RSAConference2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: LAW-R12

A CALL TO (H)ARMS: THE CRY FOR HARMONIZATION OF SECURITY AND PRIVACY LAWS

MODERATOR: **William S. Rogers, Jr.**
Partner, Prince Lobel Tye LLP
@wsrogers26
@PrinceLobel

PANELISTS: **Charles Cresson Wood**
Attorney and Security/Privacy Consultant, InfoSecurity Infrastructure, Inc.

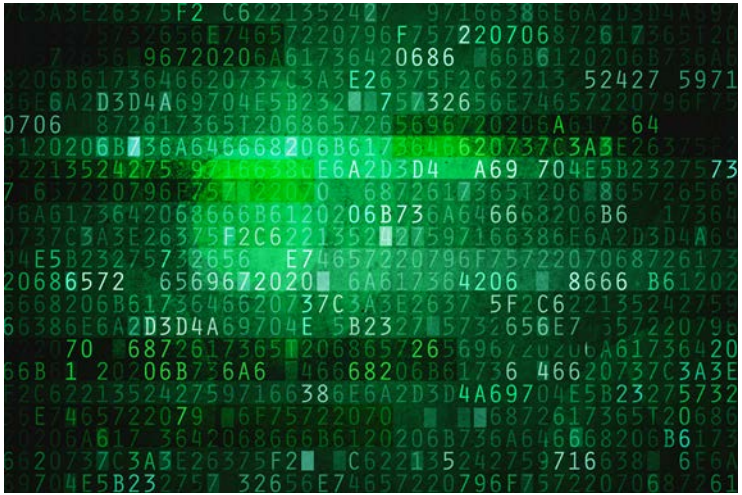
April Doss
Senior Minority Counsel, Senate Select Committee On Intelligence

Ralph Spencer Poore
X9F1 Vice Chair, X9 Financial Services

Piecemeal, Patchwork, or a Crazy Quilt?

- In today's legal environment, achieving cyber/privacy compliance requires meeting the standards of a diverse and dispersed set of rules:
  - State, national, and multinational laws and regulations
  - Contractual requirements
  - Common law theories – e.g., fraud, invasion of privacy, other liability

Legislative and Regulatory Frameworks Vary Widely



- “Traditional” data breach laws focus on consumer protection – with liability tied to the impact on individuals
- U.S. federal regulations vary by sector
- International legal framework growing more complex

New Approaches And Unregulated Problems

- Novel approaches are beginning to emerge
  - NYDFS 500
    - Requires specific cybersecurity best practices
    - Emphasizes business continuity and consumer protection
    - Widely influential – a reg that punches above its weight
- But a growing number of thorny problems have no legislative or regulatory solution, e.g.
  - Bias in artificial intelligence and analytics
  - Meaningful consent to use of data
- And legislative and regulatory approaches struggle to keep pace

Legislative schemes, regulatory schemes, and quantum policy

- Challenges with existing approaches
  - Legislators often lack deep technical expertise
  - Legislation tends to move slowly and is hard to change
  - Corporate interests can be extremely influential
  - Regulatory frameworks can change with political elections, leading to uncertainty
  - Judicial interpretations accumulate slowly over time
  - Cross-border differences are hard to resolve
- What a “quantum” approach to policy could mean

Jurisdictional Fragmentation

- Confusion, unnecessary costs, and lack of action
- Laws based on national boundaries don't synch with Internet, satellite cell phones, and globalization
- Complexity of multi-layered software conceals user location (encryption, bots, virtual reality avatars, etc.)
- Cloud providers need load balancing, performance management, contingency planning, and other services
- Inconsistencies in extradition treaties, search warrants, courts, alternative dispute resolution forums, and electronic discovery processes hamper investigations and prosecutions

Information Explosion

- Existing decision-making systems overwhelmed by volume of disputes, population increases, and complexity
- Connectivity and interdependency reflected by the IoT world threatens to create chaos
- Number of involved parties in modern information systems, often with unclear interfaces, tasks, and roles, creates a legislative and regulatory nightmare
- New approaches that categorize events and situations with predetermined criteria are needed like: automated dispute resolution via artificial intelligence, smart contracts, digital signatures, and block chain encryption

