Legal Opinion Letter

Vol. 27 No. 1 February 16, 2018

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

The FTC's Black-Box Determination of Information's Sensitivity Imperils First Amendment and Due-Process Rights

by Gerard M. Stegmaier, Wendell J. Bartnick, and Kelley L. Chittenden

"Sensitive information" is hard to accurately define, but the Federal Trade Commission (FTC or the Commission) seemingly knows it when it sees it. The lack of definition is troubling. Businesses and the FTC have skirmished over what "reasonable" security is for years, and reasonableness frequently hinges on sensitivity. The FTC has not defined "sensitive information," and given its vast power as a consumer-protection enforcement agency, continued guessing games exacerbate regulatory uncertainty and embolden prospective plaintiffs in class-action litigation.

On January 9, 2018, the FTC declared that posting intimate images of people with names and contact information violates the FTC Act.[1] While recognizing such images as "sensitive" may be easy (and nonconsensual, public distribution could certainly be "unfair") recognizing how the FTC makes such determinations outside of obvious cases is more difficult.[2] The consequences of this black-box oversight are increasingly dangerous to businesses and to constitutionally-protected First Amendment activities.

The FTC requires businesses to implement reasonable security measures. Reasonableness likely depends on the type and nature of the information itself and the relationship of the parties to one another and to the information—all touching on the sensitivity. The FTC, however, has little public precedent addressing these considerations either independently or collectively. For example, the FTC has not addressed whether information already in the public domain should be considered "sensitive" and why, and guidance would create certainty.

For at least fifteen years, the FTC has sought to regulate the collection and handling of sensitive consumer information, which it typically describes as information about children, health, and personal finances.[3] Since 2012, the FTC has newly claimed that geolocation[4] and device-specific television viewing information[5] is "sensitive." The Commission's growing, enumerated list provides little guidance on how the agency determines sensitivity. Accordingly, each new incremental prosecution, without the benefit of industry and consumer input, yields a small piece of a puzzle while lacking an explanation tied to the use, content, context, and/or actual or potential resulting injury. This presents serious constitutional and pragmatic policy concerns.

---

[1] *See* Fed. Trade Comm'n Press Release, *The FTC and Nevada Seek to Halt Revenge Porn Site* (Jan. 9, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/ftc-nevada-seek-halt-revenge-porn-site.

[2] *See generally Comments of Washington Legal Foundation to the Federal Trade Commission Concerning Informational Injury Workshop* (Oct. 27, 2017), http://www.wlf.org/upload/litigation/misc/10-27-2017FTCInfoInjury_Comments.pdf.

[3] *See, e.g.*, Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond* (Oct. 4, 2001), https://www.ftc.gov/public-statements/2001/10/protecting-consumers-privacy-2002-and-beyond. Information has been deemed worthy of protection in a patchwork fashion. *See* Paul Ohm, *Sensitive Information*, 88 S. Cal. L. Rev. 1125, 19-27 (2015).

[4] Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change 47, n. 214 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[5] *See In re Vizio, Inc.*, FTC Docket No. 1623024, Complaint 8 (Feb. 6, 2017).

Gerard M. Stegmaier is a Partner in the Washington, DC office of Reed Smith LLP, **Wendell J. Bartnick** is an Associate in the firm's Houston, TX office, and **Kelley L. Chittenden** is an Associate in the firm's Washington, DC office.

The current "we know it when we see it" approach puts businesses in a difficult position to identify and determine data-security obligations, especially if the information is already public. Before the *Vizio* prosecution, for instance, it is unlikely businesses would have considered device-specific television viewing data "sensitive" or that the FTC held such a view. The decision begs the question of when and what other "viewing" or "browsing" data is "sensitive." The FTC's failure to provide a transparent and predictable framework exposes it to First Amendment claims that it is advancing a speculative governmental interest or its actions impact more speech than is necessary to advance the government's goals.

One option the FTC should consider is formally designating a list of data types that rise to the level of "sensitive." Admittedly, technology and data usage rapidly change, and the FTC is working to keep up. However, the ambiguity and lack of clear enforcement doctrine subjects businesses to "stop and frisk black-box justice."[6] The FTC's current approach also suffers from a lack of nuance. For example, the average person would likely only consider geolocation information "sensitive" if it has certain characteristics (*e.g.*, public, highly precise geographically, and either real-time or a large volume of historical data). These characteristics relate directly to whether exposure of such information can cause harm.

Sensitivity determinations could be based, in-part, on the propensity to cause harm. For example, privacy torts typically remedy actions that are "highly offensive to a reasonable person."[7] Information that is not currently on the FTC's list could be "sensitive" when public availability could cause harm. Home addresses are not typically considered "sensitive," for example, but they could be for participants in a witness protection program or for abuse victims. The FTC reiterated at its Informational Injury Workshop that sensitivity correlates to the potential injury to individuals from unauthorized use and disclosure, but a workable fault analysis requires consideration of actual causation. One scholar proposes using a "threat model" to classify sensitive personal information based in part on the probability of significant harm,[8] and the U.S. government already uses an injury-based model to classify national security information.[9]

Context, independent of data elements, can also factor into the sensitivity of the information and reasonable consequences of dissemination or disclosure. An individual may consider information more "sensitive" when it is in the hands of a trusted recipient. Information that some may consider "sensitive" may not be if it is already public. For example, if an individual voluntarily posts his or her medical diagnosis online, that information should not be "sensitive." Sensitivity might also be based on accuracy, relevance, or how current the information is—an invalid credit card number and PIN combination is not "sensitive."

Ultimately, the subtleties of considering propensity to cause harm and other contextual factors show a simple list of "sensitive" data types can be both over-inclusive and under-inclusive. Therefore, a clear analytical framework illustrating how to make such determinations can lead to better outcomes for individuals and help businesses make decisions.

As it stands, businesses are in the dark when predicting how the FTC will view the sensitivity of information and the FTC's data security expectations. Predictability can come from preset lists of sensitive information that cannot be changed without reasonable notice or from publicly describing a framework through public guidance and enforcement efforts. These and other options can help businesses implement appropriate data security measures to protect consumer information.

---

[6] *See* Testimony, Prepared Statement of Gerard M. Stegmaier, *The Federal Trade Commission and its Section 5 Authority: Prosecutor, Judge and Jury* (Jul. 24, 2014), https://oversight.house.gov/wp-content/uploads/2014/07/Stegmaier-Statement-7-24-FTC.pdf.

[7] Restatement (Second) of Torts § 652D.

[8] Paul Ohm, *supra* note 3, at 1172.

[9] *See* Executive Order 13526, Part 1, § 1.2(a)(1)-(3), 1.4.

 ISBN 1056 3059