II. Security

The Advisory Committee also examined how to ensure the security of personal data gathered by commercial websites.

A. Competing Considerations in Computer Security

Security has often been treated as an obligation of companies that handle personal data. But security, particularly computer security, is difficult to define, particularly in a regulatory or quasiregulatory context. Identifying the most effective and efficient solution for data security is a difficult task. Security is application-specific. Different types of data warrant different levels of protection.

Security – and the resulting protection for personal data – can be set at almost any level depending on the costs one is willing to incur, not only in dollars but in inconvenience for users of the system. Security is contextual: to achieve appropriate security, security professionals typically vary the level of protection based on the value of the information on the systems, the cost of particular security measures, the costs of a security failure in terms of both liability and public confidence.

To complicate matters, both computer systems and methods of violating computer security are evolving at a rapid clip, with the result that computer security is more a *process* than a *state*. Security that was adequate yesterday is inadequate today. Anyone who sets detailed computer security standards – whether for a company, an industry, or a government body – must be prepared to revisit and revise those standards on a constant basis.

When companies address this problem, they should develop a program which is a continuous life cycle designed to meet the needs of the particular organization or industry. The cycle should begin with an assessment of risk; the establishment and implementation of a security architecture and management of policies and procedures based on the identified risk; training programs; regular audit and continuous monitoring; and periodic reassessment of risk. These essential elements can be designed to meet the unique requirements of organizations regardless of size.

In our recommendations to the FTC, we attempt to reflect this understanding of security. Our work, and this report, reflect the various types of on-line commercial sites, and the fact that they have different security needs, different resources, and different relationships with consumers. The report reflects this understanding and seeks to identify the range of different possibilities for balancing the sometimes competing considerations of security, cost, and privacy.

B. Regulating Computer Security – Preliminary Considerations.

Before turning to the options it is worthwhile to comment on several issues that the Committee considered but did not incorporate directly into its list of options.

First, we considered whether guidelines or regulations on security should contain some specific provision easing their application on smaller, start-up companies or newcomers to the online environment, but we ultimately determined that new entries should not receive special treatment when it comes to security standards. In part, this is because organizations that collect personal data have an obligation to protect that data regardless of their size. In part, this is because we concluded that any risk assessment conducted to evaluate security needs should take into account the size of the company (or, more appropriately, the size of a company's potential exposure to security breaches). In many cases (but not all), a smaller website or less well-established company will have fewer customers, less data to secure, and less need for heavy security. A smaller site may also have an easier time monitoring its exposure manually and informally. And of course, even a small site may obtain security services by careful outsourcing.

Second, we noted that several of the proposed options depend on or would be greatly advanced by inter-industry cooperation and consultation on appropriate and feasible security standards. In conjunction with the adoption of any of the proposed options, we urge the FTC or the Department of Justice to make assurances to industry members that cooperation in the development or enforcement of security standards and procedures will not result in antitrust liability.

Third, it is vital to keep in mind that companies need to protect against internal as well as external threats when considering solutions designed to secure customers' personal data. Many companies have already implemented information security policies that protect sensitive corporate data (i.e., compensation information) by limiting access to only those employees with a "need to know." Companies need to implement similar measures that protect customer data from unauthorized access, modification or theft. At the same time, mandated internal security measures can pose difficult issues. For example, it is not easy to define "unauthorized" employee access; not every company has or needs rules about which employees have authority over computer or other data systems. And many companies that have such rules amend them simply by changing their practices rather than rewriting the "rule book." Even more troubling is the possibility that internal security requirements that are driven by a fear of liability could easily become draconian – including background checks, drug testing, even polygraphs. We should not without serious consideration encourage measures that improve the privacy of consumers by reducing the privacy of employees.

Fourth, we are concerned about the risks of regulation based on a broad definition of "integrity." Some concepts of security – and some legal definitions – call for network owners to preserve the "integrity" of data. Data is typically defined as having integrity if it has not been "corrupted either maliciously or accidentally" [Computer Security Basics (O'Reilly & Associates, Inc., 1991)] or has not been "subject to unauthorized or unexpected changes" [Issue Update on Information Security and Privacy in Network Environments (Office of Technology Assessment, 1995, US GPO)]. These definitions, issued in the context of computer security rather than legal enforcement, pose problems when translated into a legal mandate. If integrity is read narrowly, as a legal matter it would focus on whether a Website has some form of protection against malicious corruption of its data by external or internal sources. If the definition is read broadly, it could lead to liability for data entry errors or other accidental distortions to the private personal information it maintains.

