# Understanding and Improving Privacy "Audits" under FTC Orders

**April 2018**

**by Megan Gray**

## Table of Contents

# Understanding and Improving Privacy "Audits" under FTC Orders

**April 2018**

**by Megan Gray***

## I. Introduction

The Federal Trade Commission (FTC) is the primary federal agency protecting consumer privacy. The agency regularly touts its important and extensive work as the chief consumer privacy "cop on the beat." But this chest-thumping can backfire -- consumers may more readily share personal information via online platforms based on a belief that the FTC is guarding against misuse. The FTC actually has pursued only a small number of privacy cases relating to a company's unreasonable or excessive collection, use, and retention of consumer data, carving out those instances when the company acts contrary to an express privacy statement, fails to adequately protect against malicious and unknown hackers, or violates a specific federal statute (e.g., COPPA, FCRA).

This is why the FTC's 2011 and 2012 orders against Google and Facebook were heralded so heartily. For the first time, it was thought, the FTC had the unambiguous ability to ensure the companies instituted reasonable privacy protections.[1] As Berin Szoka of Tech Freedom noted, "the FTC is finding a way to regulate online privacy sans national legislation directly addressing the issue."[2] Moreover, the orders required independent,

---

* The author is a non-residential Fellow at Stanford Law School's Center for Internet and Society. This is a paper in progress, published to stimulate discussion and critical comment. The author has researched and written this paper, based on publicly available documents, in her non-work, non-family time, which is necessarily limited; she anticipates future edits will greatly improve on this draft. The views expressed in this paper are those of the author and do not necessarily reflect the author's past, present, or future employers or clients.

[1] The orders state the company must "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information. Such program, the content and implementation of which must be documented in writing, shall contain privacy controls and procedures appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the covered information..."

[2] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

third-party audits, it was thought, to verify the companies' compliance, thereby relieving any concern the FTC did not have the resources to monitor compliance.[3]

David Vladeck, the then-Director of the FTC's Consumer Protection Bureau, asserted, "I think the [audit] commitment that Google and Facebook have made is really an important one. Auditors are going to come in and make sure they are actually meeting the commitments laid out in their privacy policy. The audits are designed to make sure that companies bake privacy in at every step of offering a product or service. This is going to require the expenditure of a lot of money and a lot of time for companies that did not start out doing things this way. ….They've got to go back and rebuild their business in a way that takes privacy into account."[4]

According to Maneesha Mithal, of the FTC's Privacy and Identity Protection Division, "The main difference is that a [data breach] security audit is about how to protect info from unauthorized access, while a privacy audit is about how to protect info from authorized *and* unauthorized access."[5] An outside privacy expert elaborated: "[D]ata security audits...focus on ensuring that information the company has on us isn't vulnerable to hackers. But a privacy audit focuses more on how a company is using

---

[3] Not all FTC privacy or data security cases have a third-party audit provision. *See*, e.g., *FTC v. Frostwire, LLC* (2011), https://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon.

[4] "The FTC Privacy Cop Cracks Down" by Technology Review (June 26, 2012), https://www.technologyreview.com/s/428342/the-ftcs-privacy-cop-cracks-down/. *See also* David Vladeck closing letter to Google on the StreetView wi-fi collection: "...Google should develop and implement reasonable procedures, including collecting information only to the extent necessary to fulfill a business purpose, disposing of the information no longer necessary to accomplish that purpose, and maintaining the privacy and security of information collected and stored." https://www.ftc.gov/enforcement/cases-proceedings/closing-letters/google-inquiry.

[5] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/. *See also* 2012 FTC letter to Commenter Meg Roggensack of Human Rights First: "[T]he order requires Facebook to...obtain biennial privacy audits by an independent third-party professional. We believe that the biennial privacy assessments will provide an effective means to monitor Facebook's compliance with the order, including with respect to its relationship with its service providers. Each assessment will involve a detailed, written evaluation of Facebook's privacy practices over a two-year period, and will require the auditor to certify that Facebook's privacy controls have adequately protected the privacy of 'covered information' throughout the relevant two-year period." https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookcmbltrs.pdf.

someone's personal information internally -- how it's aggregated or re-purposed -- and when it's being shared with third parties (such as advertisers)."[6] Jim Kohm, of the FTC's Enforcement Division, predicted that any audit might take an entire six months to conduct, and would likely cost hundreds of thousands of dollars.[7]

## II. Closer Inspection of FTC Privacy Orders

The initial excitment eventually dissipated. On closer inspection, the orders arguably did not require "reasonable privacy protections." Rather, the orders were more constrained, and required only a "comprehensive privacy program" that was "reasonably designed" to "address" "privacy risks." Under this language, given the companies' lengthy privacy policies essentially stating that users did not have any privacy, the FTC could face an uphill battle in asserting misuse of consumer data. This struggle would be complicated by the orders' inclusion of a reasonableness standard – the FTC carries the burden of proof in any judicial proceeding, and (arguably) no consensus exists on reasonableness in this context. Moreover, in transforming any privacy case against the companies from a Section 5-based violation into an order-based violation, the FTC arguably increased its challenges, because it would have to relinquish control over any such case -- the Department of Justice (DOJ), not the FTC, litigates the agency's civil penalty cases.[8]

---

[6] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

[7] "So What Are These Privacy Audits That Google and Facebook Have To Do For the Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/.

[8] 15 U.S.C. §56(a) (1). If DOJ rejects the case or does not file the civil penalty action within 45 days, the FTC can file the lawsuit itself, but DOJ rarely declines FTC referrals. Few practitioners understand the legal intricacies distinguishing an FTC civil penalty case, an FTC contempt case, and an FTC Section 5 case (which itself can be subdivided into Section 5 administrative cases and Section 5 federal court cases). Key points: (a) violation of an FTC administrative order (e.g., Google, Facebook) is a civil penalty case, filed by DOJ in the name of the United States; it carries a "preponderance of evidence" standard of proof and can result in money fines without evidence of actual consumer harm, as well as injunctive relief; (b) violation of an FTC federal court order (e.g., Wyndam) is a contempt action filed by the FTC; it carries a higher "clear and convincing" standard of proof, and monetary awards are difficult to obtain in the privacy context; (c) Section 5 privacy cases carry a "preponderance of evidence" standard of proof, but, when the consumer has incurred no direct out-of-pocket loss, the company almost never pays money; and (d) Section 5 administrative cases cannot result in a monetary award, but, following the conclusion of the case, the FTC can file a second case in federal court under Section 19 to obtain financial resitution for consumers.

