Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices

By Patricia Bailin, CIPP/US, Westin Research Fellow

iapp

IAPP
WESTIN RESEARCH
CENTER

Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices

By Patricia Bailin, Westin Research Fellow

Table of Contents

One of the major policy questions in the data governance space these days is what constitutes a reasonable level of privacy and data security that could provide a company with a safe harbor from U.S. Federal Trade Commission (FTC) enforcement action. Over the past several months, two companies facing FTC action – as well as a chorus of lawyers and scholars – have complained that enforcement is misguided absent clearer data security standards. Complicating matters, the FTC has been particularly tight-lipped about what data security standards it expects to see, and industry calls for policy guidance documents or workshops have been left unheeded. Essentially, the industry is arguing that the FTC is shifting the goalposts during the game.

Regardless of the merits of such arguments (industry groups fight tooth-and-nail against data security legislation even as they urge clearer guidance), the Westin Research Center has explored FTC privacy and data security consent decrees in an attempt to parse out what an acceptable level of privacy and data security could be. This study is part of the Westin Research Center's project to provide a comprehensive casebook of FTC privacy and data security enforcement actions.

Overview

In at least 47 cases since 2002, the FTC has cited companies for failing either to design or to implement an appropriately comprehensive privacy or data security program. Almost all of these cases have been settled. The settlement requirements include relatively standardized language outlining the parameters of a data security program and begin to chart a path toward the development of similarly standard language for privacy programs. However, aside from requiring the designation of an adequately trained chief data security or privacy officer and the undertaking of regular risk assessments, the standard language that the FTC uses is terse and offers little in the way of specifics about the components of a compliance program. Consequently, anyone seeking to design a program that complies with FTC expectations would have to return to the complaints to parse out what the FTC views as "*un*reasonable"—and, by negation, reasonable—privacy and data security procedures.

The following analysis is the result of this approach. It suggests possible guidelines for complying with FTC privacy and data security standards based on what the FTC has determined is *in*adequate. In other words, by pointing out what companies *did not* have in their programs, the FTC provides a peek at what, in its opinion, these companies *should* have done. The guidelines below are drawn from the 47 cases, loosely organized into seven categories that are not mutually exclusive: Privacy, Security, Software/Product Review, Service Providers, Risk Assessment, Unauthorized Access/Disclosure and Employee Training.

We emphasize that the requirements below reflect neither legal advice by the Westin Research Center nor express guidance by the FTC; rather, they are extrapolated from FTC assertions of corporate wrongdoings. (Ostensibly, there could be a gap between what the FTC views as inadequate and the guidance below; i.e., a company may not be cited for a Section 5 violation even if it does not fix all of its shortcomings under the FTC complaint.)

Privacy

In the four decisions requiring companies to establish a comprehensive privacy program,[1] companies allegedly failed to respect user choices. According to the FTC, these companies ignored consumer privacy preferences or misled consumers by providing inaccurate or incomplete information about user privacy, notice and control. In all four cases, the companies allegedly violated their own privacy policies and their statements on privacy settings. It is possible to deduce from the FTC's complaints that companies should:

- Perform risk assessments during the design and development stage of a new product or service to identify and address privacy vulnerabilities;
- Conduct regular testing and monitoring of the effectiveness of privacy controls, settings and procedures to ensure that user choices are respected;
- Conduct regular reviews of privacy statements and product design in order to ensure a match between privacy policies, available user options, disclosures to third parties and product functions, and
- Obtain explicit user consent to override prior user choices or to apply new privacy policies to previously collected data when privacy options or policies change.

CASE IN FOCUS: MICROSOFT

In one of its earliest data security cases, the FTC settled charges with Microsoft in 2002 over alleged misrepresentations of the information protections in its single sign-in and payment services, Passport, Passport Wallet, and Kids Passport. Though Microsoft claimed that its Passport system offered reasonable and appropriate security safeguards, the FTC found that it did not employ measures to prevent or detect unauthorized access to the Passport system. In addition, the FTC claimed that purchases made through Passport were no more secure than those made without it; that Passport collected more personal information than it stated; and that Kids Passport did not in fact offer parents control over the information their children provided online. The FTC found Microsoft's actions unfair and deceptive, making Microsoft one of the first companies required to implement a comprehensive security program.

