Electronic Communications Privacy Act of 1986 (ECPA) was the last significant update to the privacy standards of the electronic surveillance laws. Astonishing and unanticipated changes have occurred since then.... These changes have left gaps and ambiguities in the surveillance law framework. Most fundamentally, as a result of these changes, personal data is moving out of the desk drawer and off of the desktop computer and out onto the Internet. More and more, this means that information is being held and communicated in configurations where it is in the hands of third parties and not afforded the full protections of the Fourth Amendment under current doctrine. The government argues that this is a choice people make - you can keep the data in your own home and you can stay off the Internet if you care about privacy. But in a world where the Internet is increasingly essential for access to commerce, community, and government services, personal privacy should not be the price of living online."[23]

Cyber Spying

The government isn't the only online sleuth. Online investigation and surveillance by private actors has never been easier. A recent technological innovation allows a disgruntled spouse, for example, to secretly track all the Web pages and email that the other spouse visits.[24] In fact, this software reportedly will do much more. Spector 2.1 boasts that it "secretly takes hundreds of snapshots every hour, very much like a surveillance camera. With Spector, you will be able to see what your kids and employees have been doing online and offline."[25] Another software package from the same company, eBlaster 2.0, allows a computer user to:

McChrystal

Gleisner

Kuborn

Michael McChrystal, Marquette 1975, is a professor of law at the Marquette University Law School. **William Gleisner,** Marquette 1974, both a practicing attorney and computer consultant, maintains a law firm-based litigation support service bureau in Milwaukee. **Michael Kuborn,** Marquette 1998, is with Olsen, Kloet, Gundersen & Conway, and is trained in computer recovery and computer search and seizure techniques. Products and services mentioned in this article should not be construed as an endorsement.

"[T]rack spouse, children, or employee online activity by receiving email reports of everything they do online. eBlaster delivers detailed activity reports, including all Web sites visited, all applications run, and all keystrokes typed, right to your email address, as frequently

as every 30 minutes."[26]

Cyber spying has been around long enough[27] that it has spurred the development of defensive software intended to detect such "spyware."[28] While Spector software may not be visible to the ordinary user, it can be detected by software designed to recognize unusual text file growth, for example. The potential for mischief, however, is great because of continuing efforts to improve spyware and because the use of defensive programs is hardly ubiquitous.

Some cyber spying is clearly illegal or tortious. For example, under Wisconsin Statute section 943.70 (2)(a)(2) it is illegal to access, copy, modify, or destroy data, computer programs, or supporting documentation without authorization to do so. Under Wisconsin Statute section 895.50, tort remedies are provided for certain invasions of privacy.[29]

Notwithstanding these statutory provisions, the law's protection for online privacy remains uncertain. Part of the uncertainty is due to the requirement that privacy invasions be "highly offensive"[30] before they are actionable. What is a highly offensive invasion of online privacy is far from clear. Courts have yet to take a clear stand as to whether users must cede their privacy to the most aggressive online marketers, or, for that matter, the most paranoid family members or employers, under the rationale that constant data gathering about online activity is not highly offensive.

Legal uncertainty about the extent of online privacy also is exacerbated by the complex role of consent in the law of privacy. Generally, consent defeats any claim in tort. In online contexts, consent can be an elusive concept. For example, if an Internet user sets the computer's browser to accept cookies, is there consent to whatever cyber spying is conducted through the use of cookie files? (For a discussion of cookies, please see the article by John Barlament elsewhere in this issue.) Similarly, if a consumer visits a Web site that contains a "privacy policy" that provides a sugar-coated warning that the visitor's privacy will not be honored, has consent been granted? Does it matter whether the consumer read or expressly agreed to the policy? Case-by-case answers to these questions may substantially shape the law of online privacy, unless legislative solutions are enacted.