As a result, the third-party audits took on added significance. Because the public versions of those audits are heavily redacted and written in almost impenetrable language, the public learned little.[9] Careful review, however, shows the audits are woefully inadequate."[10]

## III. Closer Inspection of Privacy "Audits" Under FTC Orders

The third-party "audits" required under FTC orders sound more impressive than they actually are.[11] For example, the Google audits evaluate just seven points, so vague or duplicative as to be meaningless. In sum: (1) Google has a written, comprehensive privacy program; (2) Google has specific employees working on the privacy program; (3) Google has a privacy risk assessment process and undertakes to mitigate those risks; (4) Google has procedures to address identified privacy risks; (5) Google monitors the effectiveness of its privacy program; (6) Google has contracts with third parties who are capable of protecting privacy; and (7) Google evaluates and adjusts its privacy program as needed when its business changes.

---

[9] Redacted versions are available on ftc.gov and epic.org. Standard FTC order language can confuse. FTC orders require an initial compliance report, which is written by the company itself and is fully available to the public (i.e., unredacted). The initial third-party "assessment" is submitted later, with only a redacted version publicly released; subsequent third-party assessments, depending on particular order requirements, might not be submitted to the FTC at all. *See*, e.g., https://epic.org/privacy/ftc/googlebuzz/FTC-Initial-Assessment-09-26-12.pdf, https://epic.org/foia/FTC/facebook/EPIC-14-04-26-FTC-FOIA-20130612-Production-2.pdf, https://epic.org/foia/FTC/facebook/EPIC-13-04-26-FTC-FOIA-20130612-Production-1.pdf, https://www.ftc.gov/system/files/documents/foia_requests/1209googleprivacy.pdf. The initial third-party Google privacy assessment, as posted at epic.org, appears to be missing page
24 but is available at ftc.gov (with the entire page redacted).

[10] *See* "Assessing the FTC's Privacy Assessments, by Chris Hoofnagle (2016), https://ieeexplore.ieee.org/document/7448350/. *See also* Robert Gellman's critique of the audits conducted by the self-regulatory organization Network Advertising Initiative (NAI): "Lacking in Facts, Independence, and Credibility:
The 2011 NAI Annual Compliance Report" (July 2012), https://bobgellman.com/rg-docs/RG-NAI-2011.pdf.

[11] "Why Facebook's 2011 Promises Haven't Protected Users," Wired (April 11, 2018) (discussing third-party audits), https://www.wired.com/story/why-facebooks-2011-promises-havent-protected-users/.

This seven-point privacy program was "audited" by an independent, third-party "assessor," whose role was merely to find some evidence that supported actual implementation of the seven points. For example, the auditor confirmed that Google has a publicly available, written privacy policy; employees who focus on privacy risks; privacy training for some employees; privacy settings available for users; a form for managers to complete when a privacy issue arises; and contractual privacy provisions with third parties.[12]

These assessments could not be more starkly different from what FTC management described in earlier news reports.[13] What happened?

[12] Some businesses, particularly small start-ups, may only need a de minimus privacy program like this. *See* AICPA's Privacy Maturity Model, https://iapp.org/media/pdf/resource_center/aicpa_cica_privacy_maturity_model_final-2011.pdf. While FTC orders require assessors to "explain how the privacy controls are appropriate to the respondent's size and complexity, the nature and scope of the company's activities, and the sensitivity of the covered info," assessors do not appear to do so, other than to verbatim parrot that text. For example, in answering this question, the Facebook assessor intones, "Based on the size and complexity of the organization, the nature and scope of Facebook's activities, and the sensitivity of the covered information (as defined in by [sic] the order), Facebook management developed the company-specific criteria (assertions) detailed on pages 77-78 as the basis for its Privacy Program. The management assertions and the related control activities are intended to be implemented to address the risks identified by Facebook's privacy risk assessment."

[13] "We don't want [an auditor] who is going to just rubber stamp their procedures," said the FTC's Jim Kohm. "So What Are These Privacy Audits That Company and Facebook Have To Do For The Next 20 Years?" by Kashmir Hill, Forbes (Nov. 30, 2011), https://www.forbes.com/sites/kashmirhill/2011/11/30/so-what-are-these-privacy-audits-that-google-and-facebook-have-to-do-for-the-next-20-years/. While the agency may not have fully appreciated this rubber-stamp risk when the orders issued, it became aware of the problem at some later point. *See,* e.g., World Privacy Forum comment in *FTC v. Uber* (September 2017), "While this requirement for assessments appears impressive on the surface, it has serious shortcomings. The obligation for an assessment is less than meets the eye.... Commission staff also sometimes refers to the assessments as audits.... We find this to be significantly misleading. We suggest that any Commission staff member who discusses a Commission consent decree in public and who refers to an assessment as an audit be required to stay after work and write 100 times '*An assessment is not an audit*'....", https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141341.pdf.

## IV. An "Attestation" Is a Type of "Audit," Which Is a Type of "Assessment" that Relies on "Assertions"

Of the many audit models available from national and international standard-setting bodies, Google and Facebook selected the "attestation" model, which relies on conclusory hearsay, formally known as "management assertions."[14] As a result, assessments can be circular (e.g., "Management asserts it has a reasonable privacy program. Based on management's assertion, we certify that the company has a reasonable privacy program.").[15] The FTC's privacy cases have not usually stemmed from intentional transgressions; rather, the cases usually arise from issues the company

[14] The contracts ("engagement letters") between the assessors and the assessed companies are not publicly available. *U.S. v. Consumer Portfolio Services* (a 2014 FTC civil penalty case) could provide model language: "The management letter between [the company] and the third party monitor shall grant Commission staff access to the third party monitor's staff, work papers, and other materials prepared in the course of the...audit...", https://www.ftc.gov/enforcement/cases-proceedings/112-3010/consumer-portfolio-services-inc.

Because the engagement letters are non-public, and because of the heavy redactions in the assessments themselves, one cannot be sure which auditing standards apply. The assessors may not have followed the professional standards by which they are bound. The assessments state they are attestation models governed by AICPA (American Institute of Certified Public Accountants) and IAASB (International Auditing and Assurance Standards Board). AICPA categorizes privacy audits as either attestation engagements, privacy review engagements, or agreed-upon (specified auditing) procedure engagements. AICPA further subdivides attestation engagements into SOC1, SOC2, and SOC3. Based on features of the redacted Google and Facebook assessments, they are likely SOC2 attestations. AICPA subdivides SOC2 into Type 1 and Type 2 engagements. AICPA's SOC2 Guide is only available for purchase. This Guide is an authoritative AICPA interpretation and application of AT Section 101, which is the official standard for a SOC2 engagement. SOC reports are a new development, following the auditing world's transition in June 2011 from SAS 70 (AICPA's Standards on Auditing Statements) to SSAE 16 (AICPA's Standards on Attestation Engagements), a transition to align more closely to IAASB (and its ISAE 3402, which incorporates ISAE 3000 as foundation).

