The FTC's Privacy Leadership Role in the United States
Keynote Address Before Privacy Laws & Business Conference on
Privacy in a Connected World
Commissioner Julie Brill
July 6, 2015

Good afternoon. Thank you, Stewart, for your introduction. And thank you so much for inviting me to address you today. The problem of how to protect privacy in the digital economy is immediate and of global import. And what better place to grapple with the issue than here at St. John's college, one of the most storied and revered institutions of higher learning in the world? I say *one of* – and not *the* – just in case there are Oxonians – or Trinity College alumni – in the audience. As Voltaire said on his deathbed, when asked to renounce the Devil, "This is no time to be making new enemies."

So in preparing my remarks for today, I planned to focus, in a rigorous and academic manner befitting our setting, on the historical underpinnings of the United States Federal Trade Commission's (FTC), approach to data protection and data security. I wanted to explain how – in this brave new world of Big Data, the Internet of Things, social media, mobile marketplaces, and virtual reality – the FTC acts to protect consumer privacy in a manner that adapts to changing technology yet adheres to bedrock principles of consumer protection – principles our agency has held at its core since its founding, one hundred years ago.

One hundred years ago. That sounded pretty impressive, until it was pointed out to me that construction on the Great Gate through which I entered this morning was finished in 1516. Section 5 of the FTC Act, which gives my agency the legal authority to go after companies that deceive consumers or treat them unfairly[1] – an authority we continue to use today to protect consumers' data online – was added in 1938. I am pretty sure the mattress in my hotel room is older than that.

For those of you celebrating the Magna Carta's 800th anniversary, "history" may seem a grand word to use for my discussion of how the FTC has become the leading consumer protection agency in the United States, and how our long record of consumer protection enforcement, policy development, and education have influenced our work on privacy and data security. But as Winston Churchill said, "Study history, study history. In history lies all the secrets of statecraft." Who am I to defy the British Bulldog on his home turf? Besides, even though when measured in Magna Carta years, the FTC's history is beyond brief, I believe a quick review will give you a better understanding of how the FTC protects privacy and where I would like to see the agency's efforts go in the future.

The Consumer Protection Foundations of FTC Privacy Enforcement

The FTC derives its authority to protect consumers from an amendment to the FTC Act, so-called "Section 5," enacted a couple of years before Churchill first became prime minister. Section 5 gives the FTC broad authority to provide remedies for consumers harmed by deceptive

[1] 15 U.S.C. § 45(a).

or unfair practices in the market place. It is a flexible statute that grants the FTC consumer protection authority that changes as technologies and business practices change – an authority that dates from the days of newspaper and radio advertising but serves equally well in the era of connected devices, mobile payments and facial recognition.

To protect consumers from deception, the FTC had long held that it would presume a company's express representations to consumers, as well as certain implied representations, about a good or service are material to consumers' decisions about whether to use it. We have brought hundreds of cases against companies for making deceptive claims in advertising. We have shut down scams that falsely promise to deliver credit repair, mortgage relief, business opportunities, and other services that predominantly target vulnerable consumers. And we have been a leader in stopping robocalls and abusive telemarketing practices.

As consumers spend more and more time in the online marketplace, the FTC has moved its efforts to protect consumers there as well,[2] a migration apparent from a brief look at our work on online companies' privacy policies. Consumers want to know what information they are

not be household names. The settlements in these cases – more than 40 of them dealing with privacy, and nearly 60 dealing with data security – have brought greater protections for

provides the basis for the FTC's Safe Harbor enforcement and so plays a pivotal role in sustaining a program that is central to data flows between Europe and the United States.

The second case involves Internet-connected video cameras. Though widely regarded as being about data security, this

These cases demonstrate clearly how data brokers' violations of consumer privacy can create real harm, and how appropriate it is for the FTC to pursue the violators with our consumer protection jurisdiction. And we have not stopped with enforcement activities. A year ago, the FTC took a deep look at this industry and published its findings and recommendations.[25] We found that data brokers put consumers into "segments" that track sensitive characteristics, including race, religion, ethnicity, sexual orientation, income, and health conditions. I see a clear potential for these profiles to harm low-income and other vulnerable consumers. I fully support the Commission's call for data broker legislation that would bring more transparency, accountability, and consumer control to the data broker ecosystem.

Developing Policies and Best Practices for a Data-Driven World

Our data broker report and recommendations are an example of how the FTC looks

found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[31] The FTC is recommending a "security by design" approach that incorporates security into the entire lifecycle of products and services,[32] and we are engaging developers big and small in this ongoing conversation.[33]

Privacy protections will also play an integr

security, legislation that supplements the FTC's current "reasonable security" standard with FTC rulemaking and civil penalty authority would put the FTC in a stronger position to hold accountable those companies that fail to take the necessary steps to protect the data that consumers have entrusted to them.

* * * * * *

To sum up, let me return for a moment to Winston Churchill. He said: "History will be kind to me for I intend to write it." While the FTC has been true to our history of protecting consumers and their privacy as our world has moved into the Internet age and beyond, we are also aware we are writing the history for future generations of consumers for whom "online" will become synonymous with "alive." We strive today to make sure the consumers of tomorrow are protected in the cyber-marketplace from unfair and deceptive practices – by encouraging