Security

Since the FTC's settlement with Microsoft in 2002, the commission has made clear that companies handling consumer information must implement a program that contains "administrative, technical, and physical safeguards appropriate to [the organization's] size and complexity, the nature and scope of [its] activities, and the sensitivity of the personal information collected from or about consumers."[2] Such a program must set forth procedures not only for data collection, but also for its storage, handling, transport, and disposal.

The commission has reiterated several times that formal data security procedures should employ "readily available" technology and practices for safeguarding consumer information. The programs must consider not only well-known threats but also business-specific vulnerabilities, and they must be tailored to an organization's specific business model and data needs. Specific language in FTC cases indicates that security policies should include consideration of password procedures, access limitations, encryption protocol and processes for data retention and disposal.

[1] Google Inc., Docket No. C-4336 (October 24, 2011); MySpace LLC, Docket No. C-4369 (May 8, 2012); Facebook, Inc., Docket No. C-4365 (August 10, 2012); and Snapchat, Inc., (May 14, 2014).
[2] Microsoft, Inc., Docket No. C-4069. (Dec. 20, 2002), at 10.

Passwords

Despite the well-documented importance of complex user credentials, corporate employees, as well as average consumers, continue to generate weak user ID and password combinations. Password policies are therefore fundamental to a company's data security, as the FTC notes with increasing frequency. A company should:

- Establish and enforce rules requiring strong,[3] hard-to-guess[4] user IDs and passwords. Strong credentials can be achieved through default requirements that prohibit the use of common dictionary words;[5] forbid the use of the same word or a close variant of the word for both the password and the ID,[6] and deny a user the ability to create credentials that he or she already employs elsewhere on the network, especially passwords used to access third-party programs, websites, and networks;[7]

- Require periodic changes of user credentials, such as every 90 days, for customers and employees with access to sensitive personal information;[8]

- Suspend user credentials and/or disable administrative passwords[9] after a reasonable number of unsuccessful login attempts;[10]

- Prohibit the use of default passwords[11] or the sharing of user credentials,[12] as these practices reduce the likelihood of detecting or accounting for unauthorized activity;

- Establish and enforce policies to prohibit storage of administrative passwords in plain text on computers,[13] in cookies,[14] or in personal email accounts,[15] and

- Implement procedures for verifying or authenticating the identity of users who create new credentials for systems or programs that will enable them to access personal information.[16]

CASE IN FOCUS: TWITTER

Twitter's allegedly deficient login system and password practices attracted the attention of the FTC after hackers were able to gain access to administrative accounts on two separate occasions in 2009. In the three years prior to the breach, all Twitter employees had administrative access to the company's system, entered their administrative credentials via the same public login page through which users accessed their accounts, and used personal email accounts for business activity because Twitter did not provide company accounts. In addition, because Twitter neither established nor enforced security policies related to passwords, employee passwords were particularly vulnerable to attack. Access to employee administrative accounts provided the hackers with the capacity to view nonpublic tweets and nonpublic user information, the authority to reset a user's account password, and the ability to send unauthorized tweets from a user's account. The FTC cited Twitter for its inadequate data security practices and for falsely representing its security policies to consumers. The company settled with the FTC on two counts of deceptive trade practices.

[3] *E.g.*, The TJX Companies, Docket No. C-4227 (July 28, 2008); CardSystems Solutions, Inc., Docket No. C-4168 (Sept. 5, 2006).
[4] *E.g.*, LifeLock, Inc., (Feb. 23, 2010); Twitter, Inc., Docket No. C-4316 (Mar. 2, 2011).
[5] *E.g.*, Reed Elsevier, Inc., Docket No. C-4226 (July 29, 2008).
[6] *E.g.*, Lookout Services, Inc., Docket No. C-4326 (June 15, 2011).
[7] *E.g.*, Twitter, Inc., *supra* note 4.
[8] *E.g., Id. See also* Lookout Services, Inc., *supra* note 6; Reed Elsevier, Inc., *supra* note 5.
[9] *E.g.*, Twitter, Inc., *supra* note 4.
[10] *E.g.*, Lookout Services, Inc., *supra* note 6; Reed Elsevier, Inc., *supra* note 5.
[11] *E.g.*, BJ's Wholesale Club, Inc., Docket No. C-4148 (Sept. 20, 2005); DSW Inc., Docket No. C-4157 (Mar. 7, 2006).
[12] *E.g.*, Reed Elsevier, Inc., *supra* note 5.
[13] *E.g.*, Guidance Software, Inc., Docket No. C-4187 (Mar. 30, 2007).
[14] *E.g.*, Reed Elsevier, Inc., *supra* note 5.
[15] *E.g.*, Twitter, Inc., *supra* note 4.
[16] *E.g.*, United States v. ChoicePoint Inc., No. CV-00198 (N.D. Ga. Filed Jan. 30, 2006); United States v. Rental Research Services, Inc., FTC File No. 072 3228 (Dist. Ct. Minn. Filed March 5, 2009).

