The FTC's privacy program seeks to address these concerns through law enforcement, policy initiatives, and education. Many of our efforts are guided by three basic principles that build on the long-established fair information practices. First is Privacy by Design – build meaningful privacy and data security protections into your business model from the very start. Don't add them afterwards as an afterthought. Second is Transparency – tell consumers how you will collect, use, and share their data. But don't just tell them in a privacy policy; provide them with important information at the moment of a transaction or in some other prominent place where can see and act on it. Third is Choice – give consumers choices about any collection, use, and sharing that isn't obvious or implied from the context, and provide opt-in choice whenever sensitive data is involved.

I. FTC Jurisdiction and Authority

Before I tell you about our specific initiatives, I'd like to provide a little background for those of you who aren't familiar with the Commission. The FTC has broad jurisdiction over most entities engaged in commerce – just not banks and few other exceptions. Our primary authority is the FTC Act, which prohibits unfair and deceptive trade practices.[2] The basic rules are that companies can't deceive consumer or engage in practices that cause substantial consumer injury without countervailing benefits to consumers or competition. The FTC Act is flexible by design, and we've used our authority to challenge a very wide range of practices. False claims and material omissions about how data will be used or shared. Failure to provide reasonable security protections for consumer data. Invisible spyware that infects consumers computers or

steals their information. Invasive and unwanted spam. Impersonating consumers in calls to financial institutions, in order to obtain their data. Posting consumers' sensitive data online and then seeking money from the consumers to take it down. Tricking consumers into consenting to certain data practices. Capturing people's private communications and photos through tracking software. Selling data that is then used for fraud. Etcetera.

The Commission also enforces a number of sector-specific privacy laws. These include the Fair Credit Reporting Act, which protects the privacy and accuracy of sensitive consumer report information;[3] the Gramm-Leach-Bliley Act, which imposes privacy and security requirements on non-bank financial institutions;[4] the Children's Online Privacy Protection Act;[5] the CAN-SPAM Act;[6] and the Telemarketing and Consumer Fraud and Abuse Prevention Act[7] with its Do Not Call Rule.[8]

In addition, the FTC educates consumers and businesses, conducts studies, testifies before Congress, hosts workshops, and writes reports regarding the privacy and security implications of technologies and business practices that affect consumers. We issue educational materials on a wide range of topics – from mobile device security to kids' online safety to preventing and repairing identity theft, our top source of consumer complaints from year-to-year. Our outreach efforts are designed to prevent law violations and harm before they happen, and are therefore integral to our mission.

We are not the only US agency working on privacy and data security issues. A variety of other federal agencies, such as the Federal Communications Commission and the Consumer Financial Protection Bureau, have privacy authority in specific sectors. And many of the US States also have robust privacy laws and active enforcement

with using a deceptive registration process to trick thousands of consumers who signed up for its online billing portal into also consenting to the collection of their detailed medical information from pharmacies, medical labs, and insurance companies.[12]

Then there are extortion websites that harvest sensitive data, post it online, and seek payment to take it down. We took action against two of those this year. In one, defendant Craig Brittain solicited sexually explicit photos from women's ex-boyfriends and others – in many cases through deception – to post on his website, isanybodydown.com.[13] He then used another site to pose as an attorney and charge $250 for removing the information. We brought a similar actions against a company called Jerk.com, which posted photos of kids and teens,

Other recent data security cases include actions against service provider Accretive Health,[20] supplement companies Genelink[21] and Genewize,[22] medical transcriber GMR Transcription Services,[23] and debt brokers Bayview[24] and Cornerstone.[25] These cases all involved the failure to secure sensitive information – in some cases health data, in some cases financial data. And we have ongoing litigation against Wyndham Hotels[26] and LabMD[27] – and a contempt action against Lifelock[28] – for alleged failures to protect sensitive financial and health data. In *Wyndham*, the Third Circuit recently reaffirmed the FTC's authority under the FTC Act to hold companies accountable for security failures.

against4.72 Tm (28)Tj EMC /P <</MCIDu4-0 0 8.52 110.4 684.3[D 6 >>BDC 0.0-Tw 12.

that data brokers InfoTrack[34] and Instant Checkmate[35] sold detailed background checks to employers and landlords without ensuring that the data was accurate, or that purchasers

In addition, last fall, we hosted a workshop entitled *Big Data: A Tool for Inclusion or Exclusion?*

[27] *LabMD Inc.*, Docket No. 9357 (filed Aug. 28, 2013), *available at* https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter.

[28] *FTC v. Lifelock Inc.*, No. 2:10-cv-00530-MHM (D. Az. filed July 21, 2015), *available at* https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.

[29] *See* FTC Press Release, *FTC Kicks Off "Start with Security" Business Education Initiative*, June 30, 2015, *available at* https://www.ftc.gov/news-events/press-releases/2015/06/ftc-kicks-start-security-business-education-initiative.

[30] *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-5/06/de

[42] FTC Staff Workshop Report, *The Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things.

[43] FTC Workshop, *Follow the Lead: An FTC Workshop on Lead Generation* (Oct. 30, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/10/follow-lead-ftc-workshop-lead-generation.

[44] FTC Workshop, *Cross Device Tracking* (Nov. 16, 2015), *available at* https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking.

[45] *See* FTC Press Release, *FTC Announces PrivacyCon, Issues Call to Whitehat Researchers and Academics for Presentations* (Aug. 28, 2015), *available at* https://www.ftc.gov/news-events/press-releases/2015/08/ftc-announces-privacycon-issues-call-whitehat-researchers.