BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

The FTC Offers Some Guidance, but Leaves Open Questions

BY ANDREW B. SERWIN

In 2007 the Federal Trade Commission issued two key pieces of guidance, ''Protecting Personal Information: A Guide for Business,'' and ''Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles.'' While neither is binding on businesses, they offer key insights into current FTC thinking, and will shape the discussion of privacy and security issues.

The FTC's New Guidelines on Protecting Personal Information

''Protecting Personal Information: A Guide for Business''[1] is based upon five key principles:

- Take stock.
- Scale down.
- Lock it.
- Pitch it.
- Plan ahead.

While not directly tied to any particular statute or legal requirement, these principles offer companies helpful guidance as they attempt to navigate compliance with the numerous information security and privacy requirements that are now imposed. Furthermore, they certainly offer some insight into what the FTC might consider an ''unfair'' business practice in the information security and privacy arena—which has become a theory the FTC has used in several enforcement matters.[2]

Take stock.

This principle is the starting point of the guidance and it focuses on an important factor—assessing what information your company collects. It also includes analyzing how information flows occur in your company, so that a true assessment of security can occur after this information is gathered. This includes doing a hardware inventory of all systems that store sensitive data, tracking personal information by talking with those that have access to the information, including sales and marketing, IT, HR, accounting, as well as others, including third-parties that access sensitive data.

Taking stock also includes assessing: who sends personal information to your business; how your business

[1] Located at http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf, last visited Jan. 9, 2008.

Andrew B. Serwin is a partner with Foley & Lardner LLP, San Diego, and is the author of Information Security and Privacy: A Practical Guide to Federal, State and International Law (West 2007), and the Internet Marketing Law Handbook (West 2007). His practice includes advising companies regarding information security and privacy matters. Serwin may be reached at (619) 685-6428 or aserwin@foley.com.

[2] *See, e.g., In the Matter of BJ's Wholesale Club Inc.* Links to case documents, including complaints and the consent agreement, are available at http://www.ftc.gov/os/caselist/0423160/0423160.shtm.

 ISSN 1538-3423

receives personal information; what kind of information is collected at each collection point; where is the information stored; and who has access, or could have access to the information.

Given the value to identity thieves, the FTC recommends paying particular attention to Social Security numbers, credit card or financial information, or other sensitive information.

Scale down.

This principle focuses on reducing your company's data footprint. The FTC recommends not keeping, or even collecting, data where there is no legitimate business reason to do so. In addition to the reasons identified by the FTC, reducing your company's data footprint also in many cases will reduce the number of laws you are subject to, thereby reducing the compliance burdens.

The FTC recommends only collecting Social Security numbers for lawful purposes, such as paying employee taxes, but not using them as an employee or customer identification number.

Lock it.

The FTC also recommends properly securing sensitive personally identifiable information. Though electronic breaches get significant attention, the FTC correctly notes that many data losses occur with paper records.

Paying attention to physical security can help solve these issues. Locking away media, paper or electronic, that contains personally identifiable information is recommended. Having protocols to ensure that employees put sensitive information away at appropriate times, including at the end of a work day, is also recommended, as is implementing appropriate access controls to your physical environment. Limiting access to offsite storage and encrypting information when it is transported is also recommended.

Electronic, or technical, security is also covered by this guide. Identifying the servers or other areas where sensitive electronic information is stored is recommended, as is doing a vulnerability analysis of systems and connections, particularly against common attacks is also recommended. If possible, storing sensitive information on a computer that is not connected to the Internet is identified as a step to take to secure information, as is encrypting information that is sent to a third-party over a public network, or stored on removable media or a computer network. The FTC also suggests that thought be given to encrypting e-mails where sensitive information is sent. Doing due diligence on your computer systems is also recommended. Scanning for vulnerabilities, and closing unnecessary ports is identified by the FTC, as is using secure socket layer (SSL) encryption when transmitting credit card information or other financial information. Having adequate password management is identified as an important factor, as is providing training to employees regarding potentially fraudulent activities, and steps they can take to secure information. This includes running background checks on employees that will have access to sensitive information and making employees sign a policy stating that they will follow your company's policies. Assessing which employees have access to sensitive data is also recommended.

Restrictions on devices with removable media, including limiting the use of laptops, and the type of data that is stored on them, is also an FTC recommendation.

The FTC suggests that companies consider using an intrusion detection system, and maintain a central log of security-related information so that monitoring and spotting suspicious activities is facilitated.

Investigating the security practices of third-parties who receive sensitive information is also recommended by the FTC.

Pitch it.

This principle focuses on data destruction. Not surprisingly, the FTC recommends that reasonable appropriate data destruction regimes be put in place, because the failure to destroy data can facilitate identity theft. This may include shredding of paper records, as well as wiping electronic devices. Making sure that employees who work remotely follow these policies is also important. The FTC does note that the type of regime put in place depends upon the type of data, as well as other factors.

Plan ahead.

The FTC suggests that a company have an incident response plan in place before a security breach happens. It recommends that companies immediately disconnect a compromised computer from the Internet, and that investigations into security incidents start immediately. Planning out notification, both from an internal and external perspective, is also suggested.

