A number of years ago, the Commission adopted separate statements on deception and unfairness to explain how we will interpret Section 5 in the consumer protection area. Those statements continue to guide the Commission today. Here's how they work:

The deception statement explains that deceptive practices are representations, whether explicit or implicit, about material facts that

When Detective Mode was activated, the software could log key strokes, capture screen shots, and take photographs using a computer's webcam. It also presented a fake software program registration screen that tricked consumers into providing their personal contact information and did not register software. Data gathered by DesignerWare and provided to rent-to-own stores using Detective Mode revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home, as well as geolocation data.

Our complaint against DesignerWare and the rent to own companies included both unfairness and deception counts. The deception count was straightforward and was based on sending consumers the fake registration forms to obtain their contact information. Clearly, this was an explicit representation about a material fact that was likely to mislead a consumer acting reasonably.

The Commission also charged that licensing and enabling Detective Mode, gathering sensitive personal information about renters, and disclosing that information to the rent-to-own businesses was unfair. Specifically, the complaint alleged that the collection and disclosure of private and confidential financial and medical information about consumers caused or is likely to cause substantial injury to consumers. I believe that this is consistent with the unfairness statement, which identifies financial and health harms as substantial.

The complaint also alleged that the defendants' intrusion into consumers' homes, the tracking of their locations over time, and the capture and disclosure of information, including images of partially undressed individuals and sexual activity, was also unfair. This intrusion into the home, the sharing of such images, and the tracking of precise consumer locations over time, in my opinion, caused substantial injury to consumers by creating an unwarranted safety risks that could arise from stalking or similar behavior triggered by such exposure and tracking.

As for the other requirements of unfairness, because Detective Mode functioned secretly, consumers could not reasonably avoid this harm, and any possible benefits of the practice did not seem to outweigh its harms, particularly because

prominent companies, as well as nineteen Children's Online Privacy Protections Act (COPPA)[5] actions.

Calls for New Legislation

In the FTC's Privacy Report, released shortly before I joined the Commission, some of my fellow Commissioners called for a new privacy law that would go beyond Section 5, but did not specify what such new legislation should look like.[6] The Report also did not identify what substantial harms are occurring now that Section 5 cannot reach, although it did appear to embrace an expansion of the concept of harm to include reputational or other intangible privacy interests, which the FTC's unfairness statement indicated would not make an injury unfair. In addition to the FTC Report, there have been other calls for a new, more general privacy law from other quarters.

In thinking about these calls for new legislation, I would like to share with you a personal analogy that I readily confess may have a bit of a gender bias to it. With the onset of such nice, crisp fall days, I start thinking about transitioning my closet to my cooler weather wardrobe. But before I hit the stores and buy new items, I've learned from experience to take an inventory of the clothes already in my closet to avoid buying things I already have.

I believe it is similarly important for policymakers to take an inventory of what is already in stock in the FTC closet before seeking new privacy laws. I'm not necessarily against legislation and there are a number of existing laws in addition to Section 5, such as COPPA, the Fair Credit Reporting Act, GLB, and others, that are an important part of the agency's enforcement arsenal.[7] There are also other privacy laws, such as HIPPA, as well as the CPNI and cable privacy rules, that provide important protections for consumers.[8]

Before seeking new privacy legislation, it is important to identify a gap in statutory authority or to identify a case of substantial consumer harm that we'd like to address, but can't, with our existing authority, especially given the array of financial, medical, and health and safety harms already reachable under our current FTC authority or other laws. Otherwise, it is difficult to tell whether the additional protections are necessary or will, on balance, make consumers better off because information sharing has benefits for consumers such as reducing online fraud, improving products and services, and increasing competition in the market overall.

---

[5] The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2006).
[6] FED. TRADE COM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUS. AND POLICYMAKERS (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[7] The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (2006); The Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (2006); The Gramm–Leach–Bliley Act, 15 U.S.C. §§ 6801-6809 (2006).
[8] The Health Insurance Portability and Accountability Act (HIPPA), Pub. L. N467 TD-.y4.3(0)( )6(( )]TJ-2PLl cons4J-2PL-1025(TJ-2P

public interest that those decisions, in the aggregate, be intelligent and well informed. To this end, the free flow of commercial information is indispensible."[10]

A policy that limits the ability of advertisers to access and use information (whether collected directly from consumers, or indirectly through affiliates, different brands within the company, or from third parties) to reach target audiences may have unintended effects on consumers and the marketplace that any policymaker, particularly one with responsibility for consumer protection and competition, must consider.

To raise the question of the effect on competition does not mean that I would never support any new privacy law, it simply means that I believe we must at least ask the question if we want to ensure the best outcome for consumers.

A Uniform Standard for Data Security

Turning back to my earlier shopping analogy, there is one new accessory that I would support adding to the FTC's fall wardrobe: a uniform federal law for data security and breach notification. Although the FTC can proceed using its Section 5 authority—and since 2001 it has brought over thirty cases against companies for failing to protect consumer information—there are gaps that could be closed through carefully crafted federal legislation. Currently, almost all states have data security laws on the books that require consumer notification if personal information has been compromised. Although some of the laws are similar, they are not identical. This means that companies need to comply with separate state notice requirements and consumers may get notifications that are different and are triggered by different types of breaches.

A single standard would let companies know what to do and consumers know what to expect. I believe that, if carefully crafted, such a law is likely to benefit both consumers and business, particularly because, unlike uses of consumer information for advertising, product improvement, or fraud reduction, there are no benefits to consumers or competition from allowing consumer data to be stolen. Any such law would have to consider carefully, however, what are reasonable precautions for safeguarding various types of data to avoid imposing undue costs that are not justified by consumer benefits.

Business and Consumer Education

Law enforcement is critically important, but in some respects the Commission's consumer and business education mission impacts a greater percentage of American consumers that anything else we do. For example, the information available on our webpage to help consumers avoid becoming victims of identity theft has had millions of hits, and the paper edition has been distributed through many channels to millions more. And if prevention doesn't work, we offer excellent resources on steps to take to mitigate the damage of having your

[10] *Va. Pharm. Bd. v. Va. Consumer Council*, 425 U.S. 748, 765 (1976).

have also reached out to industry to work on improving the disclosures. The Unit is now following up with a survey to find out how frequently apps aimed at kids actually collect data. In addition, it has brought six law enforcement cases.

Conclusion

I've covered a lot of territory with you today. Let me briefly restate the three points with which I hope to leave you. First, I am not convinced that the FTC is currently lacking any statutory authority in the general privacy area; for now, Section 5 is sufficient to protect consumers. Second, the Commission must analyze issues under its purview from a perspective that covers both consumer protection and competition scrutiny, or it will not reach the best result for consumers. Finally, the Commission should use all of the tools in its arsenal: law enforcement, regulatory and business and consumer education to reach the maximum target audience. As the newest Commissioner, but the one with the most experience at the agency, I pledge to ensure that we do all in our power to further the interests of American consumers.