ACM's New Effort in Computer Science and Law

Joan Feigenbaum

http://www.cs.yale.edu/homes/jf/

13 June 2019; EPFL Summer Research Institute

Inaugural ACM Symposium on Computer Science and Law

- October 28 – 29, 2019 at New York Law School
- General Chair: Joan Feigenbaum (Yale Univ., Comp. Sci.)
- Program Co-Chairs
  - Pam Samuelson (UC Berkeley, Law School and Inf. School)
  - Danny Weitzner (MIT's Internet Policy Research Initiative)
- Keynote Speakers
  - Jack Balkin (Yale Univ., Law School)
  - Shafi Goldwasser (Simons Institute for Theory of Computing)
  - Ed Felten (Princeton Univ.; Comp. Sci., Woodrow Wilson School of Public and Int'l. Affairs, and Center for Inf. Technology Policy
- https://computersciencelaw.org/

Background

- ACM wants to revise its scope and structure in response to the changing and expanding definition of “Computer Science.”
- Since ACM’s founding (mid-20th century), computers have become essential tools in almost all aspects of human endeavor.
- New phase:
  - Sophisticated computation has become a thing in activities ranging from finance to journalism to dating.
  - **People who can understand and exploit computational methods and principles, rather than simply use computers as appliances, now have a decisive advantage over their less computationally astute competitors.**
  - In the research world, **there’s a broader idea of “who counts as a computer scientist?”** Many CS researchers are now doing things that used to be considered social science.

➢ ACM’s new scope will include more interdisciplinary areas, including Computer Science and Law.

What is “Computer Science and Law”?

- Formulating and solving problems that are **simultaneously computational problems and legal problems**, *e.g.*, crypto-currency, content moderation, the gig economy, *etc.*

- **Counter example of good CS+Law research: digital copyright**
- Copyright clause of the US constitution

  Article 1, Section 8, Clause 8: Congress shall have the power to “promote the progress of science and the useful arts by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.”
- Current instantiation is incompatible with digital creation and distribution of copyright works (copy-centric, logically incomplete, *etc.*). **We should rewrite US copyright law with both the constitution and the Internet in mind.** But there’s no effort to do so.

Example 1 of a CS-and-Law Problem

Encryption and Surveillance:
Why the "Law-Enforcement Access" Question Won't Just Go Away

What is the “LE-Access” Question?

- 1990’s “Crypto War” Redux
  - ❑ US Gov’t: Need “key escrow” to deregulate Cold-War era, strong crypto.
  - ❑ (Most) Technologists and civil-liberties advocates: Key escrow is hard to implement securely and would boost foreign competitors of US technology companies.
  - ❑ Opponents of key escrow won this war.

- 2010’s: Tech industry reacts to the Snowden revelations.
  - ❑ Broader and deeper use of E2E, default encryption.
  - ❑ Law enforcement (LE) claims that it is “going dark.” It calls upon vendors to **enable decryption by LE with a duly authorized warrant but without the user’s passcode.**
  - ❑ Vendors object, saying that LEA would hurt customers’ security and privacy.

- (Perfect) example: FBI vs. Apple

Summary of 2016 FBI vs. Apple Case (1)

- Terrorists Syed Rizwan Farook and Tashfeen Malik shot up the San Bernandino, CA health-deparment building where they worked, killing 14 and injuring 22.
- The FBI took possession of an iPhone that the health department had issued to Farook. The phone was locked, Farook was dead, and exhaustive search of the passcode space would not work.
- The FBI asked Apple to unlock the phone.

Summary of 2016 FBI vs. Apple Case (2)

- Apple said that it could not unlock an iPhone running iOS 9 without the user's passcode.
- FBI: Motion to compel Apple to develop software that would unlock ***this*** phone.
- Apple: Motion to dismiss; "undue burden."
- The legal question is still unresolved: The FBI discovered that it could use a commercially available "gray-hat" hacking tool to unlock the phone, and it withdrew its motion to compel.