Limited Access

Another common security issue raised in a number of cases is lack of sufficient control over access to personal information. Access limitations can be instituted at either a network level, for example, by maintaining multiple servers or installing firewalls or similar solutions, or at the employee level, by restricting access to personal information to personnel of specific departments or to individual employees. Limited access policies curb unnecessary security risks and minimize the number and type of network access points that an information security team must monitor for potential violations. A company is therefore advised to:

- Segment servers[17] so that unauthorized access to one does not compromise the security of all;
- Apply readily available security measures such as firewalls or isolated payment card systems[18] to control and monitor access:
  - to a computer network from wireless access points,[19]
  - between computers on a network, including between computers on one in-store network and those on other in-store or corporate networks,[20] and
  - between computers on the company network and the Internet;[21]
- Limit employee access[22] to and copying of[23] personal information based on such employee's role;
- Restrict third party access to personal information based on business need, for example, by restricting access based on IP address, granting temporary access privileges, or similar procedures;[24]
- Establish an employee login page that is unknown to consumers and separate from the customer/end user login page,[25] and
- Restrict the number of files on which data can be stored[26] in order to simplify compliance with data use limitations and deletion procedures.[27]

CASE IN FOCUS: DAVE & BUSTER'S

In 2007, a hacker exploited weaknesses in the corporate and in-store networks of restaurant and entertainment chain Dave & Buster's. The intruder managed to connect to the networks multiple times, install software, and intercept personal information in transit from in-store networks to the company's credit card processing company. The breach compromised approximately 130,000 credit cards. Although Dave & Buster's took steps to prevent further unauthorized access, the FTC asserted that its flawed security measures constituted an unfair practice.

Encryption

FTC attention has regularly focused on data encryption. In more than half (27) of the cases requiring privacy or data security programs, the FTC addressed the defendant's encryption protocols, which if noted it should have been compatible with industry standards. ValueClick, Inc., for example, was cited in 2008 for "using only an insecure form of alphabetic substitution that [was] not consistent with, and less protective than, industry-standard encryption."[28] Given the demonstrated risk of security breaches, companies should render personal information "unusable, unreadable, or indecipherable"[29] as the FTC noted in its complaint against CBR. Consequently, security programs should contain protocols to ensure the company will:

- Transmit sensitive[30] and personal information,[31] including user credentials[32] and financial account and credit card information,[33] securely in either encrypted format[34] or through cryptographic protocols (TLS or SSL), and
- Store sensitive and personal information in encrypted format,[35] including information that was encrypted during transmission[36] and any personal information on in-store networks,[37] back-up tapes,[38] or other portable media devices.[39]

[17] *E.g.*, RockYou, Inc., No. CV-01487 (N.D. Cal. Filed Mar. 26, 2012).
[18] *E.g.*, Dave & Buster's, Inc., Docket No. C-4291 (May 20, 2010).
[19] *E.g.*, *Id. See also* BJ's Wholesale Club, Inc., *supra* note 11.
[20] *E.g.*, DSW Inc. *supra* note 11.
[21] *E.g.*, Genica Corporation, Docket No. C-4252 (Mar. 16, 2009); TJX Companies and CardSystems Solutions, Inc., *supra* note 3.
[22] *E.g.*, CBR Systems, Inc., Docket No. C-4400 (Apr. 29, 2013).
[23] *E.g.*, Accretive Health, Inc., Docket No. C-4432 (Feb. 5, 2014).
[24] *E.g.*, Dave & Buster's, *supra* note 18.
[25] *E.g.*, Twitter, Inc., *supra* note 4.
[26] *E.g.*, DSW Inc., *supra* note 11.
[27] *E.g.*, Accretive Health, supra note 23.
[28] *See* United States v. ValueClick, Inc., No. CV08-01711 (C.D. Cal. Filed Mar. 13, 2008), at 13.
[29] *See* CBR Systems, Inc., *supra* note 22, at 3.
[30] *E.g.*, Credit Karma, Inc., Docket N. C-4480 (Aug. 13, 2014); Fandango LLC, Docket No. C-4481 (Aug. 13, 2014).
[31] *E.g.*, The TJX Companies, *supra* note 3.
[32] *E.g.*, TRENDnet, Inc., Docket No. C-4426 (Jan. 16, 2014).
[33] *E.g.*, Compete, Inc., Docket No. C-4384 (Feb. 20, 2013); Upromise, Inc., Docket No. C-4351 (Mar. 27, 2012).
[34] *E.g.*, BJ's Wholesale Club, Inc., *supra* note 11.
[35] *E.g.*, Genelink, Inc., Docket No. C-4456 (May 8, 2014); Guess?, Inc., Docket No. C-4091 (July 30, 2003).
[36] *E.g.*, Petco Animal Supplies, Inc., Docket No. C-4133 (Mar. 4, 2005).
[37] *E.g.*, BJ's Wholesale Club, Inc., *supra* note 11.
[38] *E.g.*, James B. Nutter& Company, Docket No. C-4258 (June 12, 2009).
[39] *E.g.*, CBR Systems, Inc., *supra* note 22.

