Roland L. Trope, roland.trope@verizon.net
E. Michael Power, michael.power@gowlings.com

Lessons for Laptops from the 18th Century

As governments attempt to prevent, investigate, or prosecute crimes by persons who use the Internet to plan and carry out terrorist acts, the protection of private, personal information stored on computers becomes the subject of controversy. It is inevitable that the home computer will become a target for surveillance, search, and seizure by government agents. As a result, courts will be asked to determine whether such agents have complied with applicable laws that condition such intrusions on meeting standards set by constitutions or laws that did not anticipate the home computer as a focal point for such controversies. Courts are more accustomed to addressing similar controversies in the context of a house and its material contents, rather than a computer and its digital files. It is likely that the judicial system will use analogies to the house when deciding controversies concerning the reasonable expectations of privacy in a home computer's contents. In apparent anticipation, the US Justice Department's policy on the search and seizure of computers in investigations uses such an analogy to justify its position that when several people share a computer, any one of them can grant the police permission to search and seize its contents.[1]

However, the Justice Department's policy may need to be refined in light of the US Supreme Court's recent decision in *Georgia v. Randolph*. In *Randolph*, the Court held that a co-occupant's refusal to permit entry renders a warrantless search unreasonable and invalid as to that person.[2] The Court's justifications included its reiteration of the "centuries-old principle of respect for the privacy of the home"[3] and its view that "the home is entitled to special protection as the center of the private lives of our people."[4] Such disputes over the incursions on the right to privacy in the home will, in all likelihood, occur also over incursions on the right to privacy in the home computer—particularly laptops that can be carried and used in and out of the home and can transmit data from their hard drives to offsite or online storage sites that might or might not be entitled to the same privacy protections as data that resides on a home computer. In this article, we explore the privacy interests at stake in personal data stored on a family's home laptop computer.

Roland L. Trope
Trope and Schramm LLP

E. Michael Power
Gowling LaFleur Henderson LLP

Your home computer

Like many busy people in today's world, you probably bring work home for the evenings and weekends. Imagine that you are a museum exhibitions manager with a home computer that holds digital photos of art, correspondence with private donors and lending institutions, project budgets, and related fund raising data. This work resides "cheek by jowl" with your teenage daughter's personal emails, instant messages, and materials uploaded to her MySpace.com page.

As computing devices become lighter, wireless, convenient, and portable, you want to reclaim desk space by purchasing a laptop. The desktop's files are transferred to the laptop and you dispose of the desktop. The laptop will accompany you on vacations and on weekend trips becoming an integral part of your home—it contains many expressions of private intimacies (diaries, correspondence, on-line searches) and is held in the belief that they will, in our lifetime, remain "private." Each evening, the laptop's contents are automatically backed up to an online storage Web site, access to which is securely limited by a two-factor authentication known only to you and your husband.

Trends

This snapshot of home computer use reflects the confluence of several trends—trends so obvious that you would take them for granted in any other context. They include the following:

- the adoption of lightweight laptop computers as the primary home computer;
- the adoption of ultra high-density portable backup media and the resulting ability to transport large volumes of data;
- the decreasing effectiveness of perimeter protections for safeguarding valuable data;
- the proliferation of hard drive search engines and the resulting increase in the ease, speed, and accuracy of efforts to find and seize

About this department

With this article, *IEEE Security & Privacy* inaugurates a new department dedicated exclusively to the subject of privacy. Privacy Interests will serve as a vehicle to explore technologies, policies, practices, and developments that enhance or diminish privacy. With each issue of *S&P*, we hope to address privacy concerns that affect not only business practices but also governmental actions that influence the balance between public and private interests in the control and protection of privacy. One of our objectives will be to provide the reader with lessons learned and best practices. We have little doubt it will be a major task to meet these objectives but do hope the articles will be of interest and use to the reader.

data contained anywhere in a hard drive;
- the tendency of law enforcement agencies to include in investigations a seizure of computers and images, including file contents, Web surfing histories, and metadata;
- the adoption of technologies promising accelerated access to unlabelled data, removing an incentive to keep data well organized on digital media, and which might inadvertently generate forgotten or "orphaned" personal data;
- the increasing probability that the usual sequence in physical investigations that proceed from search to seizure will be reversed in forensic investigations of digital media—the sequence easily becoming seizure, search, and more seizure;[5] and
- the reemergence of the home as a locus of business dealings and as a repository of business correspondence and business documents.