[15] For example, the Google assessors use the following certification language: "In our opinion, 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 reporting period, in all material respects...based upon the Google Privacy Program set forth in Attachment A of Management's Assertion in Exhibit I." (emphasis added).

overlooked or did not adequately disclose to consumers. A privacy audit that relies on management assertions will rarely uncover these blind spots.[16]

In a similar assessment context, one security expert opined that the attestation certification is not a seal of approval because the standard allows the company itself to decide what risks to document and what risk-management processes to adopt. "In sporting metaphor, [the company] **gets to design their own high-jump bar, document how tall it is and what it is made of, how they intend to jump over it and then they jump over it. The certification agency simply attests that they have successfully performed a high-jump over a bar of their own design."** (emphasis added). He added: "What would be really interesting would be if the company publishes their security requirements, their standards, their policies and risk assessments, so everyone can see what kind of high-jump they have just performed -- how high, how hard, and landing upon what kind of mat? It would be that which would inform me of how far I would trust a company with sensitive data…"[17]

Another security expert elaborated: "An example illustrating the difference between assessing security and auditing security might help clarify this point. Let's look at access controls. One component of access control security is a strong password policy. An assessment would check to see if the organization has a strong password policy while a security audit would actually attempt to set up access with a weak password to see if the control actually has been implemented and works as defined in the policy."[18]

Similarly, a ComputerWorld article trivialized an Uber privacy audit.[19] The article quotes from the purported audit: "While it was not in the scope of our review to perform a technical audit of Uber's data security controls, based on our review of data security policies and interviews with employees, we found that Uber has put in place and continues to develop a data seurity program that is reasonably designed to protect

[16] Arguably, a privacy audit relying on management assertions is wholly unsuitable when the company has been recently fined by a government agency for being less than forthright during an investigation into the company's privacy practices. In 2012, the Federal Communications Commission (FCC) fined Google on this basis in connection with its StreetView program. https://apps.fcc.gov/edocs_public/attachmatch/DA-12-592A1_Rcd.pdf.

[17] https://www.dogsbodytechnology.com/blog/iso27001-certification/.

[18] http://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm.

[19] http://www.computerworld.com/article/2880596/uber-shows-how-not-to-do-a-privacy-report.html.

Consumer Data from unauthorized access, use, disclosure, or loss."[20] The article made this point: "Let's zero in on the key utterance: 'it was not in the scope of our review to perform a technical audit of Uber's data security controls.' Based on the report and its stated methodology, the investigators weren't trying to see if Uber really obeyed its own written privacy policies. It was merely allowed to see if that written policy was an appropriate policy. But privacy policies, written by lawyers and HR specialists, are rarely the problem. The problem tends to be what employees actually do."[21]

## V. Avenues to Improve FTC Privacy Assessments

The FTC's third-party privacy assessments have the potential to be an incredibly important component of the agency's enforcement program, especially given the Commission's small size and budget. The FTC, if so inclined, could pursue a variety of avenues to obtain better assessments. Most obvious, the FTC could state that "attestations" do not comply with an order's assessment provision. However, the term "assessment" is not well defined in the orders – and a common legal principle is that ambiguous terms are construed against the drafter. That said, this doctrine arguably would not apply in this situation (e.g., the term is not ambiguous because the standard dictionary definition should apply, not a technical certified-auditor definition).

Alternatively, the FTC could go beyond any submitted assessment, and conduct its own assessment under a diferent order provision.[22] The orders require companies to retain all materials that call into question the company's compliance with the order, as well as all materials relied on in preparing the assessment. Moreover, companies must respond to any relevant FTC inquiry within ten days.[23] Under these provisions, the FTC could obtain, for example, any assessment submitted to the company itself or other regulators,

---

[20] The redacted version of the Google assessment contains a similar disclaimer. "We are not responsible for Google's interpretation of, or compliance with, information security or privacy-related laws."

[21] Commenters to FTC privacy orders have raised these issues to the Commission, but the agency has not altered the assessment provision. *See* World Privacy Forum comment in *FTC v. Uber* (September 2017), https://www.ftc.gov/system/files/documents/public_comments/2017/09/00010-141341.pdf.

[22] *But see* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.* (FTC should not fault a company's data security if a third-party assessor approved it), https://www.ftc.gov/public-statements/2015/12/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v.

[23] *U.S. v. Morton Salt Co.*, 338 U.S. 632, 650 (1950).

domestic or foreign, and use that assessment to identify discrepancies or any areas for improvement.[24]

### A. Improving Attestation Assessments

But even if the FTC did not want to entirely reject the submitted assessments or mount an argument against the "choice of model" (i.e., attestation), the FTC could insist companies submit revised assessments, improved in numerous ways, while still operating under the attestation framework. A properly designed attestation with sufficient granularity will look very much like an audit.

#### 1. Examination Focus (Scope)

At the onset, an assessor determines the scope of the project. For a large company, attestation guidance seems to require a privacy assessment to be separately conducted along product lines.[25] By lumping multiple Google divisions (e.g., automonous cars, YouTube, search, email, voice-activated assistant, etc.) into a single privacy assessment, and using the same measuring stick for all, an assessment will have such a high level of abstraction (review at 10,000-foot level) that it serves no useful function. Noting that the redacted 2012 Google assessment is a mere 22 pages, one privacy professor opined, "How could such a short document account for all the company's information collection and handling activites from its multiple product lines?"[26]

---

[24] *See* the Irish Data Protection Commission's requirement that Facebook implement 45 granular privacy changes. As conveyed in the cover letter to the Facebook initial assessment, "Our privacy efforts received a substantial boost in 2011 and 2012, when the Data Protection Commissioner in Ireland [reviewed our compliance] with European data protection law. That review resulted in two comprehensive audit reports that documented Facebook's controls...and identified areas where we can continue to improve."

[25] "The scope of the engagement can cover (1) either all personal information or only certain identified types of personal information, such as customer information or employee information, and (2) all business segments and locations for the entire entity or only certain identified segments of the business (retail operations, but not manufacturing operations or only operations originating on the entity's web site or specified web domains) or geographic locations (such as only Canadian operations). In addition, the scope of the engagement generally should be consistent with the description of the entities and activities covered in the privacy policy." www.webtrust.org/download/Trust_Services_PC_10_2006.pdf.

[26] *See* "Assessing the FTC's Privacy Assessments, by Chris Hoofnagle (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2707163.

Similarly, Google and Facebook regularly acquire a large number of companies.[27] Their redacted assessments do not indicate how those acquisitions are folded into either the company's privacy program or evaluated during the assessment period.[28] Ironically, immediately after touting the wide variety of Google services, 30,000 employees, and 70 offices in 40 countries, the Google assessor claimed that user data falls into only 3 categories: log data, account data, and [redacted].

Given these odd attributes, the FTC could insist on revised assessments with more appropriate and explicit scoping parameters. *See U.S. v. Upromise* (2017 FTC civil penalty order violation case alleging, among other issues, that "Upromise obtained and submitted assessments that were impermissibly narrow in scope...").[29]

### 2. Protocol Issues (Selection of Controls and Criteria)

Many detailed protocols exist for evaluating privacy programs. The standard-bearer is AICPA's GAPP (for "generally accepted privacy principles"), which is comprehensive and granular, even providing extensive illustrative privacy controls).[30] The Google and

[27] https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet.

