SQUIRE PATTON BOGGS

The Top Ten (Internet of) Things to Consider

The Internet of Things (IoT) has increased the amount of information organizations handle and has changed the way this information is collected, stored and used.

The collection, storage and use of IoT information also requires organizations to comply with a host of legal and regulatory obligations, which vary around the world.

While the IoT is designed to make a user's life simpler by providing devices that react and adapt to the user – whether a smart refrigerator, thermostat or home hub – to accomplish this, companies that provide these devices need detailed and specific information on the habits of the users. This information can be very personal in nature.

IoT devices frequently blur the line between previously separate sectors. As a result, it is possible that one device may be considered both a refrigerator (subject to the laws and regulations on consumer regulation) and a telecommunications service (subject to an entirely different set of regulatory obligations).

Given the significant growth in the IoT market, it is important to keep in mind the following key considerations:

1. **Design for security** – Laws, regulations and regulator expectations mandate implementing appropriate security into connected devices. The Federal Trade Commission (FTC) in particular emphasizes the need to implement security in the design process rather than an as afterthought, and California now specifically requires it.
   - What is the capability of the product to resist cyberattacks and are there exploitable gaps?
   - Is your security program reasonable (e.g., do you use industry-standard encryption; how effective are any security measures taken; and are there sufficient redundancies and safeguards built into the product)?
   - Have you implemented industry-standard security controls such as the CIS Critical Security Controls (e.g., configure securely, update continuously, block access and test and plan response)?
   - Have well-known and easily preventable security flaws been addressed (e.g., where the FTC will look first)?
   - Do you have an incident response plan to govern the disclosure of information in the event of an incident involving security or safety?
   - If you operate in the EU, have you checked whether tightening the security measures for internet-connected devices could restrict the free movement of equipment within the EU?

2. **Design for privacy** – Regulators like the FTC and state attorneys general expect privacy to be taken into account, beginning with product design, and they have penalized companies that fail to see obvious privacy flaws. It is important to assess the personal information you handle and evaluate compliance with state, federal and foreign (if applicable) privacy laws from the outset and thereafter.
   - Have you mapped and assessed how information from the product will be collected, retained, used and shared?
   - When does your product begin to collect personal information (out of the box without further consent)?
   - Does your product collect information for a limited purpose and then delete the information it no longer needs?
   - Have you provided appropriate notice to consumers (on packaging, in advertising, by salespeople and in website privacy statements) that complies with the law, best practices and regulator expectations?
   - What personal information could your product receive from consumers overseas and what procedures are there to handle compliance with foreign law (e.g., data transfer restrictions and localization requirements)?
   - If you have EU consumers, are you complying with and providing "adequate" data transfer protection under the EU General Data Protection Regulation?
   - Can compliance obligations be eased by participation in the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules system?

3. **Design for safety** – In order to comply with regulations that protect consumers from physical harm, you should build your product so that it is safe for consumer use, especially when marketed for use by children.
   - Have you considered which laws, regulations and industry standards govern your product (e.g., is it a product subject to the FDA or CPSC regulations that protect consumers from physical harm)?
   - Have you designed your product to be safe to human health for all foreseeable uses and misuses?
4. **Protect intellectual property rights** – In order to prevent litigation and protect your investment, seek national and international patent, trademark and/or copyright protection for your product.
   - Have you determined what aspects of the product are eligible for intellectual property protection?
   - Have you secured the rights to all aspects of the product design to reduce litigation risks upon launch?
5. **Request authorization from telecoms authorities** – Determine whether your product provides electronic communications subject to regulatory authorizations (e.g., from the FCC in the US or from foreign telecoms authorities if the product is sold abroad). You may also need to determine whether any other regulatory obligations apply (e.g., security, interoperability and net neutrality in the EU).
   - Which of the three FCC authorization schemes apply (i.e., verification, declaration of conformity and certification)?
   - Has your product been properly tested and classified (under all applicable laws)?
   - Is your product labeled according to FCC authorization requirements if necessary?
   - Is the product being offered outside the US and, if so, what other regulatory obligations may be applicable?
6. **Create accurate and truthful advertisements** – Ensure that all representations of product functionality and data security can be substantiated in order to safeguard the company from false or deceptive advertising claims.
   - Have you considered how your advertising will impact the regulatory classification of your product?
   - Have you ensured that your advertisements accurately reflect the performance, security and safety of your product (without overpromising on security)?
7. **Keep consumers informed through packaging and instructions** – In order to comply with the Fair Packaging and Labeling Act and other consumer protection laws, you should determine what information and instructions to include on packaging.
   - Have you considered the potential risks or vulnerabilities that can be mitigated through well-crafted warnings on your product?
   - Are you complying with the mandatory legal requirements regarding labeling your product?
8. **Set-up a continuous improvement loop** – Regulators expect companies to monitor post-sale complaints and safety or security incidents to identify vulnerabilities in either the safety or security of products and to make improvements.
   - Do you have formal procedures to monitor post-sale incidents for safety and security risks and clear criteria for prioritizing escalation and repair?
   - Do you have a product development plan to advance next generation designs and software patches to protect consumers?
9. **Examine license agreements closely** – Review all of your licensing agreements to determine whether your company is protected in the event of litigation over the intellectual property, safety or security issues that may arise after product launch.
   - Do you have formal indemnity provisions in the license agreement and how do they flow?
   - Have you ensured that your licensing partners have adequate design protections on security and safety in connection with products bearing your mark?
   - How will information be shared and incident responses handled in the event of security or safety events?
10. **Antitrust and competition** – Consider competition law as a tool to challenge or defend your IoT strategy regarding, for example, Big Data capture, portability and interoperability.
    - Does the IoT create a database that is too powerful?
    - Is the IoT based on proprietary platforms with limited ability to talk to smart products of other suppliers?
    - Does the IoT platform include or create standard essential patents (SEPs)?

Contacts

Alan Friel
Partner
T +1 213 689 6518
E alan.friel@squirepb.com

Francesco Liberatore
Partner
T +44 207 655 1505
E francesco.liberatore@squirepb.com

David Naylor
Partner
T+44 207 655 1668
E david.naylor@squirepb.com

51403/04/22