C. Notice and Education

After considerable discussion, the Advisory Committee has developed a wide range of possible options for setting standards for protecting personal data gathered by commercial websites. Before presenting these options, we will address two policy options that the group considered but determined were unsatisfactory on their own. While insufficient standing alone, the Advisory Committee concluded that development of programs to educate consumers on security issues and a requirement that companies post notice describing their security measures are approaches that should be examined as possible supplements to some of the options in Section D.

Notice. Notice is viewed as an appropriate tool for informing individuals about the information practices of businesses. It is critical to the consumer's ability to make informed choices in the marketplace about a company's data practices. In the area of security, as in the area of privacy, there is not necessarily meaningful correlation between the presence or absence of a security notice statement and the true quality of a Website's actual security. A security notice could be more useful if it allows consumers to compare security among sites in an understandable way. Since it is difficult to convey any useful information in a short statement dealing with a subject as complex as the nuts and bolts of security, most such notices would be confusing and convey little to the average consumer. Further, providing too many technical details about security in a security notice could serve as an invitation to hackers. (As was discussed at some length by the Advisory Committee, these considerations also mean that it is not possible to judge the adequacy of security at Websites by performing a "sweep" that focuses on the presence or absence of notices.)

Notice is important in triggering one of the few enforcement mechanisms available under existing law. If a posted notice states a policy at variance with the organization's practices, the FTC may exercise its enforcement powers by finding the organization liable for deceptive trade practices. But security notices are ineffective standing alone and should not be an option. At the same time, we believe that they could be useful in conjunction with one of the other options discussed in Section D. The form such notice should take will vary depending upon the option selected.

Consumer Education. In addition to notice, consumer education campaigns are also useful to alert consumers about security issues, including how to assess the security of a commercial site and the role of the consumer in assuring good security. Regardless of what security solutions the FTC decides to recommend, it would be extremely valuable for the FTC or industry associations to sponsor consumer education campaigns aimed at informing Internet users about what to look for in evaluating a company's security. In addition, no system is secure against the negligence of users, so consumers must be educated to take steps on their own to protect the security of their personal data.

D. Options for Setting Website Security Standards

The Advisory Committee has identified two sets of options for those seeking to set security standards. These security recommendations apply both to information in transition and information in storage. In essence, these options address two questions: How should security standards be defined? And how should they be enforced?

The question of how security standards should be defined requires consideration of the parties responsible for the definition as well as issues of the scope and degree of flexibility and changeability of the standards. The entries that could be responsible for setting security standards explicitly include government agencies, courts, and standards bodies. Furthermore, it could be left up to websites themselves to develop security programs (perhaps with a requirement that each site develop some security program), or it could be left to market forces and existing remedies to pressure websites into addressing security at an appropriate level.

In this section, we set forth five options for setting security standards that fall along a continuum from most regulatory to most laissez faire. Each of the proposals reconciles the three goals of adequate security, appropriate cost, and heightened protections for privacy in a different manner. Policy makers should consider this when selecting a course of action. For each option, we have presented the arguments deemed most persuasive by opponents and proponents of the option.

1. **Government-Established Sliding Scale of Security Standards –** Require commercial Websites that collect personal information to adhere to a sliding scale of security standards and managerial procedures in protecting individuals' personal data. This scale could specify the categories of personal data that must be protected at particular levels of security and could specify security based upon the known risks of various information systems. In the alternative or as part of the standard, there could be minimum security standards for particular types of data. The sliding scale could be developed by the FTC or another government agency and incorporate a process for receiving input from the affected businesses, the public, and other interested parties.

Proponents would argue:

1) A sliding scale allows for the matching of consumer protection risk to data source, thereby allowing companies to develop a more efficient compliance and technology infrastructure.

2) A sliding scale provides commercial flexibility in the way Websites comply with security standards.

Opponents would argue:

1) This option will embroil the FTC in trying first to gauge the sensitivity of numerous, different types of data and then to match the sensitivity with particular security measures. It is an impossible task, and the results will be a mess.

2) If the sliding scale is produced at a high level of generality, it will be unenforceable and probably incomprehensible; if it is made specific enough to enforce, it will be a straitjacket for many businesses and a series of loopholes for others.

3) Even if it could be prepared properly the first time, a sliding scale would have to be updated almost constantly, a task for which bureaucracies are ill-suited.

2. **"Appropriate Under the Circumstances"/"Standard of Care" –** Require all commercial Websites holding personal information to adopt security procedures (including managerial procedures) that are "appropriate under the circumstances." "Appropriateness" would be defined through reliance on a case-by-case adjudication to provide context-specific determinations. This standard would operate in a manner similar to that governing medical malpractice for physicians: as the state of the art evolves and changes, so does the appropriate standard of care. An administrative law judge of the FTC or another agency or a court of competent jurisdiction could adjudicate the initial challenge.

