



We're Watching: Why We Must Design Privacy Protections into Our Systems

by Ray Bernard, PSP

A growing convergence effect that should give each one of us significant pause is *the fading of privacy*. There are three good reasons for us to pay attention to privacy issues. First: we, personally, are not immune to privacy violations. Second: we, as security practitioners and members of the security industry, are designing, manufacturing, installing and operating systems that lessen privacy. I am sure that among the thirty-thousand plus readers of this magazine, there are some knowledgeable privacy advocates. The rest of us, however, have a third reason to pay attention: we, personally and professionally, are much more uninformed about privacy issues than we realize we are. That makes us, our systems, and ultimately our customers more vulnerable than they should be. And that result is directly opposed to our purpose as security professionals.

Current Legislation

Corporate disregard for privacy concerns in the handling of personal information has led to legislation to protect corporate customers from the devastating results of identity theft and other information abuses resulting from disclosure of personal information. Legislation typically provides significant penalties for companies that don't effectively implement safeguards. One well-known state law is California's Senate Bill 1386. This law states, "Any customer injured by a violation of this title may institute a civil action to recover damages."

Since 2001 the State of California has enacted 49 privacy laws. One of those laws prohibits the improper use of electronic surveillance equipment by rental car companies (Assembly Bill 2840). The bill defines Electronic Surveillance Technology (EST) as a technological method or system used to observe, monitor or collect information such as telematics, Global Positioning System (GPS), wireless technology, and location-based technologies. Another law (Assembly Bill 2840) prohibits the use of "black box" event data recorders in vehicles without explicit disclosure, forbids the release of data outside of the original scope and purpose, and forbids the release of identifying information when sharing data with vehicle safety organizations.

The common denominator in these laws is that they forbid using any means of electronic surveillance for other than the originally intended—and customer-accepted—purpose. Manufacturers and service companies dislike such legislation because of the high cost of retrofitting privacy controls into their physical and electronic systems, as well as in their administrative systems.

Communication and computer lawyer, and highly respected privacy scholar, Ann Wells Branscomb told *CIO* magazine:

Historically, our concern about computers was Big Brother -- the government invading our lives and having too much knowledge about and control over what we're doing. Now we're discovering that big business is the real Big Brother.¹

Fred H. Cate, Distinguished Professor and Director, Center for Applied Cybersecurity Research, wrote:

"Privacy" is among the most hotly debated topics in Washington and other national capitals today. Almost 1,000 of the 7,945 bills introduced in the 104th Congress [1995-1996] addressed some privacy issue, and this level of political activity is reflected throughout much of the world...²

After a decade of increasing activity in privacy legislation, minimal foresight is required to realize that designing privacy controls into systems initially will be far less costly than waiting for legislation to require their retrofit.

Privacy Pendulum

Robert Ellis Smith is the publisher of the Privacy Journal (www.privacyjournal.net), the oldest and most authoritative publication on privacy in the world. He is also the author of a number of books about privacy, including a 387-page book, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. This book chronicles the state of privacy and surveillance and how they relate to living conditions and community values, beginning with the Puritan settlements in New England in 1582 and continuing up to the present time.

Some degree of watchfulness is needed (i.e. surveillance) in a free society, in order to guard against criminal actions and criminal individuals and groups. Since the times of the early settlers in North America, there have been neighborhood watches and constables and private security under one name or another. There has also been an ongoing tug-of-war between the conflicting objectives of privacy and security, usually with people being willing to relinquish some degree of privacy to obtain some additional measure of security and safety.

Where institutionalized compromises to privacy have grown to extend beyond their intended bounds or purposes or have outlived their usefulness, there have been backlashes whereby the individuals affected have re-exerted their privacy rights and either put controls into place or abolished or abandoned the infringing system. The privacy interest pendulum has swung back and forth depending upon the current threats to security and the current dangers of lowered privacy.

The Role of Technology

The greatest violations of privacy in recent centuries have been those enabled by technology. As Smith states in *Ben Franklin's Website*:

"Each time when there was renewed interest in protecting privacy it was in reaction to new technology. First, in the years before 1890, came cameras, telephones, and high-speed

¹ Ann Wells Branscomb interviewed in CIO magazine, February 15, 1996
<http://www.cio.com/archive/cio_021596_qa.html>.

