Assessing the Federal Trade Commission’s Privacy Assessments

Chris Jay Hoofnagle | University of California, Berkeley

“Assessments”—evaluations performed by outside accounting firms—are a key tool for regulators to detect privacy and security problems. However, these assessments are less intense than audits and fall short of what is needed to ensure that companies honor consumer privacy expectations.

Conductors protection regulators worldwide share basic problems: the companies that regulators police are so powerful and rich that fines do not matter. Consider the French with their €150,000 fine against Google in 2014. Efficacious fines against dominant platforms would have to rise to nine-figure levels to cause change, but consumer protection agencies generally lack the authority and political will to levy such fines.

As a result, consumer protection officials ensure compliance by monitoring defendant companies. However, even this is a challenge. Although consumer protection agencies such as the US Federal Trade Commission (FTC) have decades of experience in evaluating misleading advertising, information security and privacy oversight challenges differ from advertising matters.

Because information security and privacy issues are difficult to observe and, even if detected, difficult to understand, the FTC and other enforcement agencies rely on outside “assessments” by accounting and security consultants. These assessments evaluate the veracity of defendant company managers’ claims about privacy and security protection of consumer information. Accounting and security firms now have a lucrative and growing business in performing assessments required by the FTC and state attorneys general. In a real sense, consumer privacy worldwide depends on these assessments, as international regulators rely on the FTC’s oversight of companies serving consumers in other countries.

Unfortunately, assessments are misunderstood by many in the policy realm, who mistakenly believe them to be as rigorous as a formal audit. The lack of knowledge of the differences between assessments and audits allows the FTC and respondent companies to tout assessments as an effective tool to improve practices.

In this article, I discuss efforts to oversee companies’ privacy and security programs through the lens of two assessment reports on TRENDnet and Google and offer five suggestions to increase accountability in the assessment process.

FTC Enforcement Dynamics
The FTC has brought more than 150 privacy and security cases against companies for failing to protect data or for not honoring consumer privacy expectations. Recent work by professors Kenneth Bamberger and Deirdre Mulligan found that FTC enforcement actions are critical to promoting pro-privacy practices among private firms. The FTC has broad power to prohibit “unfair and deceptive” trade practices and, in effect, creates consumer protection policy by targeting its enforcement authority against companies that violate consumer expectations. Starting with print advertising in the 1910s, the agency policed marketing and business practices on radio, then television, and in the 1990s, the Internet. Bamberger and Mulligan found that the FTC’s broad, roving power to influence consumer expectations keeps companies attentive to privacy and
security issues. The FTC’s approach produces privacy leadership instead of privacy compliance—companies must continually revisit consumer expectations to avoid the negative publicity of FTC enforcement actions.

In this article, I focus on what the FTC does after it has targeted and brought a case against a company. The FTC’s post-case settlement activities are critical, because the FTC cannot levy civil penalties, that is, direct, punitive fines for illegal activity, against these companies. Civil penalties are available only when a company violates a Trade Regulation Rule (there is no such rule for privacy) or a statute that provides for damages (such as the Children’s Online Privacy Protection Act), or where certain, burdensome procedures have been followed. For instance, civil penalties are available under what’s known as nonrespondent liability, in which a company copies the same wrongful behavior of another FTC respondent. However, this requires the FTC to win an administrative proceeding against one respondent, and then show that another company had knowledge of the cease-and-desist order and nevertheless engaged in the same unfair or deceptive practices. Finally, the FTC can obtain “redress” by winning an administrative trial against a company before an administrative law judge, and then separately going to federal district court to establish that the company’s conduct was dishonest or fraudulent.4

To make up for a lack of monetary penalty and to protect consumers, the FTC imposes lengthy terms of oversight over respondent companies, requiring companies to adhere to privacy promises; implement privacy and security plans that go well beyond the wrongdoing alleged;5 and, critically, undergo privacy and security plan assessment by an outside firm.

How Assessments Differ from Audits
FTC settlements typically require companies to obtain an outside firm’s assessment of the company’s privacy and security program; however, at times the FTC has incorrectly described this oversight of companies as including an audit. This might lead people to conclude that the oversight is more rigorous than it is.

The difference between audits and assessments is not popularly understood. Assessment is a term of art in accounting wherein a client defines the basis for the evaluation, and an accounting firm certifies compliance with the client-defined standard. An audit, on the other hand, is an evaluation against a defined, externally developed standard, such as an International Organization for Standardization (ISO) standard’s requirements.

