GartnerG2

REPORT

January 2002

Privacy and Security: On a Continuum or a Collision Course?

Viewpoint

Enterprises break trust with constituents by giving private information to third parties without explicit consent.

If the third party is the government, Americans will voluntarily forfeit some individual privacy in the interest of national security.

Dynamics

- The notion of privacy ranges from complete anonymity to greater or lesser release of information selected by the individual.
- Consumers are willing to disclose some private information, but only to parties they trust to keep that information secure.
- Third parties, particularly those unknown to individuals, complicate this privacy-disclosure continuum.
- Consumers profess great fear about privacy and security, but paradoxically take little action to safeguard them, particularly online.

Predictions

- Americans' concern for their individual privacy will revert to pre-11 September levels, probably before 2003.
- High profile abuses of data gathering by public or private enterprises will cause consumer and legislative backlash.

Recommendations

- Adjust budgets for the inevitably higher costs of safeguarding consumer trust in the post-11 September environment.
- Train board and staff at all levels in the appropriate response to government requests for private information about individuals.

Dig Deeper

- Related Research from GartnerG2
- Gartner Core Research
- Methodology

Laura Behrens

"Companies must recognize the critical distinction between commercial access to information and government access to information."

Viewpoint

Enterprises, both commercial and governmental, collect a great deal of private information on the promise (implicit or explicit) that they will keep it secure. Disclosing such information to third parties without citizens' or consumers' consent breaks a fundamental trust.

Since the 11 September terrorist attacks, Congress has expanded governments' powers to gain access to individuals' private data and communications—including information held by private companies—often without the knowledge or consent of those individuals. Although Americans appear ready to voluntarily forfeit some individual privacy in the interest of national and international security, their tolerance for greater government access does not extend to commercial third parties.

U.S. law tends to focus on government access to private data and communications, but other countries take different approaches. In particular, the European Union appears to be setting and enforcing a very high standard for safeguarding personal information and communication from unauthorized use by commercial parties, one that could become the de facto mark worldwide.

Companies, especially transnationals, must be prepared for significant changes in the legal and social landscape—changes that could cast them as victim, perpetrator or unwilling facilitator of significant breaches of citizen and consumer trust.

Dynamics

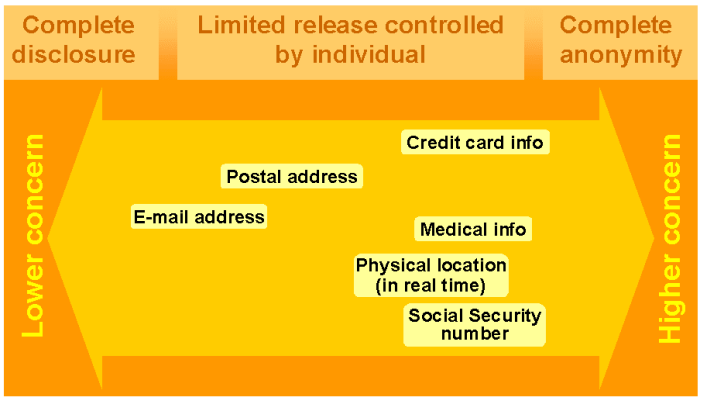
Privacy as a continuum

The notion of privacy as a continuum covers a range of conditions and behaviors from complete anonymity through the controlled release of selected information to complete disclosure. As a concept, privacy can be thought of in two pieces:

- The desire for anonymity—that my affairs are mine and no one else's…that I can do things or go places online or in the physical world without others knowing.
- The willingness to disclose limited personal information. That I might share some private information with parties I trust will keep my information secure, as in a relationship between trusted confidantes. To do this, I must satisfy myself on two dimensions before entering the relationship:
  - Motive: Do I trust this person/company to use my data only as agreed?
  - Means: Do I trust they have the ability to keep it secure?

GartnerG2 research shows as many as one-third of Americans may never do business online because they cannot get past one or both of these misgivings. The fundamental issue, however, is unrelated to the Internet—the same concerns apply to the release of paper medical records and financial information. Adequate technical security is required for an individual to give up some privacy; thus, security is not only a necessary condition, but an enabler, of privacy. "Adequate" does not necessarily mean "perfect"—an individual may give information to a less-trusted party if the value of the return is high or the number of acceptable alternatives low.