Proponents would argue:

1) This approach allows for an assessment of security tied directly to considerations of circumstance and knowledge. It is impossible to summarize in any detail the balance that must be struck between security and usability; even for the most sensitive data, such as medical information, it may be necessary to lower security standards in order to assure prompt treatment for the injured.

2) The creation of a general standard that is informed by the security practices of others similarly situated at a certain date and time allows for flexibility and growth while encouraging ongoing progress. A similar approach is found in judging medical treatment: doctors are not regulated by an elaborate rulebook but rather by the requirement that they practice medicine in accordance with accepted professional standards. The law leaves definition of those standards to the particular case.

3) This approach is designed to encourage increasingly strong security practices. If a bright line rule is adopted, there is little doubt that the pace of technical change will leave the adequacy of regulation in the dust, and what was intended to be a regulatory floor will become a ceiling in practice. Rising tides do raise all boats, except those that are anchored to the bottom.

Opponents would argue:

1) In the absence of clear minimum security standards, courts and companies will lack guidance, because there are no universally accepted security standards.

2) For consumers, the absence of any clear definition of what is sufficient security may put their personal information at risk from companies who do not share the same risk assessment about what is "appropriate under the circumstances."

3) For commercial websites, there are also disadvantages to this approach; their security precautions will not be judged until after a breach has occurred, which means that the precautions are more likely to be viewed as inadequate in hindsight.

4) An after-the-fact security standard could lead many websites to ignore security until they are sued.

3. Rely on Industry Specific Security Standards – All businesses operating online that that collect personal information could be required to adhere to security standards adopted by a particular industry or class of systems. There are three quite different options for how the standards are developed:

a. The standards could be developed by a government-authorized third party through a process that encourages public participation (notice and comment) and may include governmental review.

b. The standards could be established by any third-party but the FTC could require that the standards address specific topics (e.g. access, data integrity, notice, authentication, etc.).

c. The standards could be developed by any third-party as long as the identity of the standard-setting organization is revealed to consumers (this is in effect a security "seal" program).

Proponents would argue:

1) No government agency is smart enough or fast-moving enough to set network security standards for a particular industry. Industry-specific standards should be set by industry because each sector has different computer security needs and methodologies.

2) Industry groups will have a strong incentive to avoid setting too low a bar. Every company with a brand name is held accountable for the products sold under that name. So too with security standards-setting organizations; those that are associated with serious security breaches will lose the confidence of the public.

3) The three options presented under this heading are quite different, and c. is significantly better than the others. It associates a security standard with a "brand name" so that consumers can

decide whether security at the site is sufficient. Option b. simply adds a requirement that the standards address certain issues. In most cases this will be unnecessary and in other cases insufficient. Option a. requires that the government license standard-setting organizations; it also requires notice and comment and perhaps government review for such standards. This option is nearly indistinguishable from requiring government-written standards and will require that the FTC or some other body make hundreds if not thousands of individualized decisions about what security practices should be required in which industries, decisions that will have to be remade every three months as security standards and challenges evolve.

Opponents would argue:

1) Allowing industry to develop (and police) itself invites lax standards and under-enforcement. Self-regulatory organizations that are comprised solely of the industry at issue will not develop robust standards because doing so may subject its members to additional implementation costs and expose them to greater liability.

2) The insular nature of the standard setting process does not adequately assess and address the needs and values of other parties – other industries, the public, policy makers. In the absence of other stakeholders industry will fail to address important concerns or craft proposals that undercut other important public policies.

3) The standard setting process lacks public accountability. It is inappropriate to develop substantive policy through entities and processes that lack institutional mechanisms for ensuring public accountability and oversight.

4) Opponents will find that options a-c do not address their general concerns with industry-generated standards. However, opponents may find that proposal “a” partially responds to criticisms 1 and 2 because it constructs a process for soliciting public and policy maker input and review and to a limited extent addresses concerns about industry capture, and stakeholder participation. However, because it does not permit other stakeholders to participate in the formulation of the standards it is unlikely to fully ameliorate these concerns. In addition, the fact that the item to be protected, personal information, is likely to be considered less valuable by the business than individuals, the concern about lack of representation is heightened. Opponents may find that proposal "b" while weaker than "a" provides some restraint on the standard-setting process by allowing outside interests to decide what issues must be addressed. Option "c" will garner the greatest opposition from opponents as it fails to address any of the concerns outlined above.

4. Maintain a Security Program – Require all commercial Websites that collect personal information to develop and maintain (but not necessarily post) a security program for protecting customers’ personal data. This option could take one of two forms:

a. The contents and methodology of the security program could be specified, and businesses could be required to post a brief notice indicating their compliance.

b. The requirement could be limited to a simple mandate that the website adopt a security strategy without specifying the details or requiring that it be posted.

Proponents would argue:

1) A security program is necessary for a commercial website of any size that collects personally identifiable information and wishes to keep the information confidential.