Data Retention and Disposal

The FTC has proscribed companies' continuous storage of data after it has served its business purpose. While the FTC does not specify a precise threshold for data retention, it has stated that data should be stored only for as long as it serves a legitimate business need. Companies should also have policies in place for disposing of data once such business needs have been met. Companies should thus:

- Formalize policies regarding the length of time consumer data will be stored. Data should not be stored indefinitely, but rather for a period of time commensurate with legitimate business needs.[40] Information for which there is no longer a business need should be destroyed.[41]

- Implement and monitor compliance with policies and procedures for rendering information unreadable or otherwise secure in the course of disposal. Securely disposed information must not practicably be read or reconstructed.[42]

CASE IN FOCUS: CVS CAREMARK

Between 2006 and 2007, CVS pharmacies were in the media spotlight for insecurely disposing of personal information. In at least 15 cities, the press reported finding documents containing customer and employee personal information in publicly accessible dumpsters. The FTC charged CVS Caremark with unfair trade practices, citing the corporation's allegedly inadequate information security policies, employee training, and compliance monitoring.

Software/Product Review

Companies are responsible for managing the privacy and security of personal information that is processed by the products they develop and use. Accordingly, they are required to instate checks and controls on the products they use as well as throughout the development process of new products and services.[43] The goal is to ensure that all products and software function according to an organization's stated privacy and data security policies and any applicable industry standards. More specifically, companies should:

- Implement appropriate checks and controls on the review and testing of software and products intended for internal use;[44]

- Follow well-known, commonly-accepted secure programming practices, including secure practices that are expressly described in the product's operating system guides for manufacturers and developers,[45] and

- Perform security reviews and testing of software and products at key points in the development cycle:

  - Such procedures may take the form of a security architecture review, vulnerability and penetration testing, and reasonable and appropriate code review and testing to verify that security and privacy protections are consistent with user choices and company policy;[46]

  - Special procedures should exist to test for any excessive collection of personal information, i.e., information that does not serve a legitimate business need;[47] unauthorized collection of personal information,[48] and products or software that will override existing, promised, or standard defaults without employing substitute security measures.[49]

[40] *E.g.*, Ceridian Corporation, Docket No. C-4325 (June 8, 2011); Life is good, Inc., Docket No. C-4218 (Apr. 16, 2008).
[41] *E.g.*, CBR Systems, Inc., *supra* note 22.
[42] *E.g.*, CVS Caremark Corporation, Docket No. C-4259 (June 18, 2009); PLS Financial Services, Inc., No. 12-CV-08334 (N.D. Ill. Filed Oct. 17, 2012).
[43] *E.g.*, Credit Karma, Inc. and Fandango LLC, *supra* note 30.
[44] *E.g.*, Eli Lilly and Company, Docket No. C-4047 (May 8, 2002).
[45] *E.g.*, HTC America Inc., Docket No. C-4406 (June 5, 2013).
[46] *E.g.*, TRENDnet, Inc., *supra* note 32.
[47] *E.g.*, Compete, Inc., *supra* note 33.
[48] *E.g.*, Snapchat, Inc., *supra* note 1.
[49] *E.g.*, TRENDnet, Inc., *supra* note 32.