[28] The most recent Google assessment identifies its Motorola acquisition, but unilaterally carves out its compliance for over a year after the acquisition. Of separate interest, FTC orders have a provision requiring companies to report "any change in [the company] that may affect compliance obligations arising under this order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order..." (emphasis added). Arguably, the emphasized text requires reports on many acquisitions, particularly those implicating user data enhancement or user profile applications.

[29] https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc.

[30] GAPP is of course different from GAAP ("generally accepted accounting principles"). *See* https://en.wikipedia.org/wiki/Generally_Accepted_Privacy_Principles; http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_Principles%20and%20Criteria.pdf. At last check, GAPP was being updated. ISACA (Information Systems Audit and Control Association) may also have a robust privacy protocol (denominated G31). Microsoft also promotes a robust, well-documented data governance program, https://download.microsoft.com/download/2/0/a/20a1529e-65cb-4266-8651-1b57b0e42daa/protecting-data-and-privacy-in-the-cloud.pdf, https://www.microsoft.com/en-us/trustcenter/about/transparency, https://www.microsoft.com/en-us/trustcenter/privacy/we-set-and-adhere-to-stringent-standards. Aprio is another entity that provides extensive auditing protocols for online businesses, https://www.aprio.com/wp-content/uploads/aprios-iso-27001-certification-program2.pdf.

Facebook assessments rejected GAPP in favor of customized checklists, which bear no resemblance to GAPP.[31]

By using tailor-made controls and criteria within an attestation framework, the Google and Facebook assessments are almost indecipherable, requiring certified-auditor knowledge.[32] The auditing profession uses dense and confusing terms, the meanings of which are often counter-intuitive or have a heightened-scrutiny illusion. For example, a company could be subject to an auditor's "examination" and "testing" of certain data – but this activity could be as simple as the auditor confirming that the company has a posted privacy policy. For example, the Google assessor states that it "independently tested each Google privacy control listed in the Management Assertion and Supporting Privacy Controls" and "[o]ur test procedures included, where appropriate, selecting samples and performing a combination of inquiry, observation, inspection, and/or examination procedures." Yet, pursuant to auditor nomenclature, the assessor's "inquiry test" could have been merely interviews of certain employees to ask rote questions repeating the management assertions. Similarly, while it may be reassuring to learn an assessor reviewed thousands of individual artifacts that were collected from dozens of company employees, in reality, this is meaningless without additional context (e.g., what is an artifact, were any duplicative or irrelevant).[33]

To better understand the protocol grounds on which the FTC could question the assessment, one must understand two key terms. "Controls" are policies and procedures that address risks associated with reporting, operations, or compliance and, when

---

[31] Confusingly, while the Google assessment claims to follow AICPA, it does not track GAPP. Rather, the assessment complies with AICPA rules for attestation engagements; it does not follow AICPA for the substantive protocol. AICPA procedural rules do not require use of the GAPP substance for controls/criteria; AICPA says use of GAPP is merely a recommendation. Thus, both use and non-use of GAPP is a "procedure and standard generally accepted in the industry," which is the applicable FTC order requirement. Similar to Google, the Facebook initial compliance report and the cover letter to its initial assessment claim it has adopted the GAPP framework as a benchmark, but that is not borne out in the mangement assertions undergirding the assessment. However, "[I]f a practitioner does not apply the attestation guidance [i.e., GAPP] included in an applicable attestation interpretation, the practitioner should be prepared to explain how he or she complied with the SSAE provisions addressed by such attestation guidance." AICPA AT Section 50 (para 6), Defining Professional Requirements in Statements on Standards for Attestation Engagements.

[32] While the FTC often hires consultants for technical issues, it has a limited budget. The agency could request assistance from its sister agency, the U.S. Governmental Accounting Office (GAO); James Dalkin is a GAO director with expertise in AICPA attestations.

[33] *See also* AICPA AU 325 (standards for defining "deficiency in internal control," "significant deficiency," and "material weakness").

operating effectively, enable an entity to meet specified "criteria." "Criteria" are the benchmarks used to measure compliance with the controls. In an attestation, company management selects the criteria. However, the standard-setting body for auditors conducting attestations states that "any relevant factors [that are] omitted [can not] alter the conclusion [of the report]."[34] The FTC could point to a plethora of missing, conclusion-altering factors that make the selected controls and/or criteria inadequate, as detailed below.

**i. Failure to Assess Fair Information Principles:** The FTC could insist the protocol include the long-standing Fair Information Principles (FIPs) -- Notice, Choice/consent, Access/participation, Integrity/security, Enforcement/redress, Use Limitation/deletion.[35] The 2012 White House's Consumer Privacy Bill of Rights also included Respect for Context, Focused Collection, and other elements.[36] An assessor who excludes a FIP from the protocol should expressly justify its exclusion. Some audits assert, "The scope of the engagement should cover all of the activities in the information cycle for relevant personal information. These should include collection, use, retention, disclosure, disposal, or anonymization. Defining a business segment that does not include this entire cycle could be misleading to the user of the practitioner's report."[37]

---

[34] *See* AT 101.24. For example, when parsed, the Google assessment shows that its management, not its auditor, determined the criteria ("PWC used pre-defined materiality criteria developed during the planning phase"). *See also* ISAE 3000, another pertinent auditing standard: "If criteria are specifically designed for the purpose of preparing the subject matter information in the particular circumstances of the engagement, they are not suitable if they result in subject matter information or an assurance report that is misleading to the intended users. It is desirable in such cases for the intended users or the engaging party to acknowledge that specifically developed criteria are suitable for the intended users' purposes. The absence of such an acknowledgement may affect what is to be done to assess the suitability of the applicable criteria, and the information provided about the criteria in the assurance report." https://www.ifac.org/publications-resources/international-standard-assurance-engagements-isae-3000-revised-assurance-enga. When last reviewed, ISAE 3000 was being finalized, and PriceWaterhouseCoopers submitted comments to weaken this portion.

[35] "Fair Information Practices: A Basic History," Bob Gellman, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. *See also* the 2017 privacy advocates' letter to FTC commissioners on incorporating FIPs into the agency's privacy work, https://epic.org/privacy/internet/ftc/EPIC-et-al-ltr-FTC-02-15-2017.pdf.

[36] *See* https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b.

[37] *See* www.webtrust.org/download/Trust_Services_PC_10_2006.pdf.