In assessments, an evaluator must only obtain “sufficient evidence to provide a reasonable basis for the conclusion that is expressed in the report.”6 Pursuant to assessment rules, an assessor might rely on statements from the company regarding its privacy practices—that is, interview relevant employees—rather than engage in testing. For instance, a company can claim that its scripts do not “respawn” cookies, and the assessor is permitted to accept that representation as true without further investigation.

In recent years, the FTC has ramped up some assessment conditions, such as requiring assessor qualifications and details of the program established to remedy privacy. For instance, in a recent settlement with Snapchat, the FTC required third-party assessments to be completed by a professional with three years of experience in privacy and security. Furthermore, the assessor had to be preapproved by a division director, a relatively high-level staff person at the FTC. This assessor is supposed to identify the various privacy controls implemented by the company; explain why the controls are appropriate, justify the use of the controls in light of the settlement terms, and certify that the controls “are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.”7

Assessment Reports

We see outside assessments through a glass darkly, because companies and the FTC itself redact assessment reports heavily before they’re released to the public. However, the TRENDnet assessment was marked “classified” instead of invoking the magic word “confidential,” and thus much of it was released unredacted. The Google assessment report is more heavily redacted, yet it elucidates the challenges the FTC faces in monitoring compliance with privacy and information security orders.
TRENDnet
The FTC’s case against TRENDnet is especially important for the emerging Internet of Things. TRENDnet is a multinational seller of network appliances, Internet-enabled cameras, and computer hardware accessories. It operates in business-to-business and business-to-consumer markets, and its cameras are popular for baby monitoring. At the time of the investigation, TRENDnet had approximately US$60 million in annual revenue, with about 10 percent of its revenue being generated from Web camera sales. Although the company had only about 80 employees, it offered a wide variety of network hardware for businesses and consumers, ranging from routers and switches to security cameras and storage devices.

In 2012, someone discovered that a configuration program for TRENDnet webcams caused many of the cameras to be broadcast online. Hundreds of TRENDnet camera feeds were discovered and linked online, allowing anyone to see and, in some cases, hear TRENDnet users in the privacy of their homes. The FTC investigated TRENDnet and discovered multiple security lapses. The FTC alleged that TRENDnet was sending and storing password information in the clear on consumers’ mobile devices.

To win a case, the FTC must establish that a company acted unfairly or deceptively. In the TRENDnet case, the company called its access software SecurView. The cameras were pictured with a lock and labeled “secure.” According to modern conceptions of consumer protection law, merely using these elements could lead a consumer to believe that a product is secure. Thus, consumers’ reasonable expectations were violated when TRENDnet failed to implement basic security protections in its cameras.

TRENDnet settled the FTC case—as the vast majority of defendant companies do. The FTC required a lot from TRENDnet in the consent decree and sought to have TRENDnet answer the question of whether it could be trusted by consumers. Yet, when one reads TRENDnet’s initial report, more questions are raised than answered.

First, no one appears to have certified an assessment of TRENDnet’s systems. Second, there’s no contact information for the company hired to test TRENDnet’s system—it is listed only as “Institute for Information Industry.” Third, TRENDnet’s CEO stated that certified information system security professionals developed its compliance system but did not identify these experts. Fourth, the FTC called for an evaluation performed by a certified secure software life cycle professional or a certified information systems security professional, but according to the TRENDnet initial report, it appears to have been done by someone who claimed the following:

Fifth, although the report includes many pages of training material and policies, there’s no attempt to explain how these meet the various risk identification and mitigation obligations that the settlement required.

Finally, the TRENDnet submission includes a device security testing report prepared by the Institute for Information Industry, which found a few vulnerabilities in TRENDnet’s camera. The testers recommended that these vulnerabilities be fixed, despite the fact that the security problems could be exploited only by individuals with local network access. Although the testers called for a remedy, the assessment report makes no mention of whether the vulnerabilities would be fixed at all.

The FTC’s attorneys clearly were disappointed in TRENDnet’s report, so they requested that the company file an updated, more complete version. I obtained that assessment too (see https://hoofnagle.berkeley.edu/ftcprivacy/wp-content/uploads/2015/11/trendnet_followup.pdf). Although it addresses many of the deficits identified earlier, it still rings hollow. Multiple pages were copied and pasted from the FTC’s order. The new assurances read like an exercise in compliance rather than a company that has inculcated the privacy values the FTC seeks to impress.

