The New York Times

The Internet of Things:
From Regulators, Guidance and Enforcement

Julie Brill is a commissioner of the Federal Trade Commission.

Updated September 8, 2013, 8:31 PM

We hear a lot about how "big data," fueled in part by the connection of an expanding array of devices to the Internet, will bring better and cheaper products and services to the market while expanding human knowledge. Connected cars will solve traffic congestion; smart grid devices will conserve money and the environment; and connected medical devices will enable early detection and smarter treatments and save lives.

The prospect of these benefits is exciting. But as society becomes more wired and connected, we must be mindful to preserve consumer privacy. To realize its potential, the coming web of connected devices must develop and grow within an ecosystem that garners consumer trust by safeguarding privacy. The Federal Trade Commission, which oversees consumer privacy, has urged companies to adopt privacy and data security best practices, like building privacy protections into the design of their products and services. Simplified privacy disclosures would tell consumers how information is being collected and used, and if any of that is surprising to consumers, companies should give them the ability to say "no" to the practice or to not engage in the transaction. Consumers should also have reasonable access to their data.

In addition to such guidance, the F.T.C. also brings enforcement actions against companies that collect and use data deceptively or unfairly, including by failing to provide reasonable data security, a crucial issue for connected devices. Last week, the commission announced its first data security action over a product that was part of the Internet of Things: Internet-connected video cameras. The commission believes the company failed to use reasonable security in the software that controlled the remote monitoring, allowing malicious hackers to put the private lives of hundreds of consumers on public display.

The critical question is not whether these principles and legal standards apply to smart devices – they plainly do – but how they should apply. How can a company provide effective notice about what data it collects about consumers and how that data is used, when its device has no user interface and consumers may not even know the device is connected? Will companies combine

the information they gain from consumers' devices with other online and offline information to create rich profiles about consumers' behavior? Should they be able to do so, and if so, under what circumstances? And what rights, if any, should consumers have to see and modify those enriched profiles?

Consumers, companies and policy makers need to have a broader conversation about these questions. The F.T.C. is leading this conversation, and will host a public workshop in November to discuss the promises of the diverse technologies and business models that constitute the Internet of Things, as well as the unique privacy and security risks on this frontier.

Creating consumer trust requires that we determine how to apply consumer privacy and data security principles to a world of increasingly ubiquitous, connected devices that are always on, that are always close at hand and that we increasingly depend on in our daily lives.