CASE IN FOCUS: TRENDNET

TRENDnet developed IP cameras and software for consumers to monitor their homes or businesses via live feeds over the Internet or from their mobile devices. However, the company's software development practices were allegedly insufficient to protect the live feeds from unauthorized access. According to the FTC, TRENDnet failed, among other things, to conduct security reviews and testing of its products at key points in their development and release. Consequently, users' login credentials were transmitted and stored in clear text and the setting that enabled users to determine whether their video streams would be public or private did not function properly. Between 2010 and 2012, hackers exploited these vulnerabilities to compromise hundreds of IP cameras, granting them visual access to private areas of users' homes, sleeping and playing children, and adults engaged in private daily activities. Some hackers posted links online to almost 700 of the live feeds, and media reports of the breach featured photos taken from real time video footage shot in consumers' homes. The FTC charged TRENDnet with three counts of deceptive and unfair trade practices.

Service Providers

Service providers who access or handle personal information on behalf of a company could create a liability for the company and must therefore be properly managed. For example, in a recent case, CBR, an umbilical cord blood and tissue bank, settled an FTC enforcement action alleging, among other things, failure to supervise a service provider adequately. In that case, the company's lack of oversight resulted in two security lapses: the retention of a legacy database for which CBR no longer had a legitimate business need, as well as the storage of personal information in that database in unencrypted, vulnerable form.[50]

Requisite oversight of a service provider will vary depending on the service and the sensitivity of the information; but companies should generally:

- Require by contract that service providers implement and maintain appropriate safeguards for consumers' personal information;[51]
- Ensure reasonable oversight of service providers' security practices and their employees' handling of personal information:[52]
  - » Adequately verify, through monitoring and assessments, that service providers implement reasonable and appropriate security measures to protect personal information;[53]
  - » Request and review relevant information about a service provider's security practices, such as its documented information security program or the results of audits and security assessments conducted on their network.[54]

[50] *See* CBR Systems, Inc., *supra* note 22.
[51] *E.g.*, Goal Financial, LLC, Docket No. C-4216 (Apr. 9, 2008); Genelink, Inc., *supra* note 35.
[52] *E.g.*, Credit Karma, Inc., *supra* note 30; Genelink, Inc., *supra* note 35.
[53] *E.g.*, GMR Transcription Services, Inc., Docket No. C-4482 (Aug. 14, 2014).
[54] *E.g., Id.*

Risk Assessment

Each time the FTC has mandated that a company implement a comprehensive privacy or data security program, it has required that such a program consider "material internal and external risks that could result in the…compromise of personal information and an assessment of the sufficiency of any safeguards in place to control these risks…in each area of relevant operation." In addition, the FTC expects to see policies in place to ensure that any issues are addressed and corrected. Risks should be continuously assessed and the program adjusted as a result of ongoing monitoring, material changes to company operations, or any other changing circumstances. Risk assessment policies should include provisions obligating the company to:

- Record and retain system information sufficient to perform security audits and investigations;[55]
- Perform assessments to identify reasonably foreseeable risks to the security, integrity, and confidentiality of personal information collected and stored on the network,[56] online[57] or in paper files;[58]
- Assess application or network vulnerabilities, particularly to commonly known or reasonably foreseeable attacks like "cross-site scripting",[59] to widely known security flaws like "predictable resource location," or to design flaws like the ability of users to bypass website authentication procedures,[60] and
- Evaluate the likelihood and risks of third party access;[61] for example, in some cases it might be sufficient to provide third parties with access to fictitious data sets rather than real personal information or to provide them with access to only certain categories of personal data rather than unrestricted database access.[62]

Unauthorized Access/Disclosures

Preventing and addressing incidents of unauthorized access to and disclosures of personal information are critical components of a comprehensive privacy and data security program. References to incident response appear in more than half (24) of the cases in this study. Extrapolating from the inadequacies described in past complaints, a company should:

- Implement reasonable measures to assess and enforce compliance with established security policies and procedures, such as by scanning networks for and blocking unauthorized downloads of applications;[63]
- Implement policies for the prevention of unauthorized access, including standard procedures, such as regularly checking for and installing security patches and critical updates on the company's network;[64]
- Implement policies for the detection of unauthorized access, including:
  - » installing antivirus or anti-spyware programs on computers,[65]
  - » employing an intrusion detection system,[66]
  - » creating a formalized process to address security warnings and intrusion alerts,[67] and
  - » logging network activity[68] and reviewing activity on the network;[69]
- Monitor and filter outbound traffic[70] and outgoing transmissions[71] to identify and block unauthorized disclosures of personal information;
- Implement procedures for receiving, reviewing, and addressing security vulnerability reports from third parties,[72] including researchers, academics, or other members of the public,[73] and
- Prepare an incident response plan that is ready to implement immediately upon detection of a security breach.[74]

