

Privacy

Our Two Cents

Executive Insight Series

Jonathan G. Gossels, Pete McLaughlin, & Dick Mackey

Introduction

Privacy is an important issue for many organizations. This brief paper is intended to help you better understand the topic in its full context.

The word *privacy* has different meanings in different contexts.

Context

It can be considered an attribute of a communications channel or data store or a specific legal term. Privacy as an attribute of a communication or storage mechanism is typically accomplished through encryption. Data is encrypted as it traverses a network or is stored on a disk.

Privacy as a cultural issue relates to peoples' collective sense of independence, anonymity, and freedom from governmental or corporate monitoring (Big Brother in the book 1984 illustrates the end of the spectrum where individuals are monitored by the government at all times).

Privacy as a legal issue pertains to requirements to safeguard and limit the use of personal information. In this context, a privacy policy is a commitment to use appropriate mechanisms to protect specific confidential information. Privacy mechanisms are used to enforce an organization's privacy policies. However, privacy policies are far broader and more encompassing than the use of particular technology.

Privacy Policies

Privacy policies dictate not only that the information is technically protected but also how it is used, who can use it, how long it can be maintained, and how access to it is controlled and audited. Privacy policies govern the compartmentalization and exposure of data even within organizations. Privacy policies answer questions like: "Is the customer service department allowed to look at financial account information? And can one retailer sell your address and telephone number to another?"

In an age where more and more of our personal data is stored and processed on systems connected to the Internet, privacy policies and the effective use of organizational processes and security technology to maintain privacy are increasingly important. Medical organizations, insurance companies, financial institutions and Federal agencies need to process confidential information and protect the data they manage. Every organization deals with similar issues, albeit at a smaller scale. Like other aspects of security, the most important first step is to identify the sensitive data and define policies regarding its use, communication, storage, destruction, and audit. Only after those "business concerns" are defined can technology be used to enforce those policies.

No Easy Answers

SystemExperts is continually involved in helping organizations deal with privacy issues, whether the issues are conceptual, regulatory, or technical. We have helped many organizations rethink their applications to avoid privacy concerns, altogether (often the most practical solution to privacy problems). When that hasn't been possible, we have helped organizations define policies, design applications, and select security mechanisms to protect confidential data.

The regulatory environment is complex. Gramm-Leach-Bliley and HIPAA impose sector-specific requirements. In some cases, the requirements of these laws conflict with other statutory or regulatory requirements. For many organizations, the best course of action is to get professional help to develop a practical compliance plan. That way, every dollar is spent most effectively.

Consideration:

Here are set of important issues one should consider when dealing with privacy both in the United States and internationally.

- There is a privacy paradox. Far more effort and money is spent managing the small part of the data privacy problem. Data is often only in transit for less than a

second but it is often stored in easily accessible ways for many years. IT privacy efforts usually focus on protecting the data in transit and fail to deal with the data in storage (where the jewels are concentrated).

- Europe began tackling the issue of privacy long before the US. By the time the US passed its first privacy regulation in the 1960's, Europe had, long before, noticed and addressed the growing concern of protecting its citizens' private information.
- Within the past year, the UK passed a regulation dictating that ISPs keep "traffic data" related to their customers for up to 7 years "in case" the police needed the information for investigations. Also, the UK developed an office dedicated to registering all entities that collect personal information and private data. These two examples illustrate the cultural willingness of UK citizens to sacrifice personal

privacy and support governmental privacy regulations and laws. Even after September 11th, it would be very difficult to pass similar legislation in the United States.

- While Europe has taken a broad approach to privacy regulation, the United States has taken a sector specific approach (HIPAA, GLB, etc.). While this makes the regulations more pertinent and perhaps better for the consumer, it leads to inconsistency.
- Citizens in the United States cherish their privacy. They abhor over involvement of the government, particularly as it pertains to their privacy. The US, as a whole, is very conscious of Big Brother and if its citizens err, they will err on the side furthest from Federal involvement. While this cultural fear of excessive governmental involvement has limited the Federal government's role, most Americans don't realize that the weak-

ness and inconsistency of domestic privacy regulation overall have created a situation where their private data becomes the property of the data collector. The collector has very limited responsibilities for stewardship. This is different than the European approach where the individual retains ownership and control over his personal data and the collecting entities, by law, have a stewardship duty.

- Fact: Privacy has become an additional and significant hurdle for successfully doing business internationally. Europe and the United States do not see eye-to-eye on the issue. If you are a US company thinking about doing business in Europe, one resource is <http://canada.justice.gc.ca/en/news/nr/1998/attback2.html>.

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Network-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

Intrusion Detection and Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento
www.SystemExperts.com info@SystemExperts.com