The recent coinage of the term "home office" obscures the fact that at the time the US Constitution and Bill of Rights were written in the late 18th century many people kept business documents in their homes. They conducted business at home, because few commuted each day to an office outside their home.

In essence, the office–home dichotomy did not exist. In the succinct list of privacy protections in the US Constitution's Fourth Amendment, which opens with "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…", no mention of "offices" or any other alternatives to "houses" as repositories of "papers, and effects" appears. Businesses and shops were often a family activity. Similarly, today's home office provides a workspace for business activities as well as highly personal activities such as writing, music composition, editing family photos or videos. Most copies will be in the home computer—increasingly a laptop with portable backup media (keychain drives, CDs, backup hard discs) and online storage (to which such copies are uploaded from the home).

Seizures and the scope of the search

Returning to our scenario, imagine that you are working from home one evening and are interrupted by loud knocks on your front door. Gazing through the peephole, you see the police, demanding entry into your home. They hand you a warrant asserting the right to search your home for evidence of a crime and describing the search area as your home living room and bedrooms. One officer notices your laptop and without asking permission, moves the mouse and a full screen image appears of *Les Beaux Jours* (*The Golden Days*) by the 20th century French artist Balthus depicting an adolescent girl reclining on a chaise longue, blouse unbuttoned, admiring herself in a mirror before a blazing fire tended by a shirtless adult male. Seeing this suggestive image (and unfamiliar with Balthus), the officer suspects child pornography. Without asking permission, the officer starts to look through the files. Ignoring your objections, he searches for files with image file extensions such as .jpeg or .gif. Your years of museum work bring up more files similar to the Balthus image. Believing his suspicions now confirmed, the officer shuts down the laptop and adds it to items seized for examination.

Weeks later, law enforcement officials file a criminal indictment against you for allegedly downloading child pornography. The laptop's seizure and the hard drive's subsequent bitstream image or mirror image become the battleground: if the seizure is a violation of your rights under the Fourth Amendment, all evidence seized from the computer might be barred from the upcoming trial.

Your "home"

Courts tend to be remarkably good at using analogies, metaphors, and redefinitions to bridge semantic gaps (between abstract terms of constitutional rights and concrete terms used to describe objects and actions, for example) to ensure that the purpose of a constitutional protection is not obscured by the advent of technologies that could not have been anticipated by the founding fathers in the US.

Judicial interpretations of the Fourth Amendment have long construed and re-defined "houses" to mean *homes*. These interpretations accord the greatest protection to home privacy, drawing "a firm line at the entrance to the house"[6] based on the view that "physical entry of the home is the chief evil against which the wording of the Fourth

Amendment is directed."[7] If government agents seek to enter a home, their invasive act requires a warrant or an exception to the warrant requirement. According to the Justice Department, "the most basic Fourth Amendment question in computer cases asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers (or other electronic storage devices) under the individual's control."[8]

With governments increasingly willing to use invasive technologies [...], the home laptop may need far greater and more sophisticated constitutional protection...

That would seem to ensure that our hypothetical family's home laptop would require a warrant before government agents could seize and search it. But unlike a search of a home for particular items, when a search of the hard drive's entire contents is authorized, the government has within its forensic grasp the entire contents of the computer, not just the images its warrant authorized it to seize. As recently noted,

> "Permitting the government to make and retain copies of our private electronic files seems inconsistent with our traditions. The idea that the government could freely generate copies of our hard drives and indefinitely retain them in government storage seems too Orwellian—and downright creepy—to be embraced as a Fourth Amendment rule."[9]