Figure 1: Privacy continuum



Source: GartnerG2, January 2002

The level of privacy any individual seeks varies according to a number of factors:

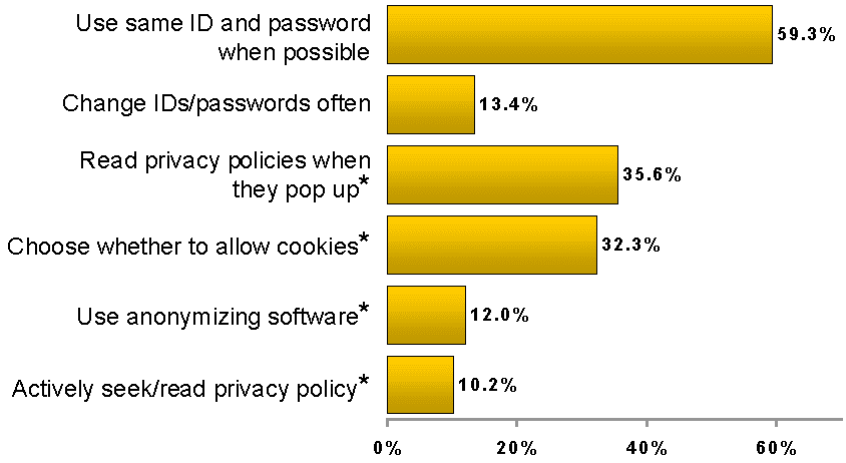
- **Sensitivity of the information.** GartnerG2 research shows consumer concern about privacy and security online, for example, breaks into three levels.
  - The highest concern is about information that would allow access to finances—credit card numbers, Social Security numbers, etc.
  - The second level applies to information that would locate a person in the physical world, such as postal address or phone number. With the growth in wireless and mobile technologies, this concern is likely to extend to physical location in real time.
  - The third level—much lower than the other two—is for information such as an e-mail address that would locate the individual only in cyberspace.
- **Consequences of loss.** If people believe a job or insurability may be at stake, they more likely want complete anonymity. On the other hand, people are more willing to let their names and addresses be shared on various mailing lists in exchange for the promise of discounts, or for the convenience of ordering from catalogs. They may not be aware of how much more than their name and address is shared by the merchant—and if they were, they might change their shopping habits.
- **Use of the information.** People distinguish between different commercial uses of their data. GartnerG2 research shows 74% of online American adults strongly disagree with the idea that failing dot-coms should be allowed to sell their customer lists to pay their debts. Yet only 38% objected as strongly to the idea that a company should have open access to customer lists when it *buys* another company.
- **Destination or path of the information.** Legal frameworks for assuring security and privacy have up to now been composed and enforced by national governments, but information flow is international. European governments are seeking to enforce their stricter standards for commercial use of data on American corporations that do business in Europe. And new U.S. laws may allow prosecution based on communications that pass through U.S.-based servers, even though senders and recipients are located elsewhere.

Do as I say

Consumers profess great fear about privacy and security, but take little action to safeguard them. In the physical world, we rarely shred the paper that could expose our credit card numbers, and we're even less careful online:

- 59% of online American adults use the same ID and password as often as they can; just 13% say they change them frequently.
- Only about one-third routinely read privacy policies even when they are intrusive (pop up) on a site, or maintain any active control over cookies.
- Only about one in 10 actually seek out a privacy policy before they will use a site, or use anonymizing software.

Figure 2: Online Americans' actions on the Web



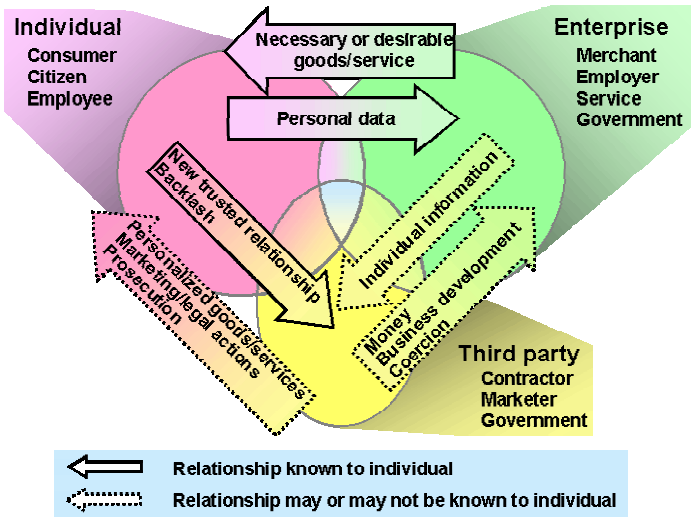
*Answered 4 or 5 on a scale on which 1 was "Never," 4 was "Frequently" and 5 was "Always."