**ii. Failure to Map Data Flow of Consumer Information:** Data flow maps are usually the key aspect of privacy audits.[38] "Understanding the data associated with personal information is useful for identifying the processes that involve or could involve personal data, and for the owner of those processes. By identifying the processes and business owners of personal information, the business can then understand the end-to-end flow of personal information including:

- Definition of specific personal information about customers and employees the organization collects and retains, including the methods in which this information is obtained, captured, stored, and transmitted.
- Definition of specific personal information that is used in carrying out business, for example, in sales, marketing, fundraising, and customer relations, including the methods in which this information is obtained, captured, stored, and transmitted.
- Definition of specific personal information that is obtained from, or disclosed to, affiliates or third parties, for example, in payroll outsourcing, including the methods in which this information is obtained, captured, stored, and transmitted.
- Identification of infrastructure components used in the receipt, processing, recording, reporting, and communication of personal information.
- Identification of personnel (including third parties) that have been granted access or potentially could access the personal information and how."[39]

From the redacted assessments, it appears companies do not map their internal or external data flows of consumers' personal information, and therefore are unable to assess whether such data goes astray. Without this, it's practically impossible to evaluate compliance with any standard.

**iii. Failure to Determine Notice and Consent:** Privacy policies are ubiquitous. Lesser known is that the FTC does not require such policies. Instead, the FTC mainstay is "notice and consent," and simply posting a privacy policy does not neccessarily satisfy this standard. Arguably, if a company knows or should know its consumers do not understand, and therefore cannot consent to, data collection, sharing, or

---

[38] *See* Keith Enright (now Google's Privacy Legal Director), "Privacy Audit Checklist," https://cyber.harvard.edu/ecommerce/privacyaudit.html. Mitre also provides an example of data mapping in privacy audits, https://www.mitre.org/publications/technical-papers/how-to-conduct-a-privacy-audit. It is difficult to imagine that any privacy program could effectively function without the company knowing what information it collects from consumers. It would be disappointing if Google or Facebook does not even internally keep an inventory of cookies or apps existing on its website. *See* University of California Berkeley Law's Web Privacy Census, with inventory of deployed cookies, https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/web-privacy-census/ (last conducted in 2012).

[39] https://www.journalofaccountancy.com/issues/2011/jul/20103191.html.

retention, the company has not satisfied its obligations to provide notice or obtain consent. As alleged in the *U.S. v. Upromise* complaint for violating a FTC privacy order, "...Upromise disclosed this information in such a way that many consumers would either not notice or not understand Upromise's explanation of the ... toolbar's data collection and use."[40] The assessments do not appear to evaluate whether consumers had actual notice or effectively consented to the companies' data pratices.

**iv. Failure to Identify Privacy Promises:** Large online companies regularly assure consumers (and regulators) that privacy is the core of their business. Such statements are frequently specific and issued at the highest level. For example, Google has a YouTube channel dedicated to privacy.[41] Yet, these company privacy statements do not appear to be inventoried or reviewed, apart from the company's essentially static, official privacy policy. The redacted assessments do not appear to identify or evaluate adherence to these more peripheral privacy statements.

**v. Failure to Analyze Order Violations:** The redacted assessments do not appear to address previously identified order violations or other breaches of self-regulatory programs that occurred or were discovered during the assessment period. For example, while the initial Google assessment covered the time period scrutinized in the FTC's Safari case, the assessement does not mention it, at least in the redacted version.

---

[40] *See also FTC v. Paypal* (Section 5 complaint for confusing privacy settings), https://www.ftc.gov/enforcement/cases-proceedings/162-3102/paypal-inc-matter. In the remedial *Upromise* order for violating the underlying privacy order, the FTC required the company to "obtain an evaluation and report from a qualified, objective, independent third-party professional specializing in website design and user experience ("evaluator")...For any disclosure or consent governed by Section I of the FTC Order, the evaluator must certify Defendant's adherence to the FTC Order's 'clearly and prominently' disclosure requirement and 'express, affirmative' consent requirement." https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc. *See also FTC. v. Special Data Processing Corp.* (2004 order describing independent, third-party verification of consumer telephonic consents), https://www.ftc.gov/enforcement/cases-proceedings/002-3213/special-data-processing-corporation. In 2014, the National Science Foundation awarded large money grants to researchers to devise effective privacy notices, https://iapp.org/news/a/researchers-earn-grant-to-study-privacy-notices/. *See also* Lauren Willis, "The Consumer Financial Protection Bureau and the Quest for Consumer Comprehension," proposing that CFPB require firms to demonstrate that a significant proportion of their customers understand key pertinent facts about purchased financial products. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2952485.

[41] https://www.youtube.com/user/googleprivacy. *See also U.S. v. Google* (alleging Google's misrepresentations based on (a) privacy statement not part of official privacy policy; and (b) compliance statement vis-a-vis NAI's Code of Conduct), https://www.ftc.gov/enforcement/cases-proceedings/google-inc.

As cited earlier, an assessment's failure to include known (or even suspected) material deviations from management assertions can crater the assessment's worthiness.

## VI. New FTC Commissioners May Revisit Privacy Assessment Requirements

The FTC will soon have an entirely new slate of commissioners. They may be amenable to a comprehensive overhaul of how the agency monitors its privacy orders.[42] For example, the commissioners could vote to issue a Policy Enforcement Statement, notifying all companies currently required to submit privacy asssessments that future assessments must have certain features or address particular subjects. The commissioners could also instruct staff to re-design the agency's model order language to explicitly require these characteristics in future orders.

More agressively, the Commission could pursue order modification.[43] The agency could also hire a consulting firm to create an auditing protocol applicable to all companies

---

[42] The prospect of massive civil penalties for administrative order violations is often overblown, and should not be presumed a strong deterrant. In the online context, a $41,484 per violation calculation may seem astronomical, but the statute and interpreting caselaw warrant caution. Under Section 15 U.S. Code § 45(*l*), administrative order violations can result in "no more than" that amount for each violation, with "[e]ach separate violation...[being] a separate offense, except that in a case of a violation through continuing failure to obey or neglect to obey [the order], each day of continuance of such failure or neglect shall be deemed a separate offense." If the order violation, for example, is a failure to require a vendor to sign a privacy pledge, that arguably is a single violation. In analyzing order violations, the first step is determining if the matter is a "continuing failure" or a discrete, affirmative violation. Depending on the answer to that question, the second step is counting either days or violations. And the final step is then calculating the suitable money amount for each day/violation. *See U.S. v. Reader's Digest Association, Inc.*, 464 F. Supp. 1037 (D. Del. 1979); *U.S. v. Alpine Indus.*, 352 F.3d 1017 (6th Cir. 2003) (FTC civil penalty calculated on per-day basis). Of note, the Supreme Court has indicated any civil penalty amount may have constitutional implications under the Eighth Amendment, because the civil penalty is paid to the government and determined by a jury. *United States v. Bajakajian*, 524 U.S. 321 (1998). The agency could be entirely precluded from seeking a civil penalty under the logic of *IntelliGender*, although its application to non-restitutionary civil penalties is questionable. *California v. IntelliGender*, 771 F.3d 1169 (9th Cir. 2014) (California Attorney General restitution claims in an unfair competition case precluded by a prior class action settlement on the same claims).