Perhaps small companies will always have assessments that lack a professional patina. Yet, even when a more established company completes an assessment, it is far from reassuring. Google’s assessments show more competence but share some of TRENDnet’s pathologies.

Google
The FTC has pursued Google for several privacy deviations. The original matter concerned how the company deployed its social network Buzz. Google was eager to compete with Facebook in the social network market and needed to quickly populate its system so that users would peel away from Facebook and spend more time in the Google platform. Google did this by loading users’ profiles automatically with their most frequent email contacts. However, in doing so, Google made these frequent email contacts public. Apparently, the company did not consider that users might have confidential or complex, contentious relationships with others...
that would become endangered through publicity. For instance, domestic violence or stalking victims could be at risk if their contacts were made public and available to the aggressors. People with confidential relationships, such as doctors and lawyers, might have their patients’ and clients’ identities disclosed. Google agreed to a broad consent agreement to settle the FTC’s case. In the settlement, Google promised to honor privacy guarantees to consumers, create a comprehensive privacy program, and be subject to “initial and biennial assessments and reports … from a qualified, objective, independent third-party professional.”

Less than one year later and while under FTC oversight, Google slipped up again by tracking Apple’s Safari browser users. Safari blocked Google’s tracking cookies by default; thus, Google told Safari users that they needed to do nothing to avoid tracking. However, Google’s engineers found a way to circumvent this setting and place a cookie from the company’s tracking network. Once this was accomplished, other cookies from Google could also be placed. Revelation of this tracking led the FTC to sue to obtain civil penalties based on the theory that the tracking violated the earlier settlement concerning Buzz.

Marked “highly confidential,” as if nuclear secrets might be at stake, the Google assessment I obtained is largely redacted. Even the assessor’s professional qualifications are blacked out. The portions that were released tend to be auditor jargon, much of which is boilerplate language from a form assessment report provided by the American Institute of Certified Public Accountants.

Accounting companies sometimes use confusing but impressive-sounding terminology to describe their activities. A company can claim that it engaged in a heightened version of assessment—known in the industry as an examination—with independent verification of facts, but this investigation can be as simple as having an accounting company visit its website to check for links to privacy policies. Assessments are short, sometimes less than two dozen pages, and are signed by an institution, rather than the individual responsible for the endeavor, which would increase accountability.

Public interest groups that have obtained copies of these third-party assessments have shown them to be less than rigorous. For instance, the Electronic Privacy Information Center obtained Google’s first privacy assessment. The document is 30 pages long; however, three of the pages are an appeal for confidential treatment and another five are the company’s privacy policy. Moreover, the document was not signed by a specific individual at the assessor company, PricewaterhouseCoopers. How could such a short document account for all the company’s information collection and handling activities from its multiple product lines? PricewaterhouseCoopers claimed it could, intoning, “Google’s privacy controls were operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the Assessment Period, in all material respects.”

Google’s assessment report for 2012 to 2014 touts Google’s significant investment in privacy thinking, including its staffing of many lawyers on privacy issues. Under Google’s terms of settlement, it must identify risks that could result in unauthorized collection, use, or disclosure of personal information. At the same time, the report disclaims any evaluation of this effort, noting, “We are not responsible for Google’s interpretation of, or compliance with, information security or privacy-related laws.” This is a key deficit in assessments.

Assessments and the Law

In theory, assessments should help the FTC police noncompliant companies. In practice, such work involves a big investment from an agency with a small budget and the exceedingly large responsibility of policing almost all consumer protection and many antitrust issues. Both TRENDnet and Google were administrative cases in which the companies settled with the FTC without going to court. For the FTC to enforce these orders and impose monetary penalties, it must go to federal court, where it has the burden to show noncompliance with the order. The FTC did this with respect to Google for its tracking of Safari users. It filed an action in federal district court to enforce the order, and Google settled the case for $22.5 million—a record fine for the FTC, but a moment’s revenue for Google.

