At the ABA Section of Science & Technology Law’s first Internet of Things National Institute on March 30-31, 2016, lawyers, policymakers, and technology specialists from across the country convened at Jones Day in Washington, DC to discuss securing the emerging IoT world. Acknowledging that up to seventy billion IoT devices may be connected by 2020, speakers addressed two key areas threatened by this technology: privacy and safety. They explained how US and EU regulations have failed to provide basic, uniform standards to secure consumer devices and critical infrastructure, and while denying the existence of any perfect, “one size fits all” solution, recommended how attorneys, manufacturers, and users can better practice “reasonable” security methods.

Concerning privacy, IoT devices generate enormous amounts of sensitive data. Fewer than ten thousand households using IoT automated systems can generate 150 million discrete data points per day. While each data point is on its own innocuous, in bulk, these independent points can constitute an almost perfect picture of an individual’s life, revealing information such as health, mood, fitness, personality, finances, religion, family, and friends. This data can be used for advertising, location tracking, surveillance, fraud, and assessing suitability for credit or employment, all without a user’s knowledge or consent. Ownership of this data has not been resolved, and it is quite common for IoT companies to process and market bulk data generated by devices to third parties. In 2014, the FTC found that twelve health-related mobile apps market sensitive health information, such as pregnancy and ovulation data accompanied by personally-identifying information, to third parties.

Privacy is not the only major concern raised by IoT, but user safety is also an issue. No device is fully immune to cyber attacks. Devices can be cheap, poorly coded, minimally tested, and many are incompatible with encryption or security updates. Hacktivists, criminals, terrorists, and nation states are targeting these vulnerabilities, sometimes by purchasing exploitation software or hiring hackers. Already, exploited IoT has caused insulin pumps to stop, a Turkish pipeline to explode, over nine-hundred nuclear centrifuges to self-destruct, and the Ukrainian power grid to shut down.

In light of the high risks to privacy and safety, regulators within the United States and Europe are adopting different approaches to enforce IoT security, resulting in a lack of harmonization and conflicting standards. The US is focusing on incentive-based approaches, hoping that the fear of litigation will prompt industries to adopt basic privacy standards. For critical infrastructure, where industry-wide standards are nonexistent, the Senate Homeland Security and Government Affairs Committee seeks to mitigate security risks through knowledge and support. Recent bills have focused on facilitating threat information sharing and instructing DHS CERT to provide companies technical assistance for incident response and prevention.

Contrastingly, the EU is taking a
much more restrictive, mandate-based approach than the US. Shown through its 2014 privacy provisions of the Article 29 Working Party and the 2015 General Data Protection Regulation, all EU IoT services must: obtain “specific, informed, and unambiguous” user consent in most situations; provide users with the right to withdraw their consent at any time just as easily as providing it; and give users the right to erase all collected personal data and withhold it from third parties.

**Absent standard IoT security provisions, here is basic advice lawyers can give their clients Advice for lawyers.** Do not assume clients have robust security measures. Ask many questions, and make sure everyone participates in the discussion: from engineers and security professionals to marketing personnel, budget approvers, and the highest levels of corporate governance. Also, partner with forensic technology specialists to understand IoT. Particularly for

**Gerar Mazarakis is ABA Section of Science & Technology Law’s student representative to Georgetown, where he is a first-year J.D. student specializing in cyber, national security, and international law.**

litigation discovery, specialists can help locate data found in obscure locations, such as in system logs, hidden files, and backups.

**Advice for users.** If your client uses IoT devices, ensure they change default passwords and apply the latest security updates. For old hardware that cannot be updated, use data analytics to monitor performance and ensure proper functionality. Set privacy configurations whenever possible, including encryption, and use Shodan, a search engine that browses for vulnerabilities in the internet of things, to detect whether your client has any insecure connected devices.

**Advice for manufacturers.** Encourage manufacturers to apply the FIPs principles: security, data minimization, notice, and choice. Regarding security: give security engineers an equal seat at the table when conceptualizing new devices; avoid hardcoded passwords; and use encryption and authentication whenever possible and practical. Consider sunsetting devices, meaning that if hardware will be incompatible with software updates after a certain number of years, allow the hardware to fail after that time. Conversely, for hardware that cannot receive updates, match expected viability of the software with the expected life of the device.

For data minimization, practice de-identification, and when possible, substitute sensitive information like precise geolocations with less-sensitive data like zip codes. Regarding notice, give consumers clear and simple notice and require consent for unexpected data collection or unexpected uses. Enable devices with privacy assistant software that will notify users of unusual data uses, such as detecting and informing users when a thermostat is broadcasting an email address.

Lastly, concerning choice, provide consumers control over the information generated by the device. Enable hub devices, such as routers connecting IoT devices to the internet, with easily-configurable, standardized privacy settings that will apply to all connected devices. When users cannot configure privacy settings, make sure they can prominently see when data-generating objects, such as sensors, are enabled and can easily shut them off.

The ABA Section of Science & Technology Law has been the national and global leader in providing lawyers, technology specialists, and users practical perspectives in emerging issues intersecting law, science, and technology. For membership, programs, committee discussions, content, and more, visit [http://www.americanbar.org/groups/science_technology.html](http://www.americanbar.org/groups/science_technology.html).