Another source of uncertainty in the law of online privacy, particularly related to cyber spying by employers and family members, is how ownership of the computer affects rights in the computer's use. An employer who owns a workplace computer may feel entitled to search all data on that computer, even though the computer is used by only one employee. Do the employer's property rights necessarily trump the employee's right to privacy? Similarly, will the law permit an employee to contract away, as part of the employment contract, all of the employee's privacy rights on the job? Again, these questions do not yet have clear legal answers, which is cause for concern by employers and employees alike.

Online Public Records

Paper records are expensive to maintain and difficult to access. In a paper record system, if someone in Kenya wants to research a court file in Wisconsin, they have to either buy a plane ticket and fly to the local courthouse that contains those records or hire someone locally to do the research for them. Either way, the cost can be high. Putting public records online is a cost-effective way to store information and make it available to the public. But by making public records readily accessible to all, privacy concerns increase exponentially.

Online access to public records is very different from what we have known throughout our history. Customarily, government documents have been made available by physically going to the office or repository where such documents are physically located. In addition, under the federal Freedom of Information Act[31] and its state equivalents, copies of public documents may be produced individually upon written application. Now, at Web sites such as the FBI's Freedom of Information Act "Reading

Room," we can all go and read what for many years was treated as confidential.[32]

Online government records are markedly different in effect then their paper equivalents. By allowing immediate and virtually cost-free access and the ability to locate quickly specific information through word searches, online government databases empower individuals. The trouble is, the power of information can be used for good or ill, fairly or abusively. Consider the great mass of information (much of it slanted and in error) created within our judicial system. Is it necessarily wise to allow everyone quick and easy access to information that might be private, out of context, or just plain wrong? What does the availability of information online do to the concept of what constitutes a "public figure"?[33] What about scurrilous or unfounded accusations that find their way into a court proceeding, or the results of "public" deposition testimony? Right now, the Internet is a virtual cornucopia of information for even the most amateur private investigators, whether they reside in Iowa or Iran. We need to consider seriously how much of this information should be placed online for all to see, even if the same information would be accessible by a trip to a courthouse or upon making an appropriate written request.

This is a policy discussion that should occur at the highest levels of government. An appropriate weighing of privacy concerns may not occur with decentralized decision-making about what public information should go online. The myriad offices of municipal, state, and federal government often become seamless to a researcher on the Web, because of their overlapping key words and helpful links. Until comprehensive policies are developed, decision-makers at every level of government should be cautious about placing information about private individuals online. We should not assume that online is always better.

Conclusion

Certainly, for those who feel sufficiently threatened by Web denizens or who otherwise feel a need to mask their Internet travels, there are several Web sites that offer help. For example, Anonymiser.com[34] offers to mask Web searches, block cookies, anonymously dial up to the Internet, and even encrypt URLs so that Web travels are hidden even from one's own ISP (Internet Service Provider).[35] Encryption technology can enhance online privacy as well. However, self-help technological remedies are no substitute for sound law.

At all levels of the legal system, we must do a much better job of addressing the threats to the privacy and security of information. Technological change has been proceeding at warp speed for some time. The law needs to catch up, before privacy is available only to the recluse.

Endnotes

1 Prof. Lawrence Lessig refers to the law and technology as West Coast Code (technology) and East Coast Code (law).

2 See, United States Senate Committee on the Judiciary, *Know the Rules - Use the Tools*, page 3, http://judiciary.senate.gov/privacy.htm. Online privacy relates to collecting and disseminating personally identifiable information about an individual - an affirmative act by the persons the consumer interacts with. Online security relates to the integrity of the Internet infrastructure and the system's ability to secure against the conduct of unauthorized third parties.

3 Gleisner, Kuborn, & McChrystal, *Document Destruction and Confidentiality*, 71 Wis. Law. 24 (Aug. 1998); *Invasions of Computer Privacy*, 71 Wis. Law. 25 (Oct. 1998); *Search and Seizure of Computer Data*, 71 Wis. Law. 35 (Dec. 1998); *Coping with the Legal Perils of Employee Email*, 72

Wis. Law. 10 (March 1999).