[43] The Commission can re-open proceedings on its own initiative to modify or set aside all or part of its order if it "is of the opinion that changed conditions of law and fact or the public interest" require it. 15 USC §45(b); 16 CFR §2.51(b). Under such circumstances, the Commission issues an order to show cause to all parties subject to the order, stating any proposed changes and the reasons the changes are needed. Each party must respond or object to the changes within 30 days; otherwise, the changes are made effective.

subject to privacy assessments. In 2011, for example, in connection with its plan to monitor healthcare providers' compliance with a new health privacy law (known as HIPAA), the Department of Health and Human Services (HHS) contracted with KPMG to develop audit protocols and assist with the audits.[44] Such a contract would be too expensive for the FTC, but the agency could seek a special appropriation from Congress or request Congressional approval to use civil penalty collections to fund the contract.

Less ground-breaking, FTC could send the company or its assessor an advance letter raising specific concerns or setting concrete expectations for the assessment.[45] In addition to the issues identified in this article, the new commission may find inspiration from the agency's "Start with Security" roadshows, which synthesized 10 principles from the agency's privacy work.[46] Needless to say, the Commission could also pursue

---

Parties themselves may also pursue order modification. The Commission recently approved Sears' petition to expand its order's online tracking provision, but did not require third-party assessments in the original order or its modification. *See* https://www.ftc.gov/news-events/press-releases/2018/02/ftc-approves-sears-holdings-management-corporation-petition.

[44] https://www.foley.com/hhs-initiates-pilot-audit-program-for-hipaa-compliance-11-22-2011/.

[45] The FTC could also send a "retroactive" letter. The legal doctrine of estoppel does not apply to government actions. *See* https://www.fcsl.edu/sites/fcsl.edu/files/ART%206.pdf. However, a five-year statute of limitations does apply to civil penalty actions. *U.S. v. Ancorp Nat. Servs.*, 516 F.2d, 198 (2d Cir. 1975); *see also Kokesh v. SEC*, 2017 WL 2407471 (U.S. Supreme Court, June 5, 2017). It is unclear if the clock starts when the violation occurs or when the agency learns of the violation. Thus, at least as a theoretical matter, the agency's prior acceptance of a company's assessment might not foreclose the Commission pursuing an order violation case less than five years following that assessment.

[46] *See also* the FTC's recent *Upromise* matter, requiring the FTC to pre-approve, not just the assessor, but the assessment's scope and design. https://www.ftc.gov/enforcement/cases-proceedings/102-3116-c-4351/upromise-inc. The Start (and Stick) with Security program addressed: (1) start with security; (2) control access to data sensibly; (3) require secure passwords and authentication; (4) store sensitive personal information securely and protect it during transmission; (5) segment your network and monitor who's trying to get in and out; (6) secure remote access to your network; (7) apply sound security practices when developing new products; (8) make sure your service providers implement reasonable security measures; (9) put procedures in place to keep your security current and address vulnerabilities that may arise; and (10) secure paper, physical media, and devices. https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business; https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

rulemaking.[47] The agency previously studied the assessors themselves, although to what end is unknown.[48]

The commissioners could also pursue bigger-picture concepts for improving oversight of its privacy orders, described in more detail below.

### A. Reconsider Legal Grounds for Redacting Assessments

Historically, the FTC has published compliance reports without any redactions, but published the assessments only in heavily redacted form.[49] The legal grounds for this disparity are unclear, and third parties seeking the assessments have not challenged the redactions in court. Evaluating whether assessment redactions are even permissible requires consideration of multiple statutes and rules. For example, the applicability of confidentiality rules and FOIA exemptions varies depending on whether the assessment is submitted pursuant to an administrative or court order, whether the assessment is characterized as being submitted voluntarily, etc.[50] A full analysis of this issue is beyond the purview of this article. That said, the subject is important enough to warrant brief discussion.

Evaluating whether the FTC is permitted to redact an assessment is not the end of the analysis. Assuming the agency has the authority to redact an assessment, the next question is whether the agency must do so. If not legally required to redact, the FTC should then consider whether the public would benefit from a full review of the

---

[47] The FTC already has a rule prohibiting some ad tracking - 16 CFR 14.12, enacted in 1978. *See* "It's Time to Remove the 'Mossified' Procedures for FTC Rulemaking," by Jeffrey S. Lubbers, George Washington Law Review, Vol. 83, p. 1979, 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560557 (finding materially longer time associated with the FTC's rulemaking under the Magnuson-Moss procedures, compared to rules enacted under the standard Administrative Procedures Act). *See also* "Performance-Based Consumer Law," by Lauren E. Willis, 82 University of Chicago Law Review 1309 (2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2485667.

[48] "FTC to Study Credit Card Industry Data Security Auditing," March 2016, https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing.

[49] Congress can obtain unredacted versions.

[50] Some FTC privacy orders (such as the Facebook order) do not require the company to submit its biennial assessments to the agency. Instead, the agency only requires the company to submit them "upon request." *See* FTC Operating Manual, Chapter 15 (Confidentiality and Access), https://www.ftc.gov/about-ftc/foia/foia-resources/ftc-administrative-staff-manuals.

assessment.[51] It may redound to the FTC's benefit to have public review and input on assessments, especially if the agency does not have sufficient resources or expertise to evaluate whether the assessors followed applicable auditing or technical standards.[52] Publication may also discourage over-reliance on management assertions, because that can negatively impact the auditor's reputation.

The agency should be prepared to counter an assessor's claim that applicable auditing rules require confidentiality of such reports. While an attestation-type audit may be a "restricted use" report, that does not mean the agency cannot distribute it. "Restricted use" merely means the assessor has to state in the report that it is not *intended* for distribution to nonspecified parties; the assessor is not responsible for controlling distribution. Indeed, the pertinent AICPA rule contemplates wide distribution: "In some cases, restricted-use reports filed with regulatory agencies are required to be made available to the public."[53] Similarly, while the contract between the assessor and the company can limit distribution, that contract does not bind the FTC.

### B. Have Assessors Report Directly to the FTC

The agency could restructure the privacy orders so the FTC hires (and directs) the assessors, with the subject company order paying for the work. The agency may initially balk at this idea due to the Miscellaneous Receipts Act (MRA). Under the MRA,

---

[51] The assessed companies would no doubt object and could file a court action to prohibit publication. Or perhaps not; *see* FTC disclosure of very specific data security audit materials in document previously filed under seal in the *LifeLock* data security contempt case, https://www.ftc.gov/about-ftc/foia/frequently-requested-records/lifelock (FOIA Number 2016-00462, Final Response to Requester [Jeff Chester]).