Unfortunately, consistency and predictability do not always exist when the courts review the deployment and use of new communications or surveillance technologies. For example, the Supreme Court held that a warrantless use of aerial photography for surveillance of a suspect's marijuana growing in his garden did not violate the Fourth Amendment,[10] but a warrantless use of a thermal imaging device for surveillance of a suspect's use of high intensity lamps to grow marijuana inside his home did violate the Fourth Amendment.[11]

Reasonable expectations

In most cases—particularly when addressing the potential invasion of privacy by the government's use of new surveillance technology or when a suspect relinquishes privacy by using new communications technology—courts now ask two questions:

- Did the individual's conduct reflect a "subjective expectation of privacy"?
- If so, is that expectation "one that society is prepared to recognize as 'reasonable'"?[12]

Such questions tend to leave the public with little guidance because no forum exists in which society expresses its view of whether an individual's expectation of privacy is reasonable. The courts appear more receptive to privacy claims that can characterize an activity as "within the home." Because the home is an enclosure, courts have analogized computers to enclosures and deemed the data within them as entitled to a reasonable expectation of privacy under the Fourth Amendment.[13] As the court in *United States v. Blas* noted, "[A]n individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container."[14]

In our earlier scenario, the government agents might argue that although their seizure of the computer exceeded the warrant's scope, the plain view they had of images they perceived to be pornographic justified seizure and subsequent search of the entire hard drive. They might also contend that you had waived all reasonable expectations of privacy by turning the computer's contents over to an online storage service, building on the Supreme Court's ruling that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[15] However, allowing such seizures in anything but the most exigent emergencies—such as imminent terrorist acts—would deeply erode the expectation of privacy that people need to have if they are to use computers in the typical ways illustrated by our hypothetical family.

Computer users, however, should recognize that the more their computer activities result in publication and disclosure to persons outside of their immediate families, the more they will undermine claims to a reasonable expectation of privacy for what they have published or disclosed. As the Supreme Court has observed, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[16]

Yet, computer users tend to be unaware of the extent to which their online activities constitute publication, a waiver of any reasonable expectation of privacy, and creation of a globally accessible record of actions in words, photographs, audio, and video that endure as long as the media remains readable. Unfortunately, as an appellate judge's recent dissenting opinion suggests, courts adjudicating

Fourth Amendment cases need to be keenly aware of the risks to privacy created by publication on the Internet, endurance of the publication, and its nearly universal access by law enforcement agencies:

> "In this age of increasing government surveillance, lawful and unlawful, and of the retention of all our deeds and thoughts on computers long after we may believe they have been removed, it is important that courts not grow lax in their duty to protect our right to privacy and that they remain vigilant against efforts to weaken our Fourth Amendment protections."[17]

If courts are to fully appreciate the risks that new communications and surveillance technologies pose to the home privacy protected by the Fourth Amendment, it is important for judges to recognize that the home laptop will increasingly become not merely part of the home, but among its most intimately private places, notwithstanding that it is also the transmission point for highly indiscreet publication of words and images.

A further question is whether Fourth Amendment protection should hinge on the use of laptops fortified with access controls. We would suggest that improved security is not enhanced privacy. The touchstone for courts should be, as noted by a Ninth Circuit Court judge, that "for most people, their computers are their most private spaces."[18]

A related issue is the use of encryption on laptops and government efforts to compel users to disclose their keys. That topic raises a series of questions, many of which relate to the Fifth Amendment and an individual's rights against self-incrimination, which we will address in a future column.

New considerations

In grappling with new technology, we anticipate that courts will distinguish between the expectations of privacy for a "home" laptop owned by individuals and one issued by an employer. Similarly, we anticipate the government will claim that once a laptop leaves the home it ceases to have the highest expectation of privacy. But few could make any reasonable use of a home computer if they could not trust that society and its courts would recognize the contents as entitled to a reasonable expectation of privacy.

In that sense, the reemergence of the home as a repository for business records is not so different from the 18th century home at the time the Fourth Amendment was written. We can only wonder, however, whether courts will accord the same privacy protection to data backed up from home laptops to online storage sites. Will those offsite repositories be recognized as entitled to a reasonable expectation of privacy or be viewed as deliberate exposures to the public that deprive such data of privacy protections?