4 "What people want [but don't get online] is the same anonymity they get when they stroll through stores in a mall." http://abcnews.go.com/sections/tech/DailyNews/privacy000410.html.

5 "Engineers designing a new way to send information across the Internet want to include a unique serial number from each personal computer within every parcel of data, an idea that ... could lead to tracing of senders' identities." http://abcnews.go.com/sections/tech/DailyNews/Internet_privacy991011.html.

6 http://abcnews.go.com/onair/WorldNewsTonight/wnt000821_cyberspying_feature.html.

7 Testimony of Alan B. Davidson before the House Committee on the Judiciary, July 24, 2000, "Carnivore's Challenge to Privacy and Security Online." http://www.cdt.org/testimony/000724davidson.shtml.

8 Electronic Privacy Information Center, www.epic.org; Center for Democracy & Technology, http://www.cdt.org.

9 "Americans say they don't like to give out personal information on the Internet; however, according to a new survey, they often do." http://abcnews.go.com/sections/tech/DailyNews pewprivacystudy000821.html. *See also,* United States Senate Committee on the Judiciary, Know the Rules - Use the Tools, page 3, http://judiciary.senate.gov/privacy.htm.

10 *Katz v. United States*, 389 U.S. 347 (1967).

11 "Does Carnivore Eat Privacy Rights? FBI's email surveillance system threatens privacy rights, critics tell Congressional hearing." http://www.pcworld.com/pcwtoday/article/0,1510,17818,00.html. There is an excellent description of Carnivore and its capabilities in the Testimony of Alan B. Davidson before the House Committee on the Judiciary, July 24, 2000, "Carnivore's Challenge to Privacy and Security Online." http://www.cdt.org/testimony/000724davidson.shtml.

12 18 U.S.C. § 3123 or 50 U.S.C. §§ 1801-1811; Wis. Stat. §§ 968.34-968.36.

13 *Id.;* http://www.cdt.org/testimony/000724davidson.shtml; telephone numbers are not protected by the Fourth Amendment, see, *Smith v. Maryland*, 442 U.S. 735, 742_45 (1979).

14 *Id.*

15 *United States Telecom Ass'n et al. v. FCC*, ___F.3d ___, 2000 WL 1059852 (D.C. Cir. Aug. 15, 2000).

16 *Id.* at 2.

17 *Id.*, citing, H.R. Rep. No. 103-827, pt. 1, at 9 (1994).

18 *Id.*, citing, 47 U.S.C. § 1001(8)(C)(i), and 1002(b)(2)(A).

19 *Id.*, citing, Third Report & Order, 14 F.C.C.R., at 16819 p. 55.

20 *Id.* in section III of the opinion.

21 *Id.* at 15.

22 18 U.S.C. §§ 2510-2520; Wis. Stat. §§ 968.28-968.33.

23 *Id.*, at http://www.cdt.org/testimony/000724davidson.shtml.

24 http://www.spectorsoft.com.

25 *Id.*

26 *Id.*

27 For example, PC Spy (http://www.softdd.com/pcspy/index.htm); PC Protect (http://www.iopus.com/); and Truster Tech's Keylog (http://trustertech.com/keylog.htm).

28 E.g., http://grc.com/optout.htm.

29 Among the actionable invasions of privacy are the following:

> Intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass.
>
> Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was legitimate public interest in the matter involved, or with actual knowledge that none existed. It is not an invasion of privacy to communicate any information available to the public as a matter of public record.

30 Wis. Stat. § 895.50.

31 5 U.S.C. § 552.

32 "Pull up a chair! The [FBI's] Reading Room displays frequently requested documents released under the Freedom of Information Act," http://foia.fbi.gov/.

33 See, e.g., Maguire v. Journal Sentinel Co., 232 Wis. 2d 236 (1999).

34 http://anonymizer.com.

35 http://www.anonymizer.com/docs/faqs/url_encryption.shtml.

Wisconsin Lawyer Main

WisBar Main

Problems? Suggestions? Feedback? Email to WisBar webmaster

Disclaimer of Liability