Respondent companies subject to a court order can sometimes put the FTC in a weaker posture when it tries to curb noncompliance. To police a rogue company under a court order, the FTC must return to court and argue that the company is in contempt. Courts construe settlement agreements akin to contracts. Despite the fact that a company engaged in wrongful practices and is under suspicion for continued noncompliance, the FTC has the burden of proving contempt. In some circuits, courts have put the burden on the FTC to show that the company engaged in substantial
noncompliance—not a mere technical violation of the order. In addition, rather than requiring only a “preponderance of the evidence standard” (that the company more likely than not violated the order), courts require the higher, clear, and convincing evidence standard of noncompliance in contempt cases.10

Both in enforcing an administrative order and in bringing contempt actions, ambiguity and incentive conflicts further frustrate the FTC’s ability to police companies. Demonstrating civil contempt requires the FTC’s commands to a defendant to be clear and unambiguous. But consider how ambiguous the requirement to have a “reasonable” privacy and data security program is. Whereas it would be simple for the FTC to obtain a contempt order if the respondent did not comply at all, a weak or partial embrace of the duty might be difficult to police in practice.

The FTC has incentives to craft orders with increasing complexity, include conditions where noncompliance can be detected, and impose duties that are amenable to the proof standard required in contempt actions. Presumably, this is where an assessor would save the day by providing a credible, outside opinion that the practices were not up to snuff. Most third parties will act professionally, but they have incentives to paint a pretty picture of the client company.

For instance, in the Google assessment, there is not a whiff of noncompliance. This is strange, given that during the assessment period, Google had several adverse court rulings on its services, including cases involving two different services that suggested the company had violated federal wiretapping laws.11 In one case, Google moved its ad-scanning appliance so it would read emails before the user received them. Such scanning violates wiretapping laws, and it was not at all clear that consumers understood that the scanning was occurring. The other case involved Google’s Street View program. As Google’s cars navigated roads and photographed public areas, the cars collected unencrypted Wi-Fi signals. In doing so, a car would have monitored individuals’ browsing and emails during the moments that it passed the Wi-Fi router. Google argued that the Wi-Fi signals were public and that users had no expectation of privacy for them. However, courts and state attorneys general disagreed. Street View was the focus of a multistate investigation resulting in a $7 million settlement. The omission of these two incidents in the report, both of which occurred during the observation period, suggests that the assessor had not read the newspaper for two years.

Furthermore, because assessments are self-certifications of compliance, they’re unlikely to document departures from the duties agreed to in a consent order. In fact, assessors can find departures from duties and still conclude that the program is in compliance.

**Improving the Assessment Approach**

The TRENDnet and Google reports highlight several weaknesses of the FTC’s assessment approach to oversight. The FTC is tasked with policing almost all consumer issues in the economy—from “dolphin-free” tuna fish labels to the legitimacy of boxing match organizations. Privacy is just one area of focus, and in that area, the FTC is already overseeing more than 150 defendant companies. FTC attorneys have to work up new cases while monitoring a growing number of completed matters, such as the ones against Facebook and Google. This is why the practice of outsourcing compliance activities is so important and likely to continue. An examination of the TRENDnet and Google assessments reveal improvements that could make the FTC more effective.

**Require Systems Compliance Tests**

Technical testing is key, but under the standard assessment procedure, sophisticated testing is not required. The FTC should require assessments to include technical testing of systems compliance.

A lack of testing is problematic because often companies do not understand how their own systems function. For instance, twice in recent years, companies have challenged my University of California, Berkeley, research team’s findings that their websites were reinstalling cookies deleted by users. In both cases, we were able to show forensically that the websites performed differently from how the executives described. The company executives were not lying. Instead, in both cases, company leadership apparently was unaware of steps that engineers had taken to make user tracking redundant. In fact, this might have been the case with Google’s tracking of Safari users—the engineers might have been trying to make all its services work uniformly across all browser platforms without consulting with management or legal teams. In such situations, an assessor who bases a certification on interviews instead of testing will simply parrot and valorize the executives’ limited understanding of system functions.
Use Audit-Like Standards

It is strange to use an assessment approach for a company that has been caught violating its own privacy policy. In a way, an FTC enforcement action results from a flawed assessment—a company declares its own privacy standards and its compliance with them, but the FTC finds inadequacy in the company’s policy or a lack of compliance. The concept of privacy suffers from a Through the Looking-Glass problem in that, just like Humpty Dumpty, each company can say what it chooses privacy to mean. Two academics analyzing how Google conceived of privacy found that the company chose an esoteric, flexible definition that was compatible with the company’s advertising revenue goals.12