In light of anticipated trends, we would suggest that the courts may recognize that the less privacy protection afforded to one's home laptop computer, the less freely one can explore thoughts, express feelings and confide in family and friends. With governments increasingly willing to use invasive technologies that seize and search without discrimination, the home laptop may need far greater and more sophisticated constitutional protection than courts might previously have envisaged. As a Canadian judge recently noted, "retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectation of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected…"[19] Privacy interests are easily viewed as expendable when challenged by a government's efforts to protect the security of its citizens, but that is precisely the time when the courts need to ensure that privacy interests do not receive short shrift because pursuit of security is seldom improved by a disregard of privacy interests.

References

1. US Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002, p. 14; www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm.
2. *Georgia v. Randolph*, no. 04-1067, 22 March 2006.
3. *Georgia v. Randolph*, quoting *Wilson v. Layne*, *US Reports*, vol. 526, 1999, p. 610.
4. *Georgia v. Randolph*, quoting *Minnesota v. Carter*, *US Reports,* vol. 525, 1998, p. 99.
5. O.S. Kerr, "Searches and Seizures in a Digital World," *Harvard Law Rev.*, vol. 119, no. 2, 2005, p. 531.
6. *Payton v. New York*, *US Reports*, vol. 445, 1980, p. 573.
7. *United States v. United States District Court*, *US Reports*, vol. 407, 1972, p. 313.
8. US Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002, p. 8.
9. O.S. Kerr, "Searches and Seizures in a Digital World," *Harvard Law Rev.*, vol. 119, 2005, p. 560.
10. *California v. Ciraolo*, *US Reports*, vol. 476, 1980, p. 207.
11. *United States v. Kyllo*, *US Reports*, vol. 533, 2001, p. 27.
12. *Katz v. United States*, *US Reports*, vol. 389, 1967, p. 361, (Justice Harlan, concurring).
13. *United States v. Barth*, *Federal Supplement, 2nd Series*, vol. 26, 1998, pp. 936–37.

14. *United States v. Blas*, no. 90-CR-162, 4 December 1990, p. 21 (US District Court for the Eastern District of Wis.).
15. *Smith v. Maryland*, *US Reports*, vol. 442, 1979, p. 745.
16. *Katz v. United States*, *US Reports*, vol. 389, 1967, p. 347.
17. *United States v. Gourde*, *Federal Reporter, 3rd Series*, vol. 440, 2006, p. 2382 (Justice Reinhardt, dissenting, US Court of Appeals for the Ninth Circuit).
18. *United States v. Gourde*, *Federal Reporter, 3rd Series*, vol. 440, 2006, p. 2376 (Justice Kleinfeld, dissenting, US Court of Appeals for the Ninth Circuit).
19. *Jainarine Somwar v. McDonald's Restaurants of Canada Limited*, *E-Business, Privacy & Technology Law Journal*, Ontario Superior Court of Justice, 2006, p. 5.

Roland L. Trope *is a partner in the New York City office of Trope and Schramm LLP and an adjunct professor in the Department of Law at the US Military Academy. He provides strategic and legal advice on mergers and acquisitions, export and defense trade controls, trade sanctions, anti-money laundering, personal data protection, information security, intellectual property, cyberspace law, and defense procurements. Trope has a BA in political science from the University of Southern California, a BA and an MA in English language and literature from Oxford University, and a JD from Yale Law School. He coauthored the treatise* Checkpoints in Cyberspace: Best Practices for Averting Liability in Cross-Border Transactions *(American Bar Association, 2005). Contact him at roland.trope@verizon.net.*

E. Michael Power *is a partner in the Ottawa, Canada, office of Gowling LaFleur Henderson LLP, where he provides strategies and legal advice on technology, privacy, regulatory, and information management issues. He has a BA, an LLB, and an MBA from Dalhousie University, Canada. Power and Trope recently coauthored* Sailing in Dangerous Waters: A Director's Guide to Data Governance *(American Bar Association, 2005). Contact him at michael.power@gowlings.com.*