Who Is The More Active Privacy Enforcer: FTC or OCR?

Robert Gellman
Privacy and Information Policy Consultant
www.bobgellman.com
bob@bobgellman.com

Originally Posted on the Concurring Opinions Blog, August 23, 2013

Those who follow FTC privacy activities are already aware of the hype that surrounds the FTC's enforcement actions. For years, American businesses and the Department of Commerce have loudly touted the FTC as a privacy enforcer equivalent to EU Data Protection Authorities. The Commission is routinely cited as providing the enforcement mechanism for commercial privacy self-regulatory activities, for the EU-US Safe Harbor Framework (http://export.gov/safeharbor), and for the Department of Commerce sponsored Multistakeholder process (http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency). American business and the Commerce Department have exhausted themselves in international privacy forums promoting the virtues of FTC privacy enforcement.

I want to put FTC privacy activities into a perspective by comparing the FTC with the Office of Civil Rights (OCR), Department of Health and Human Services. OCR enforces health privacy and security standards based on the Health Insurance Portability and Accountability Act (HIPAA).

Let's begin with the FTC's statistics. The Commission maintains a webpage with information on all of its cases since 1997. The FTC's website is http://business.ftc.gov/legal-resources/8/35. I've found that the link provided does not work consistently or properly at times. I can't reach some pages to confirm everything I would like to, but I am sure enough of the basics to be able to make these comments.

The Commission reports 153 cases from 1997 through February 2013. That's roughly 15 years, with an average of about ten cases a year. The number of cases for 2012, the last full year, was 24, much higher than the fifteen-year average. The Commission clearly stepped up its privacy and security enforcement activities of late. I haven't reviewed the quality or significance of the cases brought, just the number.

There are some known problems with the FTC as privacy enforcer. The Commission only has jurisdiction over some of the economy. It has little or no privacy jurisdiction over federal, state, and local government agencies; the non-profit sector; and companies engaged in transportation, insurance, banking, and telecommunications. The Commission also has no practical general privacy or security rulemaking authority. We are all waiting for a decision in the Wyndham case to tell us more about just how far the Commission can go with its unfair or deceptive trade practices jurisdiction.

The Commission has specific privacy responsibilities under various statutes, including the Fair Credit Reporting Act and COPPA. The Commission has done no more than a mediocre job with

the FCRA, as the same problems at the major credit bureaus have persisted for decades with limited response from the FTC. The Commission seems to have done better with COPPA in the last few years, however, but it is hard to tell.

Let's turn to OCR. My data source is a White Paper titled *HIPAA/HITECH Act Enforcement: 2003-2013 The Role of Patient Complaints In Medical Privacy and Data Security*. http://www.melamedia.com/White_Papers.html. This just-published paper is by Dennis Melamed, publisher of the Health Information Privacy/Security Alert newsletter (http://www.melamedia.com/).

OCR enforces the HIPAA privacy and security rules. HIPAA covered entities had to comply with the privacy rule, the earliest of the HIPAA rules, in 2003 and with the security rule in 2005. Amendments to HIPAA from the HITECH Act added security breach notification, and that change took effect in 2009. Compliance with the most recent set of rule changes is required in September 2013. In other words, not all of the HIPAA rules enforced by OCR were in place during the entire ten-year period.

For a variety of reasons, it may be unfair to compare enforcement actions by the FTC and OCR. Everyone here knows how to play lawyer and tease out distinctions based on differing authority, budget, staffing, and other factors. OCR has actual rules, but the FTC does not, except under a few specific statutes. I know that Dan Solove and Woody Hartzog have a paper touting the FTC's importance in establishing privacy standards through its cases. I'm ignoring that type of analysis. For the moment, I just want to compare numbers.

According to the Melamed White Paper, OCR investigated 19,726 complaints that revealed a violation during the ten-year period ending in April 2013. That's an average of almost 2000 complaints a year. There were more investigations that did not find a violation.

The FTC, which has jurisdiction over a much larger portion of the US economy than the OCR does, managed only ten complaints a year over a fifteen-year period. A moving average would bump the Commission's numbers up somewhat, but the numbers are still in the low twenties at best.

On the numbers, OCR's efforts exceed the FTC's efforts by two orders of magnitude. 2000 versus 20 some. I don't need to factor in the differences in the size and number of the industries subject to FTC and OCR jurisdictions to underscore the same point. The FTC looks wimpy enough based on raw numbers. If we consider the denominator, the millions of companies, lines of business, and webpages that fall under the Commission's unfair or deceptive trade practices jurisdiction, the Commission only looks worse.

I'm not arguing that OCR is perfect. OCR was criticized for a long time in not seeking penalties against HIPAA covered entities that violated the rules. In the first years of HIPAA, OCR was more interested in seeking compliance than penalties, a not-unreasonable approach for a new law. Lately, however, OCR has imposed significant financial penalties measured in the millions of dollars. I think some of that is excessive, but that's a different set of issues.

It seems to me that it is difficult to look at the numbers and still think that the FTC's record justifies grand claims about the role of the FTC as a general enforcer of privacy standards in the commercial sector. At best, the FTC dabbles in privacy. OCR shows that a government agency can do better. Much better.

Not convinced? Consider two additional points. The business community has been one of the biggest cheerleaders for the Commission's privacy enforcement activities. Why is it that those whose privacy activities are regulated by the Commission are its biggest promoters? Hospitals are not fans of OCR. Banks regulated by the Consumer Finance Protection Board hate the agency and have been lobbying to undermine its legislation or to kill the Board altogether. Why does the regulated community love the FTC but not OCR or CFPB? I leave this question as an exercise for the reader.

Second, just recently, the telecommunications industry started a campaign to transfer telecom privacy jurisdiction away from the Federal Communications Commission and give that jurisdiction to the FTC. That's one of the goals of the 21st Century Privacy Coalition (no website yet as far as I can tell). One of the leaders of the coalition is former Federal Trade Commission Chairman Jon Leibowitz.

It is interesting to observe that the FCC has actual rule making authority, but the FTC's privacy rulemaking powers are so attenuated as to be non-existent. I'm not prepared to evaluate the FCC's performance on privacy, but I wonder if anyone believes that a regulated industry would hire Leibowitz and other high-priced talent in order to move from a weaker privacy regulatory regime to a stronger one. You can buy the Coalition's argument that it wants uniformity, but even if that argument passes the laugh test, the Coalition wants uniformity at the lowest possible end of the scale.

I don't mean to suggest that the FTC is worthless or poorly motivated. The Commission just doesn't do much in the way of privacy enforcement, and I don't see any likelihood of improvement. Numbers matter. I've said in the past that unless your privacy violation or security breach ends up on the front page of a newspaper, the chance that the FTC will come after your company are about the same as the chance of being hit by a meteorite. That may be a rhetorical exaggeration, but it's not much of one.