To address these deficits, the FTC can make monitoring efforts more audit-like and definite by specifying the standards that respondents must meet in their assessments, so respondents are no longer able to generate their own skewed privacy definition and declare themselves compliant with it. Although often maligned, privacy standards are indeed emerging in both policy and engineering circles. For instance, the Generally Accepted Privacy Principles (GAPP) represent a comprehensive framework for organizational procedure and practice. There are indications that the FTC is using GAPP as a road map for a comprehensive privacy program. In the privacy-by-design field, academics and practitioners have proposed specific approaches to build privacy values into technology.14,15 Building privacy into the system architecture is an attempt to make data misuse more difficult and ensure that such misuse is documented. Privacy-by-design approaches typically include requirements to minimize the amount of data collected at the outset.

However, Google has taken a different, surveillance-by-design approach. Under its conceptualization of privacy, Google can pass an assessment because it perceives no privacy invasion when it collects personal information. But when we change the privacy lens to a standard that embraces data minimization and normative aspects of privacy, we see that the company’s radical posture could be brought in line with more responsible actors.

Interview Stakeholders outside the Company

Today’s assessments exist in an echo chamber, with managers declaring that their company is in compliance with FTC orders and the assessor finding a “reasonable basis” to agree with the declaration. In Google’s case, it appears that the assessor interviewed 30 company employees to come to this reasonable basis. But why would any of these employees say anything disconfirming management’s declarations?

This information deficit could be corrected if assessors interviewed stakeholders outside the company and made it possible, in an ombudsman-like fashion, to take anonymous tips from company employees. If asked, privacy advocates, competitors, and even newspaper reporters might have raised some of Google’s troubling privacy practices and public gaffes. Competitors and whistleblowers are a major source of tips about privacy wrongdoing.

Require Disclosure of System Changes

Sophisticated companies can game the assessment process. One approach is to perform two assessments—an initial one for internal use that gives the company an opportunity to fix any deficits, and a second, post-intervention assessment that is sent to the FTC. It makes strategic sense to follow this two-step approach, and there is nothing inherently wrong about a company wanting to know how its operations really stack up. But what does it mean when the second assessor avers that the company was in compliance at all times? Shouldn’t management tell the second assessor about the deficits found during the first assessment?

More problematic is another approach sometimes seen in payment system auditing—altering practices or network architecture before the assessment so that it can be changed back after the outside team leaves. This problem could be easily addressed: FTC consent orders could require that the management state whether material changes to systems have been made prior to the assessment. The FTC could then evaluate the reasonableness of these changes.

Make Assessments More Public

The FTC itself urges companies to redact their assessments. Of course security-sensitive information needs to be withheld to prevent publication of an attack road map. However, many assessments are redacted as heavily as if they involved national security concerns. Excessive redaction robs the public of the ability to evaluate both company and FTC performance. If assessments were less redacted, technologists, academics, and plaintiff lawyers could help police respondents.

One alternative to improving assessments is a market approach. We could correct the deficits in the privacy market by levying eye-popping fines against privacy violators and trust that fear of more fines will cause internal self-policing. Such an approach might be more effective because money spent on assessments could be redirected to investment in privacy by design. But alas, our Bill of Rights has been interpreted to shield companies against ultra-large fines. In addition, many consumer protection agencies can’t levy large fines, and those that can, fear...
that the institution will be targeted politically as anti-business, as the FTC was when it proposed to regulate television advertising to children.

If large fines were available, it might be economically rational to risk them. The FTC, with its $300 million budget—smaller than the US Consumer Financial Protection Bureau and dwarfed by the US Food and Drug Administration—can pursue only a small number of companies. Most privacy and security problems go undetected, and those that are detected can’t all be policed. Even those companies in the spotlight, such as Google, might deem the fines acceptable business risks. Consider Google’s Buzz case, in which the company automatically enrolled users into Google’s new social network service. If it had successfully dislodged Facebook’s dominance over social networking, paying even a 10-figure fine would have been economically sound. For these reasons, the large fines and market approaches are unlikely to be pursued and unlikely to be successful.

Realistically, we have to live with the assessment approach, but the five steps I describe in this article can make assessments more meaningful.

Acknowledgments
I thank Megan E. Gray, from Stanford’s Center for Internet & Society, for sharing her insights on assessments, which she is researching in greater detail.

References