[55] *E.g.*, Microsoft Corporation, Docket No. C-4069 (Dec. 20, 2002).
[56] *E.g.*, Genelink, Inc., *supra* note 35.
[57] *E.g.*, EPN, Inc., Docket No. C-4370 (Oct. 3, 2012).
[58] *E.g.*, James B. Nutter& Company, *supra* note 38.
[59] *E.g.*, Reed Elsevier, Inc., *supra* note 5.
[60] *E.g.*, Lookout Services, Inc., *supra* note 6.
[61] *E.g.*, Premier Capital Lending, Inc., Docket No. C-4241 (Dec. 10, 2008).
[62] *E.g.*, Genelink, Inc., *supra* note 35.
[63] *E.g.*, EPN, Inc., *supra* note 57.
[64] *E.g.*, LifeLock, Inc., *supra* note 4.
[65] *E.g.*, *Id.*
[66] *E.g.*, Genica Corporation, *supra* note 21.
[67] *E.g.*, The TJX Companies, *supra* note 3.
[68] *E.g.*, EPN, Inc., *supra* note 57.
[69] *E.g.*, LifeLock, Inc., *supra* note 4.
[70] *E.g.*, Dave & Buster's, Inc., *supra* note 18.
[71] *E.g.*, EPN, Inc., *supra* note 57.
[72] *E.g.*, Fandango LLC, *supra* note 30.
[73] *E.g.*, HTC America Inc., *supra* note 45.
[74] *E.g.*, EPN, Inc., *supra* note 57.

CASE IN FOCUS: EPN

As a debt collection company, EPN regularly maintained information about its clients' customers. Some time before 2008, an executive officer installed on the company's network an unauthorized P2P application without a legitimate business purpose. This exposed records for almost 4,000 consumers to anyone with access to the company's network – including all of EPN's clients. According to the FTC, the company's lack of an information security plan, incident response plan, and sufficient information security compliance procedures resulted in a failure to protect consumers from unauthorized information disclosures. EPN settled with the FTC in 2012 on a charge of unfair trade practices.

Employee Training

Designing and implementing an employee training program has increasingly become a standard industry practice and one that the FTC has required in numerous settlements. The employee training program should be designed to assist employees in understanding and managing privacy and data security safeguards. Once a company has a privacy and data security program in place, the employee training program should focus on ensuring compliance with it. According to the FTC, an employee training program should:

- Educate employees on the company's privacy and data security policies as well as on security risks[75] relevant to their jobs:
  - » Employees, including software/product engineers[76] and executives,[77] should receive training on information security, collection, handling, transport, maintenance and disposal of consumer personal information;
  - » Engineering staff should receive appropriate training and oversight for detecting application vulnerabilities and conducting security testing;[78]
- Provide adequate training to employees about timely and effective security incident response.[79]

Interestingly, in one case, the FTC alleged that a company suffered a security breach by "using personal information in training sessions with employees and failing to ensure that the information was removed from employees' computers following the training".[80] Of course, the training program itself must not compromise a company's data security.

Conclusion

This study sets forth the contours of a reasonable privacy and data security program based on analysis of 47 FTC enforcement cases. While providing companies with neither a safe harbor from enforcement nor immunity from a privacy or data security breach, such a program will mitigate risk and strengthen a company's hand in dealing with any adversity. Although the analysis in this study is informal and based on "reverse-engineering" the FTC's complaints, it offers a potential starting point for defining "reasonable" measures of privacy and data security, thereby helping to clear the fog of uncertainty that surrounds a constantly shifting legal landscape for compliance.

[75] *E.g.*, Upromise, Inc., *supra* note 33.
[76] *E.g.*, HTC America Inc., *supra* note 45.
[77] *E.g.*, EPN, Inc., *supra* note 57.
[78] *E.g.*, MTS, Inc. d/b/a Tower Records, Docket No. C-4110 (May 28, 2004); HTC America Inc., *supra* note 45.
[79] *E.g.*, Goal Financial, LLC, supra note 51.
[80] *E.g.*, Accretive Health, supra note 23.