ROPES & GRAY

WEBINAR

Advanced CSR and Supply Chain Compliance Webinar Series

April 3, 2017

Internet of Things Update: Considerations for Managing Supply Chain Cyber Risk

Technology partners Megan Baca and Jim DeGraw recently presented at a Ropes & Gray webinar entitled "Privacy & Data Security – Strategies For Mitigating Supply Chain Risks." The webinar was part of our Advanced CSR and Supply Chain Compliance Webinar Series. This article summarizes the main compliance takeaways from the presentation.

A replay of the webinar can be accessed here.

- **Regulation of the Internet of Things is evolving in a piecemeal fashion.** Participants in the Internet of Things supply chain must navigate a complex framework of federal and state legislation, as well as industry and consumer expectations. Possible regulatory sources include:
    - Federal regulation of trade, financial services and health and data privacy – Federal Trade Commission Act, Gramm-Leach-Bliley Act, HIPAA
    - State data breach security and notification statutes, "baby" Federal Trade Commission acts and substantive statutes/regulations
    - Foreign regulatory regimes (e.g., EU General Data Protection Regulation)

- **Companies should treat cybersecurity supply chain risk in the same manner as other high-priority enterprise risks.** Internet of Things device makers should establish processes and procedures to review, understand and mitigate cybersecurity supply chain risk at the highest organizational levels, consistent with other enterprise level risks. Data on cybersecurity supply chain risk should flow through the organization so that review can occur on a continuous basis and be based upon real-time or near real-time risk information.

- **Companies developing Internet of Things products should provide reasonable security to consumers.** In its 2014 report on the Internet of Things, the U.S. Federal Trade Commission recommended several steps companies can take to implement reasonable security measures, including:
    - Build security into devices by conducting a privacy or risk assessment, minimizing the amount of data that is collected, and testing security measures before launching products.
    - Train employees in security measures.
    - Implement a defense-in-depth approach when confronted with significant security risks.
    - Implement reasonable access control measures to the device and the consumer's data and network.
    - Monitor products throughout the life cycle and patch known vulnerabilities.
    - Retain and oversee service providers that are capable of maintaining reasonable security.

  These general suggestions are mere guidelines and do not necessarily have the force of law. Companies should be sure to check for specific laws or guidance that may apply to geographies or industry segments in which their products will be deployed.

- **Internet of Things device makers should manage security risks along the entire supply chain.** To help build security into devices, the National Institute of Standards and Technology recommends using a

cybersecurity risk management framework that emphasizes supply chain compliance. Cyber supply chain risk management should combine multiple strategies, including the following:
  - Draft cybersecurity requirements into contracts with suppliers and partners.
  - Communicate the importance of these requirements to counterparties and customers.
  - Verify that suppliers and partners are satisfying product cybersecurity requirements on an ongoing basis.

- **Contracts in the Internet of Things supply chain should address specific security issues.** While continuing to consider their location in the middle of the Internet of Things supply chain, companies should consider requiring certain terms in their contracts:
  - Representations regarding compliance with relevant law, the adoption of a security compliance program and disaster recovery plans, implementation of employee training and data encryption.
  - Covenants requiring regular system backups, return or destruction of data upon termination, broad confidentiality protection, and regular external audit updates.
  - Definitions for and terms relating to security breaches, including specific provisions determining a process for addressing breaches, identifying the party responsible for paying related costs, and deciding which party will control related investigations.
  - Carve-outs for confidentiality, data security, and indemnification from limitation of liability provisions.
  - Increases in direct damages caps for privacy or security failures.

- **When drafting contracts, device makers should consider their supply chain position.** Makers of Internet of Things devices often sit downstream from component producers and software developers and upstream from other producers and consumers within the supply chain. In this position, companies should ensure that the amount of risk they assume in contracts with downstream parties is consistent with the amount of risk assumed by upstream parties. These concerns are particularly relevant when defining the scope of representations and warranties and indemnification provisions. For instance, companies may want to avoid representing that their products are free of viruses and malware when their product contains third-party software, unless those same representations are made by the upstream supplier.

- **Companies should engage in meaningful vendor monitoring.** Legal and procurement review is a good first step in monitoring vendors but is insufficient on its own to ensure security in the Internet of Things ecosystem. Companies should partner with their vendors on privacy and security issues throughout the course of their relationships, not simply at the time of drafting the contract between the parties.