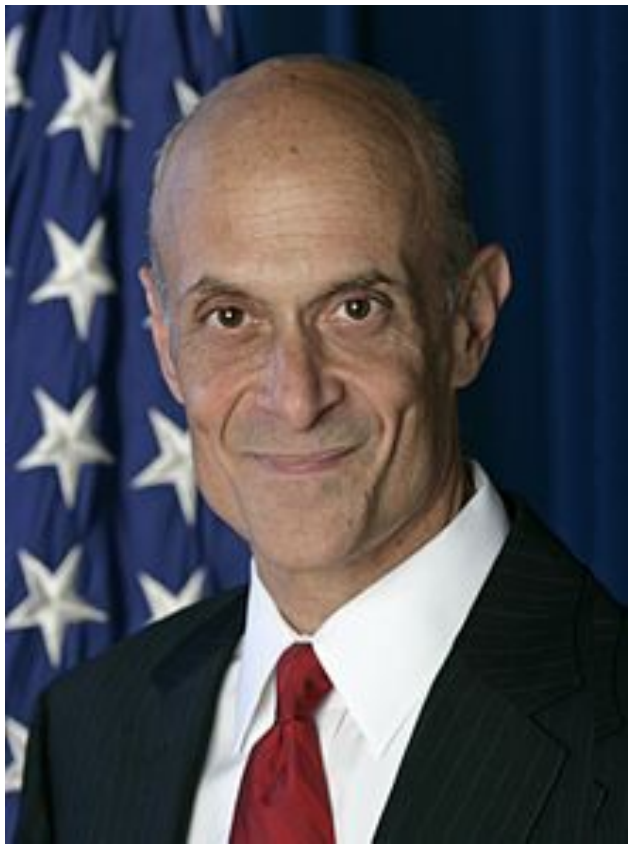
James Comey (2014)

"Those charged with protecting our people aren’t always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."

Tim Cook (2016)

"The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals. … We can find no precedent for an American company being forced to expose its customers to a greater risk of attack."

Michael Chertoff (2016)



"As you create back doors or tools, in effect you're creating a kind of malware. Once you have it, are you confident you can protect it? If it gets in the wrong hands, is that going to be a problem? …

Let me ask you this question. Would law enforcement be better off in a world where nobody had any locks on the door? It would be easier to serve search warrants, but there could be a lot more burglaries. Maybe sometimes you want to reduce the number of burglaries even if it's harder to execute search warrants."

Pro-LEA Side of the E+S *Policy* Debate

- The technology industry's post-Snowden embrace of default encryption is willfully thwarting the *lawful* exercise of warrants and court orders.

- Individuals and organizations are obligated, under the All Writs Act in the US and similar laws in other democratic countries, to assist the government in the execution of warrants.

  > 28 USC 1651(a), 1789: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages of and principles of law."

  Not "just an 18th-century law": A 1977 Supreme-Court decision said that New York Telephone was obligated under the All Writs Act to install a pen register.

- This position is fleshed out and explained well by Hennessey and Wittes [HW16].

Anti-LEA Side of the Policy Debate

- Technologists and civil-liberties advocates do ***not*** deny that E2E, default encryption hampers legitimate LE activity to some extent. But …
- **Since 9-11, there has been far too much mass surveillance. The best grass-roots response is mass encryption.**
- **Widespread use of sound encryption is our strongest weapon in the fight against intellectual-property theft, identity theft, and many other online crimes – something that LE should applaud.**
- As in the 1990's crypto war, access capabilities for use by the ***US*** LE community only (NOBUS) could boost foreign competitors.
- The ***extent*** of cooperation required by the All Writs Act is unclear. Apple might have won on the grounds of "undue burden."

Anti-LEA Side of the E+S *Technical* Debate (1)

- LEA features may create unacceptable cyber-security risk. ***Once a technical capability is built into a system, there is always a risk that it will be misused*** – sometimes by the very criminals that it was designed to thwart.
- Classic example: the Vodafone Greece scandal

