Frankfurt Kurnit Klein + Selz PC

Focus on the Data

Unique Insights and Practical Guidance on Privacy and Data Security Issues Worldwide

FTC Taps into Tapplock's Security Claims

By Elliott Siebers on April 16, 2020

On April 6, 2020, the Federal Trade Commission (FTC) announced a settlement with Tapplock, Inc., resolving allegations that the Canadian smart lock manufacturer violated Section 5 of the FTC Act by misrepresenting the security of its lock and of its

consumers' personal information. Following is a closer look at the **settlement** and underlying **complaint**, as well as an overview of the current recommendations for IoT device manufactures issued by the National Institute of Standards and Technology (NIST) in its most recent draft of the "Core Baseline" guide.

Tapplock's internet-connected, fingerprint-enabled padlock pairs with a companion mobile application to lock and unlock via a Bluetooth connection. The smart lock was touted as having an "unbreakable design" and as being "Bold. Sturdy. Secure." Furthermore, Tapplock represented in its privacy policy that it took "reasonable precautions" and followed "industry best practices" in protecting consumers' personal information.

Despite these claims, or maybe because of them, several security researchers set to testing the physical and electronic security of the smart lock and found that Tapplock's claims fell short. The FTC took particular notice of several vulnerabilities, including:

- A back panel was able to unscrew, which facilitated opening the lock.
- A vulnerability in Tapplock's Application Programming Interface (API) that allowed researchers to bypass account authentication and gain full access to all user accounts, which included usernames, email addresses, profile photos, location history and precise geolocation of their smart lock.
- Tapplock did not encrypt data sent between the lock and the app, allowing researchers to intercept it and easily identify and generate the digital keys needed for locking and unlocking any lock that was within Bluetooth range.
- Users were also prevented from effectively revoking access to their smart lock once they had provided other users access due to an additional security flaw in the app.

In its investigation of Tapplock, the FTC also scrutinized the company's security program (or the alleged lack thereof). The FTC's administrative complaint alleged that far from having "reasonable precautions" or "industry best practices," Tapplock did not have written data security policies or procedures, failed to conduct a risk assessment to identify reasonably foreseeable risks associated with its smart lock (which also prevented it from assessing the sufficiency of any safeguards that could have mitigated those risks),

and failed to develop a training program regarding privacy and security for employees that were responsible for testing and approving the mobile application software associated with the smart lock.

The Commission voted 5-0 to approved the administrative complaint and to accept the consent agreement with the company. The complaint alleged in two counts that the company engaged in deceptive acts or practices in violation of Section 5 of the FTC Act by misrepresenting 1) that its locks were secure and 2) that it had implemented a reasonable security program and industry best practices to safeguard consumers' personal information. The settlement will prohibit Tapplock from misrepresenting its privacy and security practices and require Tapplock to obtain third-party assessments of its information security program every two years. Penalties may apply if Tapplock violates the terms of the settlement.

As this action illustrates, IoT devices have tremendous potential to bring benefits to consumers in a variety of contexts, but companies in the IoT space should be conducting risk assessments and implementing risk mitigation strategies. And any company in search of more definitive guidance on how to structure their security practices should look to the NIST "Core Baseline" guide (**NISTIR 8259**) which offers several concrete recommendations relating to IoT device security. The Core Baseline builds upon NIST's previously published "Considerations for Managing IoT Privacy and Cybersecurity Risks" to help organizations manage the risks associated with different lifecycles of IoT devices. (**NISTIR 8228**).

Though the Core Baseline is in draft form and fairly technical, it still contains useful guidance that could help a company avoid the type of situation Tapplock now finds itself in with the FTC. If you're in the IoT space, the entire document is worth reading; but here are the recommendations for manufacturers briefly summarized:

- Identify expected customers and define expected use cases in order to determine which device cybersecurity capabilities the device should implement and how.
- Research customer cybersecurity goals. Manufacturers cannot completely understand all of their customers' risk because every customer faces unique risks. However, manufacturers can and should at a minimum make their devices' security align with expected customers and core use cases.

- Determine how to address customer goals by having their IoT devices provide particular device cybersecurity capabilities in order to help customers mitigate their cybersecurity risks. The baseline recommendations are:
    - Device Identification: An IoT device should have a way to identify itself, such as a serial number and/or a unique address used when connecting to networks.
    - Device Configuration: An authorized user should be able to change the device's software and firmware configuration.
    - Data Protection: It should be clear how the IoT device protects the data that it stores and sends over the network from unauthorized access and modification (i.e., encryption).
    - Logical Access to Interfaces: The device should restrict access to its local and network interfaces (i.e., authenticate the identity of users attempting to access the device).
    - Software and Firmware Update: A device's software and firmware should be updatable using a secure and configurable mechanism.
    - Cybersecurity Event Logging**:** IoT devices should log cybersecurity events and the logs should be made accessible to the owner and/or manufacturer.
- Manufacturers should consider the life cycle of the device and the hardware, software, and business resources that will be necessary to support cybersecurity at each phase.
- Define approaches and methods for communicating to customers. Many customers will benefit from manufacturers communicating to them about the risks associated with a particular device and the steps that users may take in order to mitigate those risks. Some topics that might merit being included in a customer communication could include, among others, cybersecurity risk-related assumptions that the manufacturer made when designing and developing the device.

Focus on the Data

Klein+Selz