² Fred H. Cate, *Privacy in the Information Age*, Brookings Institution Press, Washington, D.C., 1997

publishing; second, around 1970, came the development of computers; and third, in the late 1990s, the coming of personal computers and the World Wide Web brought renewed interest in this subject. In each case, the rhetoric had similar sounds to it. What worried people was not so much the technology; what worried them was that it was in the hands of large and powerful organizations.

“The coming of personal computers and the Internet has changed the equation in significant ways. In this new era, individuals and small organizations have gained cyberpower that seems comparable to what large organizations can effectively manage. A solitary individual can now publish a news periodical and reach as many readers as his or her content warrants. A solitary individual now possesses the technical wherewithal to intrude into another’s business, to keep information on other persons, and even to alter the content of information in the computer systems of large organizations. Individuals, like large organizations, can now snoop into the private activities of others and record them on audio or video tape.”³

There would be little objection to the recording of audio, video and travel information for security purposes if it weren’t for the potential misuse of such recordings. In just the past few years technology has not only lowered the cost and increased the capabilities for making recordings, information technology has greatly increased the capabilities for large scale aggregation and misuse of the recorded information in both individual and organizational hands.

A central privacy issue is the right of individuals to protect their ability to selectively reveal information about themselves, and to ensure that the use of that information does not extend beyond what their permissions have granted.

In April of 2000 Gartner, Inc. released a report titled, “Universal Surveillance vs. Personal Privacy,”⁴ which concludes:

“Emerging technologies for capturing and analyzing personal information are intensifying the debate regarding where enhanced security and service start to infringe on personal privacy.

“A number of technological forces are converging to create an unprecedented ability for enterprises to collect and analyze information. The ubiquitous connectivity of the Internet, the massive amounts of available data (e.g., from supermarket checkouts and security cameras), along with improvements in pattern recognition technologies such as data mining and face recognition are all combining to create an environment where enterprises can learn more about their customers and employees than many individuals would feel comfortable sharing.”

Our Roles

As creators, purveyors and users of this technology we must ask ourselves, why are we producing and implementing such technology without incorporating sufficient controls to assure privacy violations are either not possible or not practical? If we don’t provide the means of such

³ Robert Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Privacy Journal, Providence, RI, 2000

⁴ Jackie Fenn and Vic Wheatman, “Universal Surveillance vs. Personal Privacy”, Gartner, Inc., http://www3.gartner.com/DisplayDocument?doc_cd=105583

control on our own, history shows that legislation will force us to do so sooner or later, and with restrictions and penalties put in place that would otherwise not need to exist.

Lawyers are already paying close attention. For example, prominent attorney Senator John Edwards of North Carolina called for a bipartisan commission to examine how surveillance technologies affect privacy. In a related press release announcement Edwards said that since September 11 the F.B.I. and local police departments “have increased experimentation with video and Internet surveillance, X-ray screening, facial identification and other investigative tools.” One example he cited was a telephone-booth-sized X-ray scanner at Orlando International Airport in Florida that was “the equivalent of an electronic strip search, revealing the naked body along with any concealed weapons.” Edwards pointed out that a simple programming change could scramble images of body parts but still reveal concealed weapons.⁵ The *Tech Law Journal* made note of the press release that day, in a daily email alert and in a permanent posting on its website.⁶

When a lawyer can be one of the first people to point out a simple privacy-respecting design solution, it is obvious that we’re simply not giving privacy issues the attention that our customers (and their customers) deserve. It’s time for us to become part of the solution, rather than remaining part of the problem.

Security Monitoring “Consumers”

Most privacy legislation falls under the heading of “consumer protection”, designed to protect the rights of customers.

What’s different about the security industry is that the privacy rights of its customers—the purchasers and operators of security systems—are not the rights that are in jeopardy. It is the security customers’ employees, tenants, or customers whose privacy rights are at issue. Especially with regard to access control, they are the largest body of “consumers” of the security services provided by our systems.