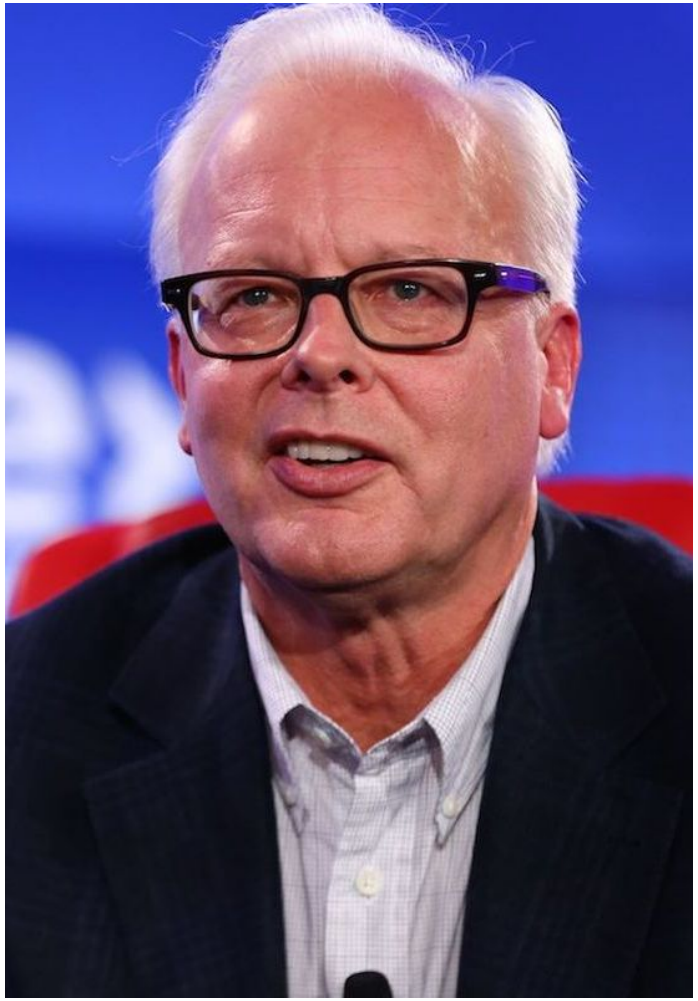
  The Greek government contracted with Vodafone to build a phone system that had a wiretapping capability mandated by US Law.

  Hackers broke into the system and used the wiretapping feature to eavesdrop on the Greek government.

Anti-LEA Side of the E+S *Technical* Debate (2)

- LE has not quantified the extent to which default encryption hinders it.
- LE often has other means of obtaining the information it needs, *e.g.*:
  - Back-up copies decryptable by cloud-service providers or corporate key-escrow systems
  - Sensitive data collected in plaintext form by ad-supported platform services
  - Vulnerability-based unlocking toolkits (the anti-climactic end to FBI vs. Apple) [BB+18]
- So far, no LEA requirements document. E.g., LE has not explained:
  - Which surveillance tasks does LE expect to accomplish despite default encryption?
  - *Who* will have LEA? There are more than 15,000 police departments in the US.
  - Will US technology vendors cooperate with LE in *all* countries in which their products are sold (including dictatorships)? If not, where will criminals buy their devices?
- These arguments are given in, e.g., [AA+15, NA+18, ZO+16], and a framework for evaluating proposed LEA designs in given in [NA+18].

Technical Ideas for LEA Features (1)



- High-level ideas. No fully specified proposals yet.
- ***Most target the unlocking of devices, with manufacturer's cooperation, by LE agents who have physical possession of the device and a warrant (but not user's passcode).***
- Best known idea is due to Ozzie:
  - Device's encryption key is stored on the device, encrypted under a manufacturer's key.
  - An LE agent extracts the encrypted device key from the phone and sends it to the manufacturer. The manufacturer decrypts the device key and sends it back to LE.
  - A device that is unlocked without the passcode "bricks" itself (tamper-evidence).
- Flaws were quickly found in Ozzie's scheme [BB+18]. It's not yet clear whether the basic idea can be built into a sound, fully specified scheme.

Technical Ideas for LEA Features (2)

- Different approach due to Wright and Varia [WV18].
- Not restricted to unlocking devices without users' passcodes. ***Enables the decryption of a limited number of ciphertexts***, which can be found in any system or application.
- Deploy cryptosystems in which the key space has less than maximum entropy. A very well resourced attacker can then:
  - Perform an extremely expensive (approx. $100M to $3B) upfront computation to narrow down the key space ("abrasion").
  - Perform a limited number of moderately expensive (approx. $1K to $1M per message) brute-force searches for the keys needed to decrypt specific, targeted messages ("crumpling").
- The "well resourced attacker" does ***not*** need to be an LE agency (much less a US LE agency). ***This is not a NOBUS approach!***
- [WV18] doesn't require LE to cooperate with manufacturers or secure-protocol developers. Lightweight constructions are woven into existing protocols and applications.