[52] The Public Interest Oversight Board (PIOB) oversees IAASB member compliance with its auditing standards. AICPA does not appear to oversee its members' compliance with Professional Attestation Standards (AT Section 101), but the organization is affiliated with The Center for Audit Quality (CAQ). *See* "Comparing Ethics Codes: AICPA and IFAC," Journal of Accountancy, https://www.journalofaccountancy.com/issues/2010/oct/20103002.html. In Nov. 2011, PCAOB published inspection findings for PriceWaterhouseCoopers (the Google/Facebook assessor), listing serious problems with more than a third of the company's financial audits. "Inspectors noted numerous instances of problems with the testing and disclosures related to fair value measurements and hard-to-value financial instruments and with goodwill impairment…[S]ome audit problems [were found] in areas that aren't typically flagged with great frequency in major firm reports, like excessive reliance on management representations, entity-level controls…" (emphasis added), https://pcaobus.org/Inspections/Reports/Documents/2011_PricewaterhouseCoopers_LLP.pdf.

[53] *See* AU Section 532. AUs are the official interpretations of AICPA requirements (similar to the Notes accompanying each Federal Rule of Civil Procedure).

whenever an agency obtains funds other than through a congressional appropriation, the agency must consider whether the MRA applies to those funds. Money can be "received" for MRA purposes either directly or indirectly. However, money is not considered received *for the government* when the agency does not use the money on its own behalf.[54] While an extensive review of the MRA is beyond the ambit of this article, suffice to note the MRA does not apply when an FTC order requires a company to spend money as part of a program designed to prevent future violations or counter the effects of violations. For example, the FTC may use funds from a defendant to accomplish fencing-in or corrective relief, when that is a reasonable remedy for the violation. When such an affirmative remedy is appropriate, but the agency is concerned whether the violator will in fact accomplish the remedy, the MRA does not preclude the violator paying for the FTC or another entity to carry out the remedy.[55]

### C. Identify and Support Violation Reporters

Historically, the agency has been loath to identify what sparks its privacy investigations.[56] But for internal purposes at least, the agency should track exactly how it

[54] When the Small Business Administration (SBA) was required by statute to perform annual assessments of certain companies, and the SBA required those companies to pay the third-party assessor, the GAO determined that the agency violated the MRA. In contrast, the FTC is not required to conduct assessments. *See* SBA's Imposition of Oversight Review Fees on PLP Lenders, B-300248 (Comp. Gen. Jan. 15, 2004). *See also* http://fcpablog.squarespace.com/blog/2014/10/1/the-much-misunderstood-miscellaneous-receipts-act-part-3.html.

[55] Although the FTC does not hire him directly, the FTC's *Herbalife* order authorizes the agency to terminate the independent compliance auditor and provides a replacement procedure. Notably, the compliance auditor in that case has to obtain advance FTC approval of his planned work and budget. If the FTC objects to the work plan or budget but the auditor does not resolve the matter to the FTC's satisfaction, the order provides a petitioning process to the court.
https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf

[56] ProPublica, for example, was unable to learn what sparked the FTC's investigation into the 2012 Google/Safari matter. *See* https://www.propublica.org/article/announcing-225-million-fine-ftc-says-investigated-googles-internet-tracking. Tracking the investigative spark will likely require corresponding attention to initial investigations and corollary requirements for internal document retention. *See* https://hoofnagle.berkeley.edu/2016/06/29/70-of-security-investigations-closed/. Doing so may be challenging; some of the FTC's privacy cases aren't even labeled as such. The International Association of Privacy Professionals (IAPP)'s casebook is designed to capture all FTC privacy and data security cases, but it does not (as one example) list *U.S. v. Consumer Portfolio Services*, a 2014 FTC civil penalty case in which the order required a comprehensive "data integrity" program and used the "audit" term.
https://www.ftc.gov/news-events/press-releases/2014/05/auto-lender-will-pay-55-million-

learns of privacy violations, whether from internal forensic research, company whistleblowers, competitive tattletales, advocacy groups, journalists, etc. If, for example, the FTC's privacy cases are often a result of whistleblowers, knowledge of that fact can help the FTC develop best practices to encourage whistleblowers to come forward, either directly to the FTC or to the assessors.[57]

Indeed, the FTC could require assessors to consider credible privacy complaints. Well-informed consumer groups regularly send lengthy and detailed complaints to the FTC; perhaps assessors should be explicitly required to evaluate their merits (in addition to the FTC's evaluation).

In addition, given consumer groups' technical and time investment in drafting these complaints – particularly if the FTC's internal review identifies them as a frequent source of its cases – the agency could consider a order provision requiring the company to "promptly and thoroughly investigate any complaint received by [company] relating to compliance with this Order and to notify the complainant of the resolution of the complaint and the reason therefor," as the Commission required in the *Herbalife* multi-level marketing order.[58]

### D. Create Positive Incentives for Subject Companies to Report Violations Independently of Assessments

Audit experts often point to an effective compliance program model developed by the U.S. Sentencing Commission.[59] The key attribute is an incentive to self-report violations. Currently, a company under FTC order has no incentive to report deficiencies in its privacy program. In fact, because data misuse (unlike data breaches) is often never discovered, a company actually has a disincentive to report problems. Rather than relying on an assessor's sleuthing abilities or a company's good faith, the FTC may be

---

settle-ftc-charges-it-harassed. Another complication may be that the FTC's records disposition requirements have not been updated since 2009. *See* National Archive and Records Administration (NARA) document N1-122-09-1, https://www.archives.gov/files/records-mgmt/rcs/schedules/independent-agencies/rg-0122/n1-122-09-001_sf115.pdf.

[57] "Ex-Facebook insider says covert data harvesting was routine," The Guardian (March 20, 2018) (describing his unsuccessful efforts in 2011 and 2012 to persuade senior Facebook executives to exercise contractual audit provisions on external developers siphoning consumer data, and his decision to denounce the company in a 2017 New York Times op-ed), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[58] https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf.

[59] *See,* e.g., http://www.acc.com/legalresources/quickcounsel/eaecp.cfm.

well served by developing a program similar to that used by the U.S. Sentencing Commission.

"[W]hen the [U.S. Sentencing] Commission promulgated the organizational guidelines, it attempted to alleviate the harshest aspects by incorporating the preventive and deterrent aspects of systematic compliance programs. The Commission did this by mitigating the potential fine range if an organization can demonstrate that it had put in place an effective compliance program. This mitigating credit under the guidelines is contingent on prompt reporting to the authorities and the non-involvement of high-level personnel in the actual offense."[60] Other attributes of the mitigation program include:

- Oversight by high-level personnel
- Due care in delegating substantial discretionary authority
- Effective communication to all levels of employees
- Reasonable steps to achieve compliance, which include systems for monitoring, auditing, and reporting suspected wrongdoing without fear of reprisal
- Consistent enforcement of compliance standards including disciplinary mechanisms
- Reasonable steps to respond to and prevent further similar offenses upon detection of a violation

Devising a similar program at the FTC might not require legislative changes or rule-making.[61] In fact, the FTC has created safe harbors in other contexts, simply by issuing a Policy Enforcement Statement or including such a provision in a consent order.[62]

---

[60] https://www.ussc.gov/sites/default/files/pdf/training/organizational-guidelines/ORGOVERVIEW.pdf.