A primary reason why people tolerate monitoring is the assertion put forth by the Security Industry Association’s President, Richard Chase, who issued a statement titled, “Redefining the Public Safety v. Privacy Debate.” Chase said the main point about surveillance technology is, “It is designed to watch out for you . . . not to watch you.” Certainly that applies to the majority of subjects recorded by monitoring systems. For example, we know that ATM cameras make our transactions safer by deterring robbers.

People also tolerate monitoring when it is being performed for the protection of physical or electronic assets critical to their organization’s operation. Regarding information systems, Gartner estimates that 70 percent of security incidents involve insiders, and the FBI reports that 70 percent of security incidents are internal.⁷ Ultimately protecting against such incidents benefits the larger community of security consumers.

⁵ Press Release of Senator John Edwards, <http://edwards.senate.gov/~edwards/press/2002/0801b-pr.html>

⁶ Tech Law Journal Daily E-Mail Alert, <http://www.techlawjournal.com/alert/2002/08/07.asp>

⁷ Richard Williams, “I Thought my Network was Secure!”, *Technical Support* magazine, September 2003, Technical Enterprises, Inc.

Complaints arise from security consumers when monitoring practices violate the Fair Information Practices, introduced into U.S. law by The Privacy Act of 1974⁸, and further defined by the Organisation for Economic Cooperation and Development (OECD) in 1980 in its guidelines governing “the protection of privacy and transborder flows of personal data”⁹.

- **Openness and transparency:** There should be no secret record keeping. This includes both the publication of the existence of such collections, as well as their contents.
- **Individual participation:** The subject of a record should be able to see and correct the record.
- **Purpose Specification:** The purposes for which personal data are collected should be specified.
- **Collection limitation:** Data collection should be proportional and not excessive compared to the purpose of the collection, and should include the consent of the individual.
- **Data quality:** Data should be relevant to the purposes for which they are collected and should be kept up to date.
- **Purpose Specification:**
- **Use limitation:** Data should only be used for their specific purpose by authorized personnel.
- **Reasonable security:** Adequate security safeguards should be put in place, according to the sensitivity of the data collected.
- **Accountability:** Record keepers must be accountable for compliance with the other principles.

These principles were codified into U.S. law 30 years ago, a time that predates the general use of computers, networks and information technology in security systems. Since that time there has been an increasing adoption of information technology in security systems, without a corresponding adoption of security principles in system design and deployment.

There has been a corresponding increase in privacy concerns by individuals, however. This was evidenced by the results of two Google searches on November 3, 2004:

Topic	Number of Pages Found	Exact Search Term
RFID	2,850,000	RFID
RFID and Privacy	1,240,000	+RFID +privacy

43.5% of the Web’s pages about RFID technology contain discussions or references to privacy concerns.

Designing for Privacy

With regard to security monitoring systems, privacy designs need to be incorporated at several levels:

⁸ The Privacy Act of 1974, <http://www.usdoj.gov/04foia/privstat.htm>

⁹ “Organisation for Economic Cooperation and Development guidelines”, downloadable from <http://www.privacy.gov.au/publications/ocedgls.doc>

- Design and of technology and systems (manufacturers)
- Strategy and design for technology and systems deployment (designers and integrators)
- Administration and system operations (system owners and operators)

Manufacturers

Jerry Cordasco is the Vice President and General Manager of Compass Technologies, Inc, a Wheelock Company that designs, manufactures and supports forward-thinking Access Control and Security Management systems. “Privacy is important at many levels. For example, our access control systems (and those from several other companies) contain a feature whereby the location of a person inside a facility can be tracked. Our customers have told us that their executives and senior management do not want to have their locations tracked and viewed by security monitoring personnel, so our software provides the capability to exclude specific individuals from tracking.”