My Position in the LEA "Debate"

- Don't implement LEA at this time.
- The arguments in [AA+15, NA+18, ZO+16] are persuasive, especially:
  - Lack of agreed-upon technical requirements: Until we know exactly what LE wants, we can't know whether it's technically feasible and cost-effective.
  - We don't yet have a fully specified LEA proposal to evaluate, build, and test.
  - I'm not convinced that LE is "going dark" or "being crippled" by encryption.
- LEA might also just be a bad idea on principle.

My Position in the LEA "Debate"

- Don't implement LEA at this time.
- The arguments in [AA+15, NA+18, ZO+16] are persuasive, especially:
  - ❑ Lack of agreed-upon technical requirements: Until we know exactly what LE wants, we can't know whether it's technically feasible and cost-effective.
  - ❑ We don't yet have a fully specified LEA proposal to evaluate, build, and test.
  - ❑ Availability of alternatives to LEA
- LEA might also just be a bad idea on principle.

- **But I also think that LEA deserves further study.**

The Status Quo is Unsatisfactory

Jonathan Zittrain (2016)

"I empathize with the idea that just how much government can learn about us should not depend on the cat and mouse game of technological measure and counter-measure. ... Ideally, a polity would carefully calibrate its legal authorities to permit access exactly and only where it comports with the imperatives of legitimate security."

The Status Quo is Unsatisfactory

- The Crypto research community should not be telling LE to:
  - ❑ Rely on the fact that there's lots of plaintext out there, or
  - ❑ Buy gray-hat hacking toolkits from Greyshift or Cellbrite or some other company that profits from unremediated bugs and might be selling those toolkits to bad actors.

  Doing so is rank hypocrisy!

- Theory of cryptography may enable us to design a provably secure, cost-effective LEA scheme ***or to prove that no such scheme exists***.

Example 2 of a CS-and-Law Problem

Imbalanced and unfair data environment[1]:

- Individual creators of commercially valuable data receive no recognition, protection, or compensation.
- Some opportunities to create value are lost, because platforms can't monetize them.

[1] Shoshana Zuboff**, Surveillance Capitalism,** Public Affairs, 2019

“Data Co-ops”

(I don’t like this term.)

- Data intermediaries that maximize aggregate value of data and minimize individual risk to users
- Could be centralized and top-down or decentralized and bottom-up.
- **Technological advances, public opinion (“techlash”), and new regulations (GDPR) make this the right time.**
- Data co-ops could offer users and small companies:
  - Contractual and technological protection
  - Provable compliance with laws and regulations
  - Data linkage and aggregation within niche domains
  - Fine-grained and changeable permission systems for secondary uses of data

Related Projects [partial list] (1)

- Making data accessible to analysts
  - Meeco: Users exchange data for personalized offers from brands.
  - CitizenMe: Users sell or donate data to academic researchers.
  - Datacoup: Users decide who can buy data for a small fee.
  - Midata.coop: Users donate health data for research in exchange for data analysis and interpretation tools.

- Restoring individual data subjects' control
  - Hub of All Things: Personal data micro-server; "wrappers" protect the data.
  - Solid: Tim Berners-Lee's "socially linked data" project
  - Enigma: Decentralized and secure "data infrastructure"

Ongoing Projects [partial list] (2)

- Creation of data collectives that advocate for members' data rights
  - The DataUnion: Aim is to form an org. that can negotiate with big tech companies.
  - The Data-as-Labor Movement: Aim is to achieve recognition, protection, and compensation for the provision of personal data.

Desiderata

- Market for data products
  - Price discovery. **“ ‘Free’ services in exchange for data” is not the only way to do things.**
  - Expression and discovery of users’ needs
  - Avoidance of data monopolies
- Technological and legal ability of data co-ops to
  - Compensate individuals for both the risks they take and the data they provide
  - Guarantee high quality and statistical validity of data products
  - Provide state-of-the-art privacy and security
- Usability by non-experts
  - Delegated decisions: **Allow individuals to determine their level of involvement.**
  - Meaningful choices about data use and the right to change permissions
- ***Research!*** (Get involved.)

Research Principles

- Broad agenda
  - Theory and experimentation
  - Basic (“curiosity-driven”) and applied (“market-driven”)
  - Intellectual rigor
- Emphasize societal benefits and “the public good”
- Transparency and oversight. Be vigilant about, *e.g.*:
  - Conflicts of interest
  - Funders’ motivations
  - Regulatory capture
- Open design
  - Don’t settle prematurely on a particular architecture.