Divergent Pace of Change

- Legal world is backward-looking but technological world is forward-looking, and legal world just keeps getting farther behind the reality of the technology deployed
- Traditional rule making systems involve checks and balances, lobbying, proposals of a bill, public comment, voting of the legislature, formal executive approval, often appeals, issuance of implementing regulations, and this is way too slow for the current pace of change
- European Parliament GDPR reveals slow American legal development, and how it lags behind what is needed
- Law of airborne drones provides good example of the gap

Waiting for a Crisis

- Common law tradition of changing the law after crisis and problems occur no longer serves us
- The rule of “stare decisis” (rule of precedent) has old and ill-fitted rules repeatedly applied
- Proactive stance required now because what is at risk has become the very infrastructure on which society is built
- Move from reactive focus of detection, recovery, correction, adjudication, and awarding damages, to proactive focus to orchestration, prevention, correction based on quality control, deterrence, and avoidance
- Zero-day exploits like Stuxnet reveal existing vulnerability

Widespread Incompatibilities

- Errors, gaps, interface inconsistencies, unclear documentation, unclear roles, unclear responsibilities, and related problems present attractive attack surface
- Research at SRI International reveals attackers consistently attack these points because they present attractive exploit opportunities (consider software patching as a generalized example)
- Digital copyright infringement gravitates to jurisdictions that do not seriously enforce copyright conventions
- Rules made by states, separately by nations, plus multi-national authorities creates an inconsistent patchwork

A Specialized Global Legal and Regulatory System Is Required

- A system which mirrors the breadth and scope of the internet is required
- The current Legislative Process is too cumbersome
- The current Adjudicatory Process is hampered by lack of experienced resources

Uniform Laws And Enforcement Mechanisms Are Also Required

- Standard definitions, uniform standards of care, etc. are required
- Priority must be given to laws which promote deterrence and accountability

Harmonization Of Multiple International Laws Can Work

- A multi-stakeholder approach to the creation of harmonized cyber-security and privacy laws is a logical approach
- The multi-stakeholder approach has achieved success in harmonizing other seemingly incompatible international regimes

Technical Issues And Standards As A Model

- Speed of technological innovation
  - New types of assets
  - Rapidly evolving products and services
  - AI and robotics
- Massive interconnectedness
- Standards essential
  - Interoperability
  - Scalability
  - Security & Privacy

Standards Model (cont.)

- Rule making and standards development
  - More forward looking
  - Must continue to support consensus processes
  - Stakeholder inclusive
  - Leverage advancing technology
  - Jurisdiction agnostic
- Compliance assessment processes
  - Automated enforcement (when/where feasible)
- Participatory
  - Theoretical, e.g., policy, forecasting, modeling
  - Practical
  - Advocacy

Questions, please!

- Please approach the microphone, and state your name and question for the panel.
- If we run out of time, the panel members and moderator will be available after the program to address questions privately.

Contact Information

William S. Rogers, Jr., Esq.
wsrogers@princelobel.com (617) 456-8112

April F. Doss, Esq.
april_doss@ssci.senate.gov (202) 224-1737

Ralph S. Poore
rspoore@ralph-s-poore.com (817)-235-8672

Charles Cresson Wood, Esq.
ccwood@ix.netcom.com (707) 937-5572.

Today's Presentation Is Based on the Following Articles:

- "A Simple Appeal to Common Sense: Why the Current Legal & Regulatory Regime for Information Security & Privacy Doesn't Work, and Can't Be Made to Work," *ISSA Journal*, December 2017 (cover story)

- "Why It's Now Time for an Internationally Harmonized Legal Regime for Information Security & Privacy," *SciTech Lawyer*, Spring 2018 (American Bar Association)

- "Why Changes in Data Science Are Driving a Need for Quantum Law and Policy, and How We Get There," *SciTech Lawyer*, Fall 2017 (American Bar Association)