2) The scope of the program may vary depending upon the size of the company and in the case of a very small business, one person may be able to effectively handle security on a part time basis. However, just as marketing, human resources, and accounting are considered essential business functions for companies of any size, maintaining a security program is also critical to any company's operations.

3) In support of option 4 a., security professionals believe that any effective program, even if managed by one person part time, should involve the elements of risk assessment, implementation of controls based on the risks, testing and monitoring of controls, and periodic re-assessment of risks.

4) Also in support of option 4 a., a statement that the company maintains a security program that assesses risks and implements appropriate controls to address the risks need not be incomprehensible to consumers or too burdensome for businesses to comply with and insures consumers and businesses that security has been considered in the system design.

Opponents would argue:

1) Developing and maintaining a program -- but not testing it or otherwise verifying or assuring that the organization is complying with the program -- will only result in an illusion of security.

2) The costs of developing, testing, verification, and assurance (especially to small or not technically savvy businesses) will be significant, diverting resources from the main business purpose. Many firms would not know where to turn or how to take the first step in developing such a program.

3) If the plan description is posted, much of it may both be incomprehensible to non-technical users and all-too-clear to technically savvy attackers.

5. Rely on Existing Remedies – Before requiring any particular security steps, wait to see whether existing negligence law, state attorneys general, and the pressure of the market induce Websites that collect personal information to generate their own security standards. It is worth noting that the insurance industry has started to insure risks associated with Internet security. The emergence of network security insurance may force companies to seriously address security issues, as the presence or absence of adequate security will be taken into account in the underwriting process utilized to determine rates for premium.

Proponents would argue:

1) Consumers who suffer harm as the result of negligence can typically bring tort actions. There is no reason to think that consumers who are harmed by a breach would lack a remedy for any specific injury they may suffer.

2) Damages are often quantifiable (credit card charges or lost work time due to identity theft for example). And even when they are not quantifiable (disclosure of embarrassing medical data, for example), the problem is no more difficult for juries to resolve than similar intangible wrongs routinely resolved by juries today (libel damages, for example, or "false light" claims).

3) It is therefore reasonable to wait for such litigation and to correct any gaps that may emerge in the law when and if the lack of a remedy has been demonstrated.

Opponents would argue:

1) This approach does nothing proactive to advance good practices in the marketplace, and will result in a long delay before security issues are addressed and consumers are protected. It will take some time before litigation based on existing negligence law results in judgments. And it will take time for the market to respond to this, if that even happens at all.

2) If relying on existing remedies fails to work, we will be in the same or worse position then as we are now, and many more consumers will have had their privacy violated due to security breaches.

3) In the meantime, businesses that would welcome guidance from experts may be left to flounder and face law suits because of a lack of awareness, even if they are well intentioned.

Recommendation

The great majority of the Committee believes that the best protection for the security of personal data would be achieved by combining elements from Options 2 and 4. We therefore recommend a solution that includes the following principles:

a) Each commercial website should maintain a security program that applies to personal data it has collected.

b) The elements of the security program should be specified (e.g., risk assessment, planning and implementation, internal reviews, training, reassessment).

c) The security program should be appropriate to the circumstances. This standard, which must be defined case by case, is sufficiently flexible to take into account changing security needs over time as well as the particular circumstances of the website -- including the risks it faces, the costs of protection, and the data it must protect.

E. Enforcement Options

1. **Government Enforcement Program** – The FTC or another agency could enforce compliance with standards using its current enforcement power or using newly expanded authority. The enforcement could establish civil or criminal fines, or both and other equitable remedies. (This option is, in some respects, modeled after the regulations governing the financial services industry as enforced by the Federal Financial Institution Examination Council (FFIEC). The FTC could establish a similar enforcement regime for other industries.)

2. **Third-Party Audit or Other Assurance Requirements** – Rely on independent auditors to ensure compliance with standards. This structure could require security standards to be verified by an external body and could require public disclosure of the findings. This option would provide more flexibility and could adjust faster to the changing threat environment. It would, however, introduce an additional cost and overhead that may not be justified by all industries and for all levels of risk exposure. It would, on the other hand, introduce a neutral, objective assessment of a company's security infrastructure relative to its industry.

3. **Create Express Private Cause of Action** – Congress could establish a private right of action enabling consumers to recoup damages (actual, statutory, or liquidated) when a company fails to abide by the security standard established through one of the options set out in Section I.

4. **Rely on Existing Enforcement Options** – Many of the options include the publication of the website's security procedures or its adherence to particular standards. Such postings are subject to traditional FTC enforcement if the statements are false. It is also of course possible for consumers to bring their own actions for fraud, false statements, or underlying negligence in the handling of the data.