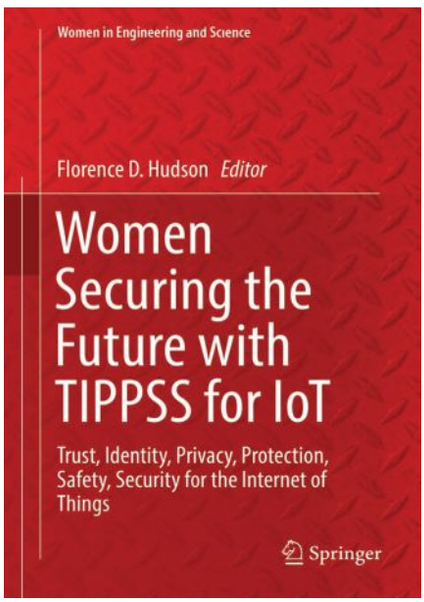
Trust, Identity, Privacy, and Security for the Internet of Things

By Soody Tronson, MS/JD
Founding Managing Counsel, STLG Law Firm / Founder and CEO, Presque, Inc.
Board Member, AWIS Palo Alto Chapter
AWIS Member since 2012

Last year, a friend asked me to co-author a book on data privacy. I said yes for several reasons. First, I always encourage women to take on new challenges and forge their path through unknown territory. Second, as an intellectual property attorney, privacy law is an integral part of my practice. Finally, as the CEO of a startup whose connected product will be using data to improve health outcomes, this is of particular relevance to my company. After the completion of the book, I met and worked with a diverse group of women I had not known before.

The book, "Women Securing the Future with TIPPSS for IoT: Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things," features contributions from 16 prominent female engineers, scientists, business, and technology leaders, policy and legal experts in the Internet of Things (IoT). With leadership from our editor, various authors have engaged in book tours and panels since its publication in June 2019. I, along with a few of my co-authors, most recently participated on a panel at the Society of Women Engineers 2019 Annual Conference.

The need for effective coordination
The IoT and data-enabled technologies have the potential to impact society at an unprecedented scale. Our legal structures, operating frameworks, and social norms concerning the IoT design, deployment, and usage of data often lack the cohesiveness needed for effective coordination. Presently in the United States, there are approximately 20



national-scale privacy or data security laws and hundreds of locally-applicable laws among the 50 states and territories. Recently some states have instituted laws directed at protecting user privacy rights, most notably the California Consumer Privacy Act (or "CCPA"). With the passage of each bill into law, comes a flurry of amendments, modifying their scope, sometimes clarifying and often introducing narrowing exceptions.

Specific federal laws preempt state laws, while others do not. Modernization of federal rules and the development of a national framework for the protection of an individual's privacy and consumer data would reasonably provide consistency for individuals and companies operating across state lines. Industry group coalitions impacted by the inconsistency of rules have been lobbying for federal regulations to override state laws. While commendable in their intent for uniformity and certainty, some suggested provisions are so ambiguous that they can be used to justify almost anything, leaving individuals with no adequate protection.

Rules and principles of privacy
Take the italicized exception, in one of the urged privacy principles: "Individuals should have meaningful controls over how personal information they provide to companies is collected, used, and shared, except where that information is necessary for the basic operation of the business or when doing so could lead to a violation of the law." An Internet-based company whose primary business model is monetization of data could then presumably collect any user data with the consumer having no control over its collection. Furthermore, some propositions do not justify the need for data collection, leaving the consumer with the choice of either refraining from using the service or consenting to the data collection.

Other proposed rules advocate for a national privacy framework, enforceable at the federal level by the FTC and at the state level by state attorneys, removing the private rights of action under state privacy laws. For example, the Illinois Biometric Information Privacy Act of 2008 ("BIPA") is one of the strictest state privacy laws directed at the uniqueness of biometrics data and information. BIPA strictly forbids private entities to collect, capture, purchase, or otherwise obtain a person's biometrics, including

1. IoT: Is It a Digital Highway to Security Attacks?
   Edna Conway
2. IoT: Privacy, Security, and Your Civil Rights
   Cynthia Dianne Mares
3. Privacy in the New Age of IoT
   Qi Pan
4. A Business Framework for Evaluating Trust in IoT Technology
   Fen Zhao, Britt Danneman
5. Ahead of the Curve: IoT Security, Privacy, and Policy in Higher Ed
   Joanna Grama, Kim Milford
6. Trust, Identity, Privacy, and Security for a Smart Campus
   Karen Herrington
7. Security for Science: How One Thing Leads to Another
   Hannah Short
8. The Dark Side of Things
   Licia Florio
9. Public Safety and Protection by Design: IoT and Data Science
   Alicia D. Johnson, Meredith M. Lee, Soody Tronson
10. Privacy Management in the Internet of Things (IoT)
    Grace Wilson Caudill
11. Securing IoT Data with Pervasive Encryption
    Eysha Shirrine Powers
12. Secure Distributed Storage for the Internet of Things
    Sinjoni Mukhopadhyay
13. Profiles of Women Securing the Future with TIPPSS for IoT
    Florence D. Hudson

a scan of their face geometry, without that person's consent, and provides private rights of action for its breach. Many Internet companies appear to have been unaware of this law, paid little attention to it, or did not weigh in on the bill. They may now be subject to substantial financial liabilities for its breach (e.g., Flicker and Facebook) and have initiated influential lobbies to weaken its provisions, including the removal of the private rights of action.

What's next

Many new U.S. laws regarding privacy and security will go into effect in 2020 (e.g., CCPA). As companies prepare for 2020, they must incorporate concrete, evidence-based, and adaptive data-protection programs mindful of the complexity and volume of code and the risk of a breach. The strategies around compliance have to be evaluated and devised in a proactive perspective rather than a retrospective band-aid approach.

Many companies with international presence will also have greater exposure to fines under the European Union's General Data Protection Regulation (GDPR), which took effect on May 2018. Other international laws may also impact companies, such as Brazil's Lei Geral de Proteção de Dados (its version of the GDPR), passed in 2018 and going into effect in 2020.

With the full range of new, and at times, conflicting state, federal, and international privacy compliance standards, it's imperative that companies have sound strategies in place, including access to robust unified database of global privacy and security regulatory requirements. ✪

Soody Tronson, MS/JD, *has over 25 years of interdisciplinary experience in technology, business, management, education, and law in start-up and fortune 100 companies. Soody is the Founder and CEO of Presque, a startup venture creating wearables that fundamentally change and improve the health of women and infants, positively disrupting the status quo. Soody is also the Founding Managing Counsel at STLG, a boutique Silicon Valley law firm counseling domestic and international clients in intellectual property and technology transactions in a wide range of technologies. After holding technical and management positions at Schering Plough and Hewlett-Packard where she took several products to market; and practicing law at HP, and a successfully acquired medical device start up, and two national law firms, HellerEhrman and Townsend and Townsend; she formed STLG. Presque was formed in 2016 to develop and commercialize a line of wearables based on Soody's original design. Guided by the belief that we each have a sphere of personal influence and it is our civic duty to use it for the betterment of our community, Soody is deeply committed to creating positive change. She serves in advisory, board, and leadership capacities with several organizations including AWIS STEM to Market national Accelerator and its Palo Alto Chapter; California Lawyers Association Executive Committee of the Intellectual Property Section, Licensing Executives Society USA/Canada, and the Palo Alto Area Bar Association. As a member of the Silicon Valley Leadership Group, a diverse public policy association of dynamic companies shaping the future innovation economy, she is actively engaged with the Technology and Innovation, Health, and Education and Work Force Development Groups.*