Federal Trade Commission

Built to Last: Section 5 and the Changing Marketplace

Jessica Rich[1]
Director, Bureau of Consumer Protection, FTC

Section 5 Symposium
Washington, D.C.
February 26, 2015

Thank you. I'm delighted to be here.

It seems fitting to start a discussion of Section 5 with the famous quote: "The only thing that is constant is change." That's a central principle behind the approach Congress took in enacting Section 5. On its face, the critical language in the FTC Act seems pretty simple – unfair or deceptive practices are unlawful. But as everyone here knows, Section 5 has been used to address many different types of law violations by many different types of companies, and is the source of a full and ever-growing body of case law.

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner.

Section 5 is the primary enforcement tool that the Commission relies on to prevent fraud, deception, and unfair business practices in the marketplace. It is a workhorse for protecting consumers, deliberately designed by Congress to enable the FTC to address a wide range of practices in an ever-changing economy.[2] Congress recognized that enumerating a list of deceptive and unfair practices was an impossible task, and instead drafted language that would give the Commission the flexibility it needed to respond to changing times.[3]

This flexibility has proven to be critical to the agency's consumer protection mission. Using its deception authority, the FTC has challenged a range of practices involving, for example, false health and weight loss claims; phony business opportunities; misleading price claims; bait and switch tactics; pyramid schemes; and the failure to perform promised services or meet warranty obligations. Using our unfairness authority, we have challenged such practices as unauthorized billing; the sale of consumers' private phone records; unilateral breaches of contract; the dismantling of home appliances by repair contractors; and the failure to warn about serious safety issues.

Since Barry and Carl asked me to discuss privacy in particular, I'm going to focus my remarks primarily on how the FTC has used Section 5 in that context.

---

2 *See FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) ("Congress . . . explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply.").

3 *See* S. Rep. No. 63-597, at 13 (1914) ("there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others"); H.R. Rep. No. 63-1142, at 19 (1914) (Conf. Rep.) ("It is impossible to frame definitions which embrace all unfair practices.").

When Section 5 was enacted, I think it's fair to say that no one could have imagined the digital explosion of today. Today, data is collected from consumers at every turn, all day long – on the internet, through their mobile phones, in stores and malls, and through devices in their cars and as they exercise. Many of the companies that obtain consumer data are behind the scenes and never interact with consumers. These companies include hundreds of data brokers that collect and combine data from multiple sources and develop detailed profiles for sale to other companies.

Adding to this, technological developments have enabled the vast storage and real-time processing of data once thought to be cost-prohibitive. As a result, data is now stored for long periods of time and used and re-used for many different, often unanticipated purposes. The companies that obtain and use all of this data may not store it securely, as shown by all of the breaches we are seeing in the marketplace. And identity theft tops the list of consumer complaints received by the FTC and other law enforcement agencies every year, affecting many millions of consumers.

On top of all of this, consumers don't have effective ways to learn about these practices and make informed choices about them. Privacy policies – once thought to be a tool for giving consumers the information needed to make these choices – are long and legalistic, impossible for the average consumer to read and understand. Consumers are not going to stop what they are doing to decipher them, especially when many of the companies that collect and use their data are third parties they don't even know about.

These issues drive much of what we do. Protecting consumer privacy is one of the Commission's top priorities and has been for decades. Although the agency's activities have varied during that time, our central goal has remained constant: to protect consumers' privacy in a way that fosters trust in the marketplace, and preserves and complements innovation.

Section 5 has been a critical tool in this effort, and we have used it to address privacy by applying the same elements of proof we have always applied. If a company makes materially misleading statements or omissions about privacy or data security that are likely to mislead reasonable consumers, such statements or omissions are deceptive. The FTC has used this authority, for example, to challenge false and misleading claims about how companies use and share consumer data; whether they track consumers' movements online; whether they are honoring consumers' opt-outs; and whether they are delivering on promises to secure consumers' financial and health data.

If a company's privacy or data security practices cause or are likely to cause substantial consumer injury that is not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers or competition, those practices are unfair. Congress expressly codified these criteria in Section 5. We have alleged a variety of harms arising from unfair privacy and data security practices, including financial harm to consumers whose data was exposed due to unreasonable data security; the knowing sale of financial account data to scam artists; and the use of software to

surreptitiously capture consumers' sensitive data, location, and even photos of them in their homes.

