

FTC Conference on Privacy and Security: Challenges, Responsibilities, and Way Forward

Presentation: 15 minutes plus Q&A

<https://youtu.be/v8Mc5PqXlpg>

13:4 Minutes

Privacy and security are ultimately public policy domains. In preparation for public policy debate and determination, the landscape must be framed in the sometimes unpleasant realities of current technology and practice that call out for industry challenges, government responsibilities, and revised expectations going forward.

Publicly airing these realities may arouse skepticism among some, strike panic among others, and prompt just a ho-hum reaction from still others. Advocates of the status quo attempt to convince us that privacy fears are unwarranted and misplaced. Victims of the OPM Cyber attack might argue otherwise.

Dealing with the stresses surrounding privacy and security where privacy is the freedom and ability to reveal oneself selectively and security is the condition of being protected against danger or loss, we find that both are reasonable goals but on a collision course nevertheless. Is it possible to have both privacy and security? Whereas Cyber Security is reasoned about in terms of trust in systems, the collision between privacy and security revolves around trust in people.

Here the question is one of civility where civility is comprised of the sacrifices one makes for others. For example, are businesses and the public willing to sacrifice privacy by sharing encryption keys with government or is government and law enforcement willing to sacrifice access to encrypted data and information? The slow walking investigation of the Hillary Clinton email and server suggests the politicization of the same federal agencies involved in the data encryption key controversy where trust in the people in government is lacking. That leaves trust in systems to reliably manage a government data encryption key database, bringing to mind again the OPM attack and the failure of government systems.

And then there is this; privacy is inexorably linked to Cyber Security. Here the minimum Cyber Security practice set include the following:

- Don't use the Internet for data and information you can't afford to lose.
- Adopt three factor authentication.
- Adopt data encryption.

When it comes to Cyber Security, it's not about money and it's not about Silicon Valley cafe amenities and automation. More broadly, it's about know how and will in meeting industry challenges and accepting government responsibilities.

- Industry challenges demand renovating the rotten core of the software profession and its Cyber Security practice and shifting the onus for privacy and security from supplier to consumer.
- Government responsibilities include removing government obstacles to consumer self-help and unleashing new Cyber weapons for privacy and security governance.
- The Way Forward calls for adopting new and useful Cyber expectations for both industry and government.

Industry Challenge #1: Renovate the rotten core of the software profession and its Cyber Security practice

The software situation in 2011 can only be described as dire. The increasing dependence of industry and government on an insecure Internet infrastructure built on an immature software profession whose promise exceeds its delivery has now become a source of risk that teeters at the tipping point. The convergence of software, national security, and global competitiveness interactions and their fragile dependence are capable of unleashing a destructive synergy of propagating and cascading effects impacting privacy and security. Simply put, the core of this apple is rotten.

There is a lack of software engineering discipline in practice. Instead there is a high tolerance for technical debt. Technical Debt is the organizational, project, or engineering neglect of known good practice that can result in persistent public, user, customer, staff, reputation, or financial cost. Of course, technical debt stems from a combination of ignorance, neglect, and even the intentional deferment of effort.

Beyond the dire software situation and high tolerance for technical debt, industry engages in free wheeling claims of unproven privacy in its public statements of privacy policy.

Industry Challenge #2: Shift the onus for privacy and security from supplier to consumer

Eliminate unchecked free riders whose presence attracts Cyber attacks *where some individuals in a population either consume more than their fair share of a common resource, or pay less than their fair share of the cost of a common resource*. The common resource under consideration here is the Internet where the minimum Cyber Security practice set includes the following:

- Don't use the Internet for data and information you can't afford to lose.
- Adopt three factor authentication: what you are, what you know, what you have.
- Adopt data encryption: private encryption not key escrow or split key.
- Eliminate the practice of technical debt.