Cordasco is active in the National Fire Protection Association (NFPA), and has an extensive background in fire and life safety systems and has a strong interest in integrating access control information with fire systems for life safety purposes. “There is tremendous potential in the utilization of access control system information for use by emergency first responders, especially with regard to building evacuation”, explains Cordasco. “What if the occupants of a particular floor are congregated in a large conference room? The typical fire evacuation instructions to ‘proceed to the nearest exit’ may not be appropriate, if the single nearest exit cannot accommodate the entire crowd. Several exits may be needed for safe and timely evacuation. However, tracking the whereabouts of every individual has privacy implications. Among other things, it means that you must restrict who can access the information and under what circumstances. These are the kinds of issues that all security system manufacturers should be considering.”

Information system audit trails are commonplace in the IT world, but access control manufacturers typically include minimal or no audit trail capabilities in their products, despite the fact that doing so is technically simple. A security system without an advanced audit trail capability is not fully secure. If one of the security personnel temporarily changed the access privilege for a friend to allow prohibited access, and then changed it back again, how would you know what happened? You would if the audit trail included what data values were changed (i.e. the “before” and “after” values). This would also provide support for the Data Quality, Security and Accountability principles of fair information practices.

Encryption of system information is important, especially for data that is transmitted over an Ethernet local or wide area network. There are still some access control manufacturers with systems whose IP-based access commands and transaction records, as well as report data, are not encrypted when sent over an Ethernet network. Not only can the transmission of human readable data violate privacy considerations, the lack of encryption is also a security vulnerability. Thus end users would be wise to verify the use of encryption on any systems deployed over an Ethernet network.

Designers and Integrators

There are four current trends that have privacy implications for security system designers and integrators:

- use of biometrics in security systems.
- integration of physical access control systems with HR personnel systems and IT identity management systems
- use of a common card for physical, IT and financial transactions
- use of security technology for operations purposes (such as remote video monitoring of warehouse operations)

Biometrics

The National Science and Technology Council (NSTC) was established by Presidential *Executive Order 12881* on November 23, 1993. This Cabinet-level Council is the principal means for the President to coordinate science, space, and technology to coordinate the diverse parts of the Federal research and development enterprise. The President chairs the NSTC. The NSTC has an *Interagency Working Group on Biometrics*, which has established a *Social/Legal/Privacy Subgroup* to develop and provide resources that enable federal agencies, and others, to better integrate social/legal/privacy analysis throughout a biometric system life cycle. In a presentation for the 2004 Biometric Consortium Conference, Peter Sand, the director of privacy technology at the U.S. Department of Homeland Security (DHS), stated that with regard to biometrics, the social/legal/privacy aspects are ever changing (laws, values, public perceptions, etc.) and that a “one-size-fits-all” privacy analysis for a specific technology or application is not possible. Instead, each application requires focusing on the questions and issues at hand in an individual analysis.

IT and HR Integration

Due to legislation like Sarbanes-Oxley and SB1386, IT departments are undertaking massive programs to revise their database designs to incorporate privacy and governance attributes that can be used to identify the data records and data fields that are subject to legislative requirements. This will allow rules-based management of data systems to accomplish compliance with legislation, including providing audit trail evidence that all data has been accessed in accordance with the restrictions and policies that apply. Even if only for their self-protection, security systems integrators and their customers need to be aware of what data their systems “touch” when they perform integrations to HR or IT systems, especially if they import data into the security systems. Just because the data is not subject to restrictions at the time of integration, doesn’t mean that it will always remain that way.

Common Cards

Where smart cards are used for both security and financial applications, care should be taken that identifiers used in the security systems are not the same identifiers used for financial transactions, or the security system data may also be subject to legislation-based privacy restrictions. This is an issue that warrants close examination given the import of current and pending legislation.

Video Surveillance Systems

When video systems are made available for operations use, especially when IP based systems are placed on the corporate business network, security management may lose control over who can access the systems and for what purpose. The security planning for the deployment of video systems should include a privacy evaluation element. Systems Integrators must be prepared to address privacy issues in their recommendations for system deployment.

Privacy with regard to both video and data systems was a topic discussed in several sessions at a recent educational conference produced by the Kansas City Chapter of ASIS International, “When Worlds Collide: The Physical/Logical Security Dilemma.” (This author was honored to be one of the conference speakers.) This was an event in which honest facts replaced hype, and practical experience replaced theorizing. In this author’s experience that kind of value is rare when it comes to convergence issue coverage.