Both theories are essential to our ability to protect consumers, and they are complementary. Our deception authority enables us to target false and misleading information that disables consumer choice, and interferes with competition. But many companies don't make claims and promises, or may operate behind the scenes. And consumers often are not in a position to learn, for example, whether a company is selling their data to fraudsters or treating their sensitive data carelessly. Unfairness allows us to address these types of harms. However, as those who know the law and our cases are well aware, unfairness requires that we analyze and prove three essential elements, including the presence of real, non-speculative risk of harm. We use this authority only when we can prove these elements.

I'd like to take the rest of my time to describe a few examples of how we have used Section 5 to address harms that would not have been contemplated when Section 5 was enacted. First is data security. Since 2001, the Commission has settled 53 cases against companies we charged with failing to provide reasonable and appropriate protections for consumers' personal information. We are currently litigating two others. These cases all involved basic security failures – failures to led to specific consumer harms or put the data, and consumers, at serious risk of harm, and failures that could have been avoided if the company had used available, cost-effective security measures. Some cases alleged deception, some alleged unfairness, and some alleged both theories.

From the outset, the FTC has recognized that there is no such thing as perfect security, and that security is a continuing process of detecting risks and adjusting one's security program and defenses. For that reason, the touchstone of our approach to data security has been *reasonableness* – a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the available tools to improve security and reduce vulnerabilities. We examine such factors as whether the risks at issue were well known or reasonably foreseeable, and the costs and benefits of implementing available tools and protections. And the fact that a breach has occurred does not mean that a company has violated the law, though it can be relevant to any reasonableness analysis.

We also focus on whether a company has undertaken a reasonable *process* to secure data. Is someone in charge and accountable? Has the company assessed risks and developed safeguards to address those risks? Is the company training its employees, overseeing service providers, and implementing appropriate limits on access to data?

I want to emphasize that, amidst many debates about privacy, data security has been an area that has generally enjoyed unanimous, bipartisan support at the Commission. If you're storing sensitive data, don't leave the door wide open for hackers or other risks of exposure. The values here are generally aligned with, not just consumer interests, but business and market interests.

Two recent examples are the FTC's cases against home security company TRENDnet and Wyndham Hotels. TRENDnet involved video cameras designed to

allow consumers to monitor their homes remotely.[4] The FTC's complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although the company claimed that the cameras were "secure," they had faulty software that left them open to online viewing, and in some instances listening. This resulted in hackers posting 700 consumers' live video feeds on the Internet.

In the *Wyndham* matter, an ongoing litigation, the FTC filed a lawsuit in federal court alleging that the company failed to protect consumers' sensitive financial data.[5] According to the FTC's complaint, Wyndham and its subsidiaries repeatedly failed to take basic security measures, such as using complex user IDs and passwords and deploying firewalls. They also stored sensitive payment card data in clear readable text. These systemic failures exposed consumers' data to multiple instances of unauthorized access. Indeed, the company allegedly suffered three data breaches in less than two years, resulting in fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of accounts to an Internet domain address registered in Russia. We alleged both deception and unfairness in this case.

Two recent examples on the privacy side include our cases against website operator Craig Brittain and data broker LeapLab. Brittain operated an alleged "revenge porn" website, on which he posted intimate images and personal data of more than 1000

4 *TRENDnet, Inc.*, No. C-4426 (F.T.C. Jan. 16, 2014) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
5 *FTC v. Wyndham Worldwide Corp. et al.*, Civil No. 13-1887 (D.N.J. Apr. 7, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation.

individuals.[6] Our complaint alleged that he used deception to acquire the images, and also solicited the images from angry boyfriends and by offering money on his website. He then advertised content removal services that could delete the images from the site in exchange for a hefty payment, pretending that this service was operated by a third party. Our complaint alleged both deception and unfairness.

In *LeapLab*, we alleged that the data broker bought payday loan applications of financially strapped consumers and then sold that data to non-lenders that it knew had no legitimate need for it.[7] These third parties included data brokers that aggregated and then resold the consumer data, and phony internet merchants. At least one of those third parties, Ideal Financial Solutions – a defendant in another FTC case – allegedly used the information to withdraw millions of dollars from consumers' accounts without their authorization. This litigation is ongoing.

These are just a few examples of how the Commission has used Section 5 to address harmful privacy practices happening in the marketplace today, but not in the 1930s or even the 1980s. Because of the flexible authority conferred through the FTC Act – defined through principles and not lists of specific business practices – we are able to keep up with the changing times and different harms we see through the decades. I am happy to answer questions.

---

6 *Craig Brittain*, File No. 132-3120 (F.T.C. Jan. 29, 2015) (proposed consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3120/craig-brittain-matter.
7 *FTC v. Sitesearch Corp. d/b/a LeapLab* (D. Az. filed Dec. 23, 2014), *available at* http://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab.