But these changes also pose immense challenges for consumer protection. Today, commerce comes at us from every direction, at every minute – through the smartphones we carry with us everywhere and the many connected devices all around us. Data predictions determine the information we receive and the offers we get. And, increasingly, consumers become the marketers, as they're enlisted in campaigns on social media to tout products and services to their friends and acquaintances.

Adding to these challenges, many of the technologies that drive these advances now have small screens or no screens at all. And many of the companies that receive and use our personal information are behind the scenes, completely invisible to us. As a result, it's harder to rely on some of the traditional tools we've all used to protect consumers, such as disclosures to avoid deception and privacy policies to describe data practices. And it's extremely hard for consumers to protect themselves.

opiates, including prescription pain medications and illegal drugs such as heroin.[5] This case is pending in federal district court.

And we're seeing more and more mobile apps marketed essentially as medical devices. Last year, we charged two app developers with deceptively claiming that their apps – Mole Detective and MelApp – could detect symptoms of melanoma, even in the early stages.[6] In fact, we alleged, the companies lacked evidence to show they could detect melanoma, early or at all.

One particularly troubling trend we're seeing involves deceptive health claims targeted at particular age groups. Many of these claims tout products offering cognitive benefits or other age-related treatments for older adults or young children – a clear effort to tap ff tt10(ar)-1610(a f)-1MC

We also took action against Ultimeyes – another health app styled as a medical device – which claimed to have scientific proof that it could "turn back the clock" on consumers' vision through a series of visual exercises.[8] In fact, we charged it had no such proof.

advertising scenarios that are likely to deceive consumers, and provide guidance on ways to avoid the guidA[(P)-8C -0.004 Tc004 Tc00oo2

providing them, at their own peril.'ll Ihave more to say about online tracking when I talk to the National Advertising Initiative next week.

Over the last two decades, the FTC has brought hundreds of privacy cases addressing a range of deceptive and unfair practices involving consumers' data – deceptive claims about how data is collected, used, and shared; failure to protect sensitive data from unauthorized access; invasive spam and spyware; the sale of sensitive data to scam artists; and the failure of seal programs to provide the promised protections. The companies we've sued have run the gamut,

volume of the consumer data they hold, the size and complexity of their operations, and the cost of available tools to secure the data.[17]

We've brought almost 60 data security cases to date, and many of the companies we've

Also, we took action against TRENDnet, an Internet of Things company that sold IP cameras for home security and baby monitoring.[23] We alleged that, due to the company's failure to properly secure the cameras, hackers were able to access and then post online the private video and even audio feed of hundreds of people's bedrooms and babies' rooms.

The FTC also issued a report on the Internet of Things last year. The report recommended a number of best practices for companies to follow, and addressed how fundamental privacy principles can be adapted for the Internet of Things. For example, one issue we addressed was the question we hear again and again about whether notice and choice have continuing relevance in the IoT, given the lack of traditional screens or interface to communicate with consumers. Our answer was "yes," and the report discussed the different tools that IoT companies are using to communicate with consumers – such as point of sale disclosures, set-up wizards, or even codes on the device. The report also discussed the importance of reasonable collection limits, de-identification of data, and strong security measures. You can find the report online.[24]

Big Data

Finally, let me turn to Big Data, by which I mean the vast collection of detailed data about consumers to make predictions about populations or groups of consumers. Big Data can of course drive valuable innovations across society, but increased collection and storage of data also increases the risks of data breach, identity theft, and the likelihood that sensitive data will be used for purposes consumers don't anticipate or want – for example, by employers, insurers, and creditors to make decisions about consumers' eligibility for important benefits.

We recently issued a report entitled Big Data: A Tool for Inclusion or Exclusion?[25] which followed up on a workshop we held.

scam artists who used the data to withdraw millions of dollars from consumers' accounts.[28] Similarly, we've brought a number of cases against fraudulent debt collectors that were able to purchase detailed information about consumers' debts, including account numbers and SSNs. These types of cases reveal a very troubling trend and help to answer the question we so often hear in privacy – "where's the harm?" When you can simply purchase this kind of highly sensitive data about consumers' and use it to defraud them, there's harm.

III. Conclusion

In closing, I hope I've made my point that while the technological landscape is constantly changing, the basic principles of consumer protection are enduring and provide a solid and continuing framework for vigorous FTC enforcement. These principles aren't just about compliance, they're about your brand and consumer trust, so you have many reasons to care about them.

I also want to put in a plug for strong self-regulation, and for your cooperation with self regulatory programs like the NAD. Self-regulation – and by that I mean strong, visible, and enforceable self-regulation that provides effective consumer protections – is an important complement to law enforcement, and helps the FTC maintain a safe marketplace for consumers and a level playing field for businesses. Thanks for having me here today.

---

[28] FTC v. Sitesearch Corp., LLC, Matter No. 142-3192 (D. Az. filed Dec. 22, 2014), available at https://www.ftc.gov/enforcement/cases-proceedings/142-3192/sitesearch-corporation-doing-business-leaplab; FTC v. Sequoia One, LLC, No. 2:15-cv-01512-JCM-CWH (D. Nev. filed Aug. 12, 2015), available at https://www.ftc.gov/enforcement/cases-proceedings/132-3253/sequoia-one-llc.