Source: GartnerG2, January 2002

Not just a two-way street

Up to now, we have been considering privacy and security as a two-way relationship substantially under the control of individuals as citizens, consumers or workers. The events of late 2001, however, have highlighted the role of a third player.

Figure 3: Three parties to the relationship



Source: GartnerG2, January 2002

The third party to the relationship is not new. Privacy policies specify third parties that may have access to individuals' data. If consumers don't like the third parties, theoretically they can opt-out. The consequence of opting-out may be as simple as choosing to buy something elsewhere, or as onerous as changing jobs, healthcare providers or mortgage lenders. Often, individuals see these more onerous alternatives as no alternatives at all.

The collision course

The size and proportion of the overlap in the three components of Figure 3 are anything but static, and can be *unknown* to at least one of the players—most often the individual. Consumers' trust in institutions rests in some measure on their faith in privacy policies and their sense of control in the relationship. Unknown third-party relationships can jeopardize that trust. Here's why:

Virtually all privacy policies specify that personal data will be released to third parties when required by law. Since 11 September, new laws (chiefly the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act—USA PATRIOT) have greatly expanded law enforcement's ability to access personal information. For example, governments may now monitor Internet traffic—including subscriber e-mail—via a cable company Internet service provider without the knowledge or consent of the monitored parties *and* without prior permission of a court.

Enterprises are in a multiple bind here. Their information and communications could be monitored without their knowledge or consent, for example. They also can be compelled by law to give up personally identifiable information in their databases—to breach their privacy policies.

GartnerG2 research has shown American consumers to be very unforgiving of businesses that abuse the trust relationship. About 90% of online consumers, for example, say they would stop doing business with sites that give up personal information or expose credit card data. As noted before, more than one-third don't want their personal information sold along with other assets to the buyer of a business.

Recognizing the difference

This points up a critical distinction between commercial access to information and government access to information. American consumers don't want personal information and communications to be bought and sold. *Government's* interest in information is not about money. As long as consumers feel that government interest in getting information about individuals will serve the common good, they will tolerate it—even embrace it.

European countries have recognized this distinction in law. Several European countries generally allow broad government access to personal information and communications, while imposing severe limits on the business use of personally identifiable information. The European Union has codified the distinction in its EU Data Protection Directive (EUDPD), which may evolve to become the worldwide standard in this area.

How it plays out

The actions of commercial third parties are much more plentiful than those of governments, with equal or greater impact on the daily lives of individuals. In the happiest example, a third party known to and approved by the individual could use personal data to offer goods or services the individual finds valuable, leading to a new relationship that benefits all parties.

On the other extreme, imagine a prospective employer gains access to an individual's medical records and chooses not to hire after deciding the person will be expensive to insure. Such an action may or may not be legal or ethical, but if it passes unknown to the individual, it is likely to be repeated. Backlash of some kind—legal, business or both—is likely to occur if and when a pattern of such actions becomes known.

Enterprises may find themselves caught between the rock of government requests for information and the hard place of consumer outrage if privacy promises are broken. They may also face conflicting law and regulation: What does the operator of a government-funded Web site do when law enforcement demands data that would track an individual's activity on the site, even though federal rules prohibit the operator from collecting such data? Although new laws generally supercede old, enterprises must examine current policies and processes for the practical implications of the new rules and adjust accordingly. The revision requires close work not only with corporate counsel, but also with staff right down to the clerks and receptionists likely to be the first contacts with warrant-wielding investigators.

The backlash factor

We pointed out earlier that security is not only necessary for, but an enabler of, privacy. A converse proposition also holds: Undue disregard for privacy will lower collective security. This could come at very high cost to:

- Individuals, whose lives are affected, sometimes profoundly.
- To businesses that go under due to loss of customer confidence, and to those that incur higher costs to retain that confidence.
- To the economy in general, as compliance erodes and workarounds, undergrounds and black markets emerge.
- To collective security, as individuals drop out of a system they no longer trust.

Public opinion polls show that in early 2002, U.S. citizens will tolerate a relative shift toward collective security at the expense of personal privacy. The two will collide when the sharing of personal data or communications with third parties leads to wrongful accusations,

resulting in denial or limitation of privileges or services. Over time, such incidents will accumulate, eventually prompting individuals to revert to pre-11 September attitudes. Just how soon the reaction will come and how strong it will be depends on the number and nature of such incidents. Of course, further terrorist attacks or other disruptive events would reinforce public acceptance of broad government access.