One of the conference presenters was Charlie Pierce, widely regarded as foremost authority in CCTV training and design, is the President and founder of *LeapFrog Training & Consulting*. A 30-year security industry veteran, Piece is known throughout the world for his dedication to the CCTV security industry.

An example of this candor typical of the Kansas City conference was the closing remarks of Charlie Pierce in his session about IP-based cameras. “Fifty years ago, you could go about your daily business, to work and back, shopping, and maybe out to a restaurant, and your image would be recorded on a camera perhaps once every two or three months. Twenty-five years ago, that was once every two or three days. Five years ago, it was once or twice a day. Today it’s five times per day. In five years, it will be 50 times per day. And we [security practitioners] are the ones who are doing it.”

Charlie’s concluding message: “Please, when you are designing your systems ... stay professional. Remember, more times than not, shutting and locking the door is the best approach. Cameras have their positions, but privacy is the greatest thing that we have and we are giving it up camera by camera by camera.”

In addition to general advice, the LeapFrog Training & Consulting website contains specific suggestions with regard to the problem of keeping a security officer from using a pan-tilt-zoom camera in ways that violate privacy, including the use of Privacy Blocking or Privacy Zone features of some CCTV systems¹⁰.

End Users

End users have two aspects of system operations to be concerned about with regard to privacy: establishing policies and procedures compliant with applicable fair information practices, and using technology and human resources to see that the policies and procedures stay in place. Disclosure should include the extent of monitoring and recording (schedules and locations), the purpose and nature of the recordings (for example, if license plate information is captured visually or otherwise), the data retention policy, and at least a mention of the security and accountability practices in use. Destruction of data, if not automatic as part of the system design, should be witnessed and documented in a signed log entry. Similarly, the issuance of any data should be recorded in a signed log entry, whether for organizational or local law enforcement usage.

Security personnel training should include education regarding privacy issues, including the use of “social engineering” to obtaining information. This author once witnessed a man give a \$20

¹⁰ Charlie Pierce, Article #31, “Peeping Tom ... Can't Work Here!”, http://www.ltctrainingcntr.com/Technical%20Library/Peeping_Tom_Cant_Work_Here.htm

bill to a security officer, stating that it had been dropped by a person who parked nearby in the parking structure. The guard then used the license plate number to look up the employee in the access control system, and invited her to come down to retrieve the \$20 bill. It was simply a scam to obtain the lady's name and to get a closer look at her as she came into the lobby. The man was not an employee of the company and had no business being in the building.

Final Comment

Security is very much about trade-offs. Sometimes we accept a little less convenience for more security, and sometimes we trade more convenience for a little less security. What we do depends upon the security problems or threats that exist at the particular time of the decision, or upon our current perception or estimation of the risks involved. Some privacy advocates reprimand people (who would trade less privacy for more security) for “selling away their rights”. This author believes these statements to be a take-off on Benjamin Franklin's words, “They that can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.” Giving up “essential liberty” and giving up “a little bit of privacy” is not the same thing. First of all, the right to privacy (as discussed here) means the right to determine under what conditions and to whom personal information is released. Releasing information is not a giving up of that right, it is an exercising of that right.

Privacy involves the establishment of safeguards so that when information is released (or its collection is permitted), the information stays within the bounds intended. That's the main point of this article. When people allow us (the security practitioners) to establish the monitoring and recording of their activities, and the accumulation of their personal data, they do so trusting that the information will be used solely as intended—to provide them with increased safety and security. Let's be worthy of that trust by establishing privacy safeguards in the systems that we manufacture, install and operate.

About the Author

Ray Bernard is board-certified as a Physical Security Professional (PSP) by ASIS International. Ray is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides high-security consulting services for public and private facilities. Ray is a technical consultant and writer who has provided pivotal direction and technical advice in the security and building automation industries for more than 17 years. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788.

Read the latest articles in Security Technology & Design magazine at:
<http://www.securityinfowatch.com/cover/security-technology-design/2SIW>