Some Open Questions

- Do current legal and regulatory frameworks support this vision? If not, how should they be changed, and what are the mechanisms for change?
- Can we move from platform-dominated value in data to data co-ops and diverse forms of value? Opportunity for economic modeling of incentives and adoption
- How many data co-ops do we want, and how big should they be?
  - A user has an incentive to join a big data co-op that has the power to bargain with platforms.
  - He also has an incentive to join niche data co-ops that clearly address his interests and share his values.
  - How many data co-ops would one person actually benefit from?
- How can we hold data co-ops accountable to their stated policies? Opportunity for research in attestation, verification, and computational proof systems

This Bears Repeating.

Get involved!

Ligett and Nissim want to:

- Build a research community
- Hear from interested researchers
- Learn about relevant projects

Conclusion

~~Conclusion~~ Exhortation

- ACM's endorsement of "Computer Science and Law" is a great opportunity.
- Advantage: "Hybrid researchers" (theory and practice)
- Advantage: Europeans
- Advantage: Liberal arts universities, especially those with prominent Law schools

- Please consider attending 2019 ACM Symposium on Computer Science and Law: http://computersciencelaw.org/

References (1)

[AA+15] H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, R. Rivest, J. Schiller, B. Schneier, M. Specter, and D. Weitzner. "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity* **1:1** (2015), pp. 69-79.

[BB+18] S. Bellovin, M. Blaze, D. Boneh, S. Landua, and R. Rivest. "Op-ed: Ray Ozzie's crypto proposal—a dose of technical reality," *ars technica.* **https://arstechnica.com/information-technology/2018/05/op-ed-ray-ozzies-crypto-proposal-a-dose-of-technical-reality/**, May 7, 2018.

[FF17] J. Feigenbaum and B. Ford, "Multiple Objectives of Lawful-Surveillance Protocols," in *Proceedings of the 2017 International Workshop on Security Protocols* (Cambridge SPW).

[FP+18] J. Frankle, S. Park, D. Shaar, D. Weitzner, and S. Goldwasser, "Practical Accountability of Secret Processes," in *Proceedings of the 2018 USENIX Security Symposium*.

References (2)

[FW18] J. Feigenbaum and D. Weitzner, “On the incommensurability of law and technical mechanisms: Or, what cryptography can’t do,” in *Proceedings of the 2018 International Workshop on Security Protocols* (Cambridge SPW), **http://www.cs.yale.edu/homes/jf/FW-SPW2018.pdf**

[HW16] S. Hennessey and B. Wittes. “Apple is selling you a phone, not civil liberties,” Lawfare. **https://lawfareblog.com/apple-selling-you-phone-not-civil-liberties**, Feb. 18, 2016.

[K14] S. Kamara, “Restructuring the NSA Metadata Program,” in *Proceedings of the 2014 Workshop on Applied Homomorphic Cryptography*.

[KR+16] M. Kearns, A. Roth, Z. S. Wu, and G. Yaroslavtsev, “Private algorithms for the protected in social network search,” *Proceedings of the National Academy of Sciences* **113(4)**, 913–918 (2016).

[KF+14] J. A. Kroll, E. W. Felten, and D. Boneh, “Secure protocols for accountable warrant execution.” **http://www.cs.princeton.edu/~felten/warrant-paper.pdf** (2014)

References (3)

[NA+18] National Academies of Sciences, Engineering, and Medicine. 2018. **Decrypting the Encryption Debate: A Framework for Decision Makers.** Washington, DC: The National Academies Press. **https://doi.org/10.17266/25010**

[SF+16] A. Segal, J. Feigenbaum, and B. Ford, "Open, privacy-preserving protocols for lawful surveillance," **https://arxiv.org/abs/1607.03659**.

[WV18] C. Wright and M. Varia, "Crypto Crumple Zones: Enabling Limited Access without Mass Surveillance," in *Proceedings of the 3rd IEEE European Symposium on Security and Privacy*, IEEE Computer Society, 2018.

[ZO+16] J. Zittrain, M. Olsen, D. O'Brien, and B. Schneier. 2016. "Don't Panic: Making Progress on the `Going Dark' Debate." Berkman Center Research Publication 2016-1. **http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552576**