Predictions

- **Americans' concern for their individual privacy will revert to pre-11 September levels, probably before 2003.** The pace will be influenced by perceived abuses of access to personal information, and conversely by perceived threats to collective security. Barring major disruptive events, overall concern for personal privacy will probably return to the levels of early 2001 by the end of 2002. People will maintain a higher tolerance for government as a third-party recipient of personal data and communications, for as long as they perceive a national security need. This tolerance does not extend to commercial third parties.
- **High-profile abuses of data gathering by third parties—public or private—will cause consumer and legislative backlash.** Although few enterprises have felt immediate commercial or investor impact even after well-publicized security lapses, an accumulation of such lapses could lead to legal or regulatory action with far-reaching consequences. The Senate Judiciary Committee convened hearings within a month of the enactment of USA PATRIOT, effectively to convey concern that the Justice Department was riding roughshod over the civil liberties of individuals. Members of Congress and several state legislatures are working on new laws to provide more safeguards for the privacy of personal information and communication on the Internet. Existing or forthcoming rules in financial services (Gramm-Leach-Bliley) and healthcare (Health Insurance Portability and Accountability Act) will put enterprises under the spotlight for compliance.
- **European data protection standards will drive much corporate policy and practice worldwide.** Organizations that meet the strict standards of the EUDPD (by signing on to the Safe Harbor Agreement or by other means) may enjoy more effective trust relationships across multiple constituencies.

Recommendations

- **Ensure that all consumer- and employee-facing policies and audits comply with fast-changing laws and regulations. Revise as needed or required, in clear language with wide distribution**. New rules may collide with old knowledge or practices, requiring constant vigilance on this point. Seek out:
  - Legal expertise.
  - Industry best-practices—technology, policy and communications.
  - The international view for the costs/benefits of complying with the EUDPD.
- **Build policy and practice on the understanding that consumers and employees consider security a necessary condition for privacy.** They will tolerate releases required by law; reassure them about what you do to prevent any other kind.

- **Communicate loud and clear about government-caused exceptions to your privacy policy.** If consumers learn you have released data (any data, not necessarily just their own), they are much more likely to forgive you if you can honestly say you were required to do so by law.
- **Adjust budgets for the inevitably higher costs of safeguarding consumer trust in the post-11 September environment.**
  - The more sensitive the information in your databases, the more you must do to protect it from those not entitled to see it, and to reassure consumers you are doing so.
  - Weigh the costs of adherence to the EUDPD against the benefits in all your markets.
- **Train board and staff at all levels in the appropriate response to government requests for private information about individuals.**
  - Board and senior executives must work closely with counsel to develop policies in line with business needs and new law enforcement powers, both in the United States and abroad.
  - Managers must devise and implement practices that carry out the policies as intended. They need a thorough understanding of the enterprise's rights and obligations when faced with requests of different natures from different agencies. Examples: A subpoena is not the same as a search warrant, and requires a different response. Employee data is held to different standards of confidentiality than customer data, depending on the industry, and a request for one does not mean you can release the other.
  - Workers "on the ground" must thoroughly understand what to do if and when they are faced with requests for more or different information than company policy allows. Complying too readily with law enforcement requests or demands could result in civil action by those whose information was released.

Dig Deeper

Related Research from GartnerG2

Report: Privacy in a Secure Setting: The Enterprise as Prudent Confidante
By Richard Trinkner (*10 January 2002))*

Report: Don't Get Blindsided by Security and Privacy Regulation
By Richard DeLotto (*04 January 2002)*

Q&A: Customer and Employee Data Post-11 September: Don't Overreact
By Laura Behrens *(19 October 2001)*

Report: Consumers Have Real Fears About Information Privacy; Deal With It
By Laura Behrens *(24 August 2001)*

Gartner Core Research

Beyond the Headlines: Privacy Issues and the Enterprise
By Arabella Hallawell *(4 May 2001)*

Summary: Information privacy concerns have attracted intense media and political attention. But how will they actually affect enterprise strategy and operations?

Methodology

Consumer survey findings are based on Gartner G2 consumer surveys conducted in 2001 with representative samples of thousands of U.S. consumers, aged 18 years and older. Results were balanced to match Census Bureau data on key demographic and socioeconomic factors, and projected to be representative of both total households and total adult population.