- **Participants in Internet of Things supply chains should play close attention to complexities that may arise when operating across international borders.** Many national regulators outside the U.S. are implementing their own approaches to data security. In order to comply with evolving international regulatory approaches, device makers should consider from a broad perspective the manner and means in which data is collected from consumers and ensure they are complying with local law in any countries where data is stored or products are sold.

Internet of Things Alert: Select Federal Trade Commission Enforcement Actions

The Federal Trade Commission has brought a number of enforcement actions dealing with privacy and security matters, including Internet of Things providers, most of which are closed out with consent decrees. A sample includes:

- In the Matter of HTC America (Jul. 2, 2013): Mobile devices manufactured by HTC had security vulnerabilities that permitted installation of malware without the user's knowledge or consent.

Vulnerabilities allegedly arose because HTC did not (i) provide its engineering staff with adequate security training, (ii) review or test the software on its mobile devices for potential security vulnerabilities, (iii) follow well-known and commonly accepted secure coding practices, or (iv) establish a process for receiving and addressing vulnerability reports from third parties. ***Takeaway: Well-established security procedures can help prevent and detect security vulnerabilities.***

- In the Matter of TRENDnet (Feb. 7, 2014): TRENDnet marketed Internet-connected video cameras for purposes ranging from home security to baby monitoring and claimed they were secure. However, some cameras could be accessed by anyone with the cameras' IP addresses. Consumers did not learn of this vulnerability until hackers posted live camera streams online. ***Takeaway: Consider and protect against device hijacking, alert customers to known vulnerabilities, and provide software updates to correct vulnerabilities.***

- In the Matter of ASUSTeK Computer (July 28, 2016): ASUS claimed its routers could "protect computers from any unauthorized access, hacking, and virus attacks." However, the router's web-based control panel featured security vulnerabilities that hackers used to change consumers' security settings without consumers' knowledge. ASUS also set a default account on every router in which the username was "admin" and the password was "admin." ***Takeaway: In advertising, accurately represent the security profile of devices, and protect against basic vulnerabilities.***

- FTC v. Vizio (February 3, 2017): Vizio advertised its Internet-connected smart TVs as "enabl[ing] program offers and suggestions." However, it failed to disclose to consumers that the TVs were recording viewing and demographic data. Vizio then sold this viewing information to third parties. ***Takeaway: Consider obtaining consumers' affirmative express consent for sensitive data collection and exploitation practices.***

- FTC v. D-Link (January 5, 2017; not yet resolved): As in ASUSTeK, the FTC has alleged that D-Link advertised its routers and IP cameras as secure but failed to prevent simple security flaws. The flaws identified by the FTC included the mishandling of a private key code used to sign into D-Link software, resulting in the key being openly available on a public website for six months. Unlike in ASUSTeK, the FTC has not alleged that hackers have actually exploited the alleged security vulnerabilities. ***Takeaway: The FTC may bring an enforcement action even absent proof that customers were actually harmed in. To mitigate risk of an enforcement action, device makers should adopt robust security programs.***

- A more complete list may be found here.

About Our Supply Chain Compliance and CSR Practice

Ropes & Gray has a leading supply chain compliance and corporate social responsibility practice. We advise clients across a broad range of regulations, commodities and geographies, and our clients include leading public and private companies, including fund managers, and trade groups from every major industry.

With on-the-ground expertise in the United States, Europe and Asia, we are able to take a holistic, global approach to supply chain compliance and CSR, to help clients efficiently and effectively structure and implement their supply chain compliance and CSR programs and mitigate risk.

For further information on our supply chain compliance and CSR practice or if you would like to learn more about the topics in this Alert, please contact your usual Ropes & Gray attorney or contact us here.

Ropes & Gray Supply Chain Compliance and CSR Mailing List

Click here to join the Ropes & Gray Supply Chain Compliance and CSR mailing list to receive Alerts, articles and program announcements relating to supply chain compliance and corporate social responsibility, or to sign up for other Ropes & Gray mailing lists.

Ropes & Gray Supply Chain Compliance and Corporate Social Responsibility Resource Center

As part of our commitment to excellence in this area, we have developed the Resource Center as a free educational tool for our clients, friends and other stakeholders. The Resource Center is the most extensive complimentary collection of supply chain compliance resources and is frequently updated to reflect new developments in this dynamic area. Click here to go to the Resource Center.