The FTC's Online Behavioral Advertising Guidance

Demonstrating the importance of information security and privacy to the FTC, in connection with its approval of the Google/DoubleClick merger, the FTC recently issued guidance regarding online behavior advertising, the *Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles*. The FTC both defined what the practice is, and identified 5 key principles regarding the practice.[3] According to the FTC, online ''behavioral advertising'' means the tracking of a consumer's activities online, including the searches the consumer has conducted, the web pages visited, and the content viewed in order to deliver advertising targeted to the individual consumer's interests.[4] The five key principles identified by the FTC are:

- Transparency and consumer control;
- Reasonable security, and limited retention for consumer data;
- Affirmative express consent for material changes to existing privacy promises;
- Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising; and
- Using tracking data for purposes other than behavioral advertising (though this is a call for additional information).[5]

[3] *See Online Behavioral Advertising Moving the Discussion Forward to Possible Self-Regulatory Principles,* http://www.ftc.gov/os/2007/12/P859900stmt.pdf, last visited Dec. 24, 2007.

[4] *Id.*

[5] *Id.*

  PVLR ISSN 1538-3423

The FTC did not simply prohibit behavioral advertising because the FTC is seeking to balance support for such innovation with the need to protect against harms to consumers' privacy. Indeed, the FTC specifically noted that while behavioral advertising provides benefits to consumers, including in the form of free web content and personalized advertisements that consumers value, behavioral marketing is considered by some to be largely invisible and unknown to consumers.[6] The FTC noted other issues with consumers, including a lack of understanding of this type of marketing, as well as information security concerns related to harm to consumers if the data fell into the wrong hands. As a result, the FTC proposed the five principles noted above, and provided some guidance for businesses as they attempt to implement these principles via self-regulation.

Principle 1—Transparency and consumer control

The FTC believes that every Web site that collects data for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that: data about consumers' activities online are being collected at the site for use in providing advertising about products and services tailored to individual consumer's interests, and; consumers can choose whether or not to have their information collected for this purpose.[7] One of the challenges noted by the FTC was the need to balance adequate disclosures with the need to make the disclosures easier for consumers to read. Also, the FTC noted that many consumers do not always read privacy policies, particularly if they are long and technical.

Principle 2—Reasonable security and limited data retention for consumer data

The FTC proposed that companies that collect or store consumer data for behavioral advertising also provide reasonable security for that data. These protections should be based on the sensitivity of the data, the nature of a company's business operations, the types of risks a company faces, and the reasonable protections available to a company.[8] Additionally, as part of the data security issue, the FTC also recommended that companies make some effort to reduce the time period of data retention.

Principle 3—Affirmative express consent for material changes to existing privacy promises

The retroactive modification principle has been a difficult one for companies to address. The FTC has stated that before a company can use data in a manner materially different from promises the company made when it collected the data, it should obtain affirmative express consent from affected consumers. The FTC specifically stated that this principle would apply in a corporate merger situation to the extent that the merger creates material changes in the way the companies collect, use, and share data.[9]

While this provides some guidance, it would not completely appear to prohibit retroactive changes if notice is provided and it was made clear at the time of data collection that the company may materially change its data practices in the future, though it provides some support for the argument that companies cannot make material and retroactive changes to their privacy policies, even if the prior policy was based upon opt-out consent.

Principle 4—Affirmative express consent to (or prohibition against) using sensitive data for behavioral advertising

This was an issue the FTC desired additional input on. While there may be people that desire to have behavioral advertising occur without affirmative express consent, there are issues, including the disclosure of sensitive information, that might make this not an attractive option for many consumers. The FTC has called for additional input on this issue.

Principle 5—Using tracking data for purposes other than behavioral advertising, a call for additional information

As with principle 4, the FTC called for additional information from groups and individuals on this issue. Among the particular concerns of the FTC was that secondary uses of this type of information are particularly invisible to consumers, and may be inconsistent with the consumers' reasonable expectations on the Internet.

Key Takeaways

While the guidance does not offer concrete requirements, general thoughts can be gleaned from these guidelines. First, monitoring and controlling your data collection regarding consumers has always been a good practice, but the FTC now has made clear this is something that companies should consider and review. Minimizing your company's data footprint also has the benefit of potentially reducing your compliance burden as well, since you may be able to reduce the number of laws that impact your company by reducing the amount of data you collect.

Second, the FTC has strongly indicated that proactive steps regarding incident response and data security are issues companies should be examining if they have not done so. Third, the FTC has recognized the balance that must be struck with information security and privacy and the benefits consumers receive from information sharing because the guidelines focus on proportional recommendations that do not flatly prohibit behavioral advertising or other forms of information sharing.

Fourth, the FTC has more expressly raised the issue of material changes to privacy policies and what level of consent is required to make a material change. The so-called ''retroactive change'' issue is still one where there are more questions than answers, but it is clear that some form of notice and consent to material changes is thought by the FTC to be important. However, this does not answer a number of other questions, including whether a consumer can consent, at the time personally identifiable information is first provided, to later material changes to privacy practices. Finally, the FTC recognized that there is a balance that must be struck between providing extensive, and sometimes difficult to comprehend, privacy disclosures, and making the policies easy for consumers to read and understand.

It remains to be seen whether the FTC's guidance will have a dramatic impact on information security and privacy issues or if these principles will provide any insights into future enforcement actions, but companies should be aware of these issues so that they can minimize the risks of security and privacy incidents.

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*