Adopt Clean Room Software Engineering. There is the need for a rigorously defined Clean Room method and process to produce a provably correct Clean System: one whose method possesses the means to investigate legitimacy, confirm intent and wherewithal of people, verify process execution, and validate outcomes achieved in determining that a legitimate Clean Room was in place and operation and one whose outcome is based on trusted software engineering principles and practices in producing provably correct software components. In addition, adopt Next Generation Software Engineering. In accordance with the austerity of the times, the immediate goal of practical Next Generation Software Engineering is to drive systems and software engineering to do *more with less... fast* using smart, trusted technologies.

Government Responsibility #1: Remove government obstacles to consumer self-help

The following government imposed obstacles are highlighted here:

- Provide industry with indemnification to enable data and information sharing.
- Permit industry unfettered use of private encryption.

Tied to Cyber Insurance and the need for actuarial information, the Government needs to concede to indemnifying industry in order to encourage data and information sharing by industry partners.

The government needs to accept and encourage private encryption and not hold out for key escrow of split key encryption. Data encryption, contested by government and slow to be adopted by industry, lies at the intersection of privacy and security. Basically plaintext is information that is input to a coding process, cleartext is information that is immediately understandable to a human being without additional processing, and ciphertext is the output of an encryption process featuring an algorithm that makes plaintext information unreadable to anyone except those who possess a unique key. To combat crime and terrorism, the government wants access to these unique encryption keys in order to return ciphertext to cleartext and its readable plaintext form; industry and its consumers and users object to any sharing of encryption keys on privacy and security grounds.

Government Responsibility #2: Unleash new Cyber weapons for privacy and security governance

In addition to providing industry with indemnification to enable data and information sharing and unfettered use of private encryption, it is the government responsibility to:

- Impose fines for neglectful Cyber Security practice.

- Enable Cyber Insurance with enhanced data and information sharing and actuarial data.
- Prosecute false claims in privacy policies.

Cyber fine imposed on the victim of a Cyber incident is straightforward. Since neglectful and unprepared organizations serve as a attraction to Cyber bad actors and their actions, these unready organizations make the Internet less safe for everyone. While fines may appear punitive, they actually operate as tough love measures that encourage organizations to take the prudent measures known to be effective in order to improve the landscape for all.

The uncertainties associated with a useful and credible Cyber Insurance market are wide ranging and depend on Cyber Security theory and foundations, reduction of theory to practice, the collection and use of empirical practice data, the validation of actual practices against the theory based on empirical data, information sharing, realistic premium setting, informed and trustworthy coverage, and straightforward dollar convertible Cyber consequences. These uncertainties have not yet been reduced to calculated risks.

The result of a shifting definition of privacy and immature privacy practices, an uncontrolled Internet infrastructure and unproven Cyber Security practices, and free riders in free spirited Internet culture has led to frivolous privacy policy assertions, promises, and commitments that border on false claims. The unproven state of Cyber Security protection is well known by the experts in the field and less known and accepted by industry executives. An enterprise whose privacy policy commitments are not matched by a capability to meet the commitments made is presenting itself in a false light and where done knowingly is guilty of actual malice.

The Way Forward: Adopt new Cyber expectations for both industry and government

The following markers of Cyber expectation need to be laid down:

1. Eliminate unchecked free riders whose presence attracts Cyber attacks
2. Don't use the Internet for data and information you can't afford to lose
3. Expect fines for neglectful Cyber Security practice
4. Expect the use of three factor authentication
5. Expect the use of unfettered data encryption
6. Expect to be prosecuted for false claims assertions in privacy policies
7. Provide industry with indemnification and expect data and information sharing
8. Expect industry partners to purchase Cyber Insurance as actuarial data improves
9. Expect zero tolerance for technical debt, defects, and intentional deferment of effort
10. Expect adoption of Clean Room Software Engineering and Next Generation Software Engineering

Conclusion

In conclusion, we need to:

- Renovate the rotten core of the software profession and its Cyber Security practice
- Shift the onus for privacy and security from supplier to consumer
- Remove government obstacles to consumer self-help
- Unleash new Cyber weapons for privacy and security governance
- Adopt new and useful Cyber expectations for both industry and government

Are there any questions?