[61] *See*, e.g., FTC's Civil Penalty Leniency Program for Small Entities, https://www.ftc.gov/policy/federal-register-notices/notice-regarding-compliance-assistance-and-civil-penalty-leniency. *See also* the FTC's Funeral Rule Offender's Program (FROP). In conjunction with the National Funeral Directors Association (NFDA), the FTC created an industry self-certification and training program to increase Funeral Rule compliance. FROP offers a non-litigation alternative for correcting apparent "core" violations of the Funeral Rule. Violators may, at the Commission's discretion, be offered the choice of a conventional investigation and potential law enforcement action (resulting in a federal court order and civil penalties) or participation in FROP. Violators choosing to enroll in FROP make voluntary payments to the U.S. Treasury or state Attorney General, but those payments are usually less than what the Commission would seek as a civil penalty. NFDA attorneys then review the funeral home's practices, bring them into compliance with the Funeral Rule, and then conduct on-site training and testing. https://www.ftc.gov/reports/staff-summary-federal-trade-commission-activities-affecting-older-americans-during-1995-1996.

[62] For example, the FTC laid out its requirements for Section 5's "unfairness" grounds in its 1980 Policy Statement, https://www.ftc.gov/public-statements/1980/12/ftc-policy-

Alternatively, the FTC could more affirmatively inject a mitigation process into a company's privacy program. The Consumer Financial Protection Board (CFPB)'s 2016 data security order could provide a model. In addition to requiring a third-party audit (using the term "audit"), the order incorporates the common-sense realization that a robust audit is likely to identify some deficiencies at every company. With this in mind, the order lays out a process for the company to create a post-audit mitigation plan, which the company submits to the CFPB for approval along with the audit report.[63]

### E. Require Board of Director Responsibility for Assessments

The FTC could require a company's board of directors to bear ultimate responsibility for order compliance. For example, the FTC could require a company's board of directors to review the third-party assessment and create a compliance plan.[64] Another model could be the 2002 Sarbanes-Oxley Act, which mandated certain corporate processes to ensure accurate financial reports, with extensive corporate board responsibilities for certifying those reports.[65]

---

statement-unfairness. The FTC has also rescinded its policy statements, as shown by the 2012 withdrawal of the agency's Policy Statement on Monetary Remedies in Competition Cases, https://www.ftc.gov/news-events/press-releases/2012/07/ftc-withdraws-agencys-policy-statement-monetary-remedies. *See also U.S. v. Civil Development Group*, (2010 FTC civil penalty case) (from the Statement of Chairman Robert Pitofsky and Commissioner Sheila F. Anthony: "Part V of the Order provides respondents with a limited rebuttable presumption that they have exercised good faith in complying with key injunctive provisions of the Order, if respondents show, by a preponderance of the evidence, that they have established and maintained the education and compliance program mandated by Part IV.") https://www.ftc.gov/enforcement/cases-proceedings/civic-development-group-llc-scott-pasch-david-keezer-united-states.

[63] *In Re Dwolla*, https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/. Although not a privacy case, the FTC incorporated a corrective action concept with the independent compliance audit required in the *Herbalife* order, https://www.ftc.gov/system/files/documents/cases/160715herbalife-stip.pdf.

[64] *In Re Dwolla*, CFPB's 2016 data security order, contains this requirement. https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-dwolla-for-misrepresenting-data-security-practices/.

[65] *See* https://en.wikipedia.org/wiki/ Sarbanes–Oxley_Act.

### F. Clarify that Merely Obtaining an Assessment Is Not a Safe Harbor

After receiving an assessor's certification in conformance with an FTC order, a company could argue the FTC is precluded from contesting it.[66] But, while an assessor may determine that a certain issue is not a "material deficiency," the FTC may not agree. To avoid confusion and a company's unwarranted reliance on an assessment, the FTC could preemptively foreclose this issue. The FTC could also clarify whether a company can be in compliance with an order but still subject to a Section 5 case alleging violations of overlapping subject matter.

### G. Fully Evaluate Privacy Order Provisions, including Assessments

The agency may benefit from a full cross-divisional review of its privacy order provisions, especially including the assessment provision.[67] Such self-reflection and critical analysis at the FTC is not unprecedented. On the competition side, the Commission was recently lauded, domestically and internationally, for its two-year evaluation of its merger remedies, identifying areas of both strengths and weaknesses.[68] However, the agency's Office of Inspector General reviewed the Bureau of Consumer

---

[66] *United States v. Am. Hosp. Supply Corp.*, 1987 WL 12205 (N.D. Ill. 1987) (defendant's notice to the FTC that it had acquired companies making prohibited products was not "exculpatory" but was considered "in mitigation" of the penalty). *But see* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.* (FTC should not fault a company's data security if a third-party assessor approved it), https://www.ftc.gov/public-statements/2015/12/dissenting-statement-commissioner-maureen-k-ohlhausen-matter-ftc-v.

[67] Former Republican FTC Commissioner William Kovacic recently advocated a review of the agency's privacy compliance monitoring. "What kind of oversight did [the FTC] exercise? You have to look at that because that was a big part of your compliance mechanism. If that failed, then you have to rethink what you are doing." An FTC spokesman responded, "[T]he commission believes the privacy audits that undergird FTC consent decrees work." https://www.nationaljournal.com/s/665918/can-ftc-handle-facebooks-digital-privacy-challenge. *See also* privacy advocates' February 2017 letter to FTC commissioners, https://consumerfed.org/wp-content/uploads/2017/02/2-15-17-FTC_Letter.pdf.

[68] The 2017 Merger Remedies Taskforce reviewed Commission merger orders from 2006 through 2012, evaluating 89 merger orders affecting 400 markets, with 79 divestitures to 121 buyers. The Taskforce evaluated 50 of those orders using a case study method, interviewing and collecting data from nearly 200 businesses in a wide range of industries. The Taskforce Report included a list of improvements, and implemented them, specifically by updating the agency's Statement for Negotiating Merger Remedies. https://www.ftc.gov/news-events/blogs/competition-matters/2017/02/looking-back-again-ftc-merger-remedies.

Protection's resource allocation and achievement of mission objectives in 2015 and did not identify any issues associated with its oversight of the privacy orders.[69]

## VII. Conclusion

The FTC is critically important to ensuring privacy protections for the public. To fulfill this mission, however, the agency should re-evaluate its orders' assessment provision, and ensure it is a robust compliance mechanism. Failure to do so could have unintended consequences for all consumers.

[69] https://www.ftc.gov/system/files/documents/reports/evaluation-ftc-bureau-consumer-protection-resources/2015evaluationftcbcpreport.pdf. *See also* FTC's Office of Policy Planning, "Post-Purchase Consumer Remedies: briefing book for policy review session," (1980), https://catalog.hathitrust.org/Record/000100549.