ACM’s New Effort in Computer Science and Law

Joan Feigenbaum
Three Decades of DIMACS
New Brunswick, Nov. 21, 2019
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.

How to Regulate (and Not Regulate) Social Media

What Cryptography Can Bring to Law

When Code Isn’t Law
What is “Computer Science and Law”?

• Formulating and solving problems that are simultaneously computational problems and legal problems

• Examples:
  - Security, privacy, encryption, and surveillance
  - Cyber espionage, cyber war, and cyber diplomacy
  - Cyber crime, cyber law enforcement, and digital forensics
  - Freedom of expression online (or the lack thereof)
  - Online market structure, platform monopolies, and antitrust law
  - Online government services
  - Digital intellectual property
  - Automation of legal reasoning and legal services
  - Fairness, accountability, transparency, etc. (FAT*) in machine learning and data mining
What is “Computer Science and Law”?

• Formulating and solving problems that are simultaneously computational problems and legal problems

• Examples:
  - Security, privacy, encryption, and surveillance
  - Cyber espionage, cyber war, and cyber diplomacy
  - Cyber crime, cyber law enforcement, and digital forensics
  - Freedom of expression online (or the lack thereof)
  - Online market structure, platform monopolies, and antitrust law
  - Online government services
  - Digital intellectual property
  - Automation of legal reasoning and legal services
  - Fairness, accountability, transparency, etc. (FAT*) in machine learning and data mining
Ubiquitous Encryption vs. Lawful Surveillance

• 1990’s “Crypto War”
  - 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 LE access to locked devices – with a duly authorized warrant but without users’ passcodes.
  - Vendors object, saying that LEA would hurt customers’ security and privacy.

• (Perfect) example: FBI vs. Apple
Brief Summary of the Case (1)

- Terrorists Syed Rizwan Farook and Tashfeen Malik shot up the San Bernardino, CA health-dept building where they worked, killing 14 and injuring 22.

- The FBI took possession of an iPhone that the health dept 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.
• 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

• The legal question remains 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.
Competing Rights and Fears

• We have a right to privacy.
• Our governments routinely violate that right.
• The only effective grass-roots response to mass surveillance is mass encryption.

• Monopoly tech platforms have too much power.
• As “surveillance intermediaries,” they amass private data and decide whether law enforcement can access them.
• Citizens and their elected government should make those decisions.
Three Approaches to LE Access

• **Secure-systems community: Try to build it.**
  - Ozzie, Savage, and others: Protocols to unlock a device given an authenticated warrant and a manufacturer’s key
  - Wright and Varia: Protocols that use reduced-entropy key spaces discoverable in “crypto crumple zones”

• **Crypto-research community: Fight it tooth and nail.**
  - Claim 1: It can’t be done securely and cost-effectively.
  - Claim 2: It isn’t needed: The sought-after information is often available in plaintext form (e.g., in a social-media account); if all else fails, vulnerability-based, gray-hat hacking will always work.

• **JF: Use the crypto toolkit, and don’t be hypocritical.**
  - Claim 1: Prove it!
  - Claim 2: Since when do we praise ubiquitous plaintext and buggy software?
Freedom of Expression vs. Freedom from Harm

Section 230 of the Communications Decency Act (1996):

(1) No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) No provider or user of an interactive computer service shall be held liable on account of

   (a) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

   (b) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).
Treat Social Media Platforms as Publishers? (i.e., throw out (1) in Section 230?)

Three approaches to “content moderation” at scale*:

- Editorial review: Modeled on traditional broadcasting and publishing, but might be automated to some extent.

- Community flagging: Having transferred content creation from employees to users, do the same for content moderation.

- Automated detection: Use technology to lessen the severity of some problems inherent in “community” flagging.

*Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, 2018
First Two Approaches Don’t “Scale” Adequately

• “Given the scale that Twitter is at, a one-in-a-million chance happens 500 times a day. ... Say 99.999 percent of tweets pose no risk to anyone. There’s no threat involved. . . . After you take out that 99.999 percent, that tiny percentage of tweets remaining works out to roughly 150,000 per month.” (Del Harvey, vice president of Trust and Safety, Twitter, 2014)

• Facebook’s task is two orders of magnitude larger: It receives millions of community flags to review each day.
Mandate a 1\textsuperscript{st} Amendment for Social-Media Platforms? 
(i.e., throw out (2) in Section 230?)

Jack Balkin at the inaugural ACM Symposium on CS and Law:

\begin{itemize}
  \item \textbf{This is exactly what we should not do!} The 1\textsuperscript{st} Amendment, like the rest of the Bill of Rights, restricts \textit{government} power. Corporations aren’t analogous to governments, \textit{and we don’t want them to be}.
  
  \item We want a broad range of social-media platforms, with varying content-moderation policies and a robust culture of professional responsibility. Together, they would constitute a \textit{digital public square}.
\end{itemize}
“CS and Law” Research on Content Moderation

Combine (the best of) human and automated moderation:

• Explore and formalize “content-moderation policies.”
  ❑ Exactly what are “community flaggers” supposed to flag?
  ❑ Is there an (approximately) equivalent policy in which much but not all of this flagging can be automated?

• Use distributed algorithms, e.g., collaborative-filtering schemes, to aggregate and act on large numbers of (human-generated) flags?
Interdisciplinarity: “And = ∩” Will Be Hard!

Computer Science

• Papers are about results.
• Values breakthroughs
• Outdated technology usually dies.
• Powerful, new technologies will have unforeseen uses.
• Often tries to ignore “political reality”

Law

• Papers are about persuasion.
• Values intellectual continuity
• Outdated laws often live forever.
• Regulation can be based on “what are you going to use it for”?
• Sometimes tries to ignore technical reality
Examples in which “And = ∩” Has Been Hard

• US copyright law
  ❏ Fundamentally at odds with digital distribution
  ❏ This has been obvious for about 25 years.
  ❏ Copyright industries fight change tooth and nail (of course).
    😞 Legal scholars have suggested tweaks, not clean-slate redesign.

• Ubiquitous encryption vs. lawful surveillance
  😞 LE community “demands” technically sound access to locked devices:
    “Nerd harder.”
  😞 Crypto-research community says “this is just the key-escrow fight, which
    we have already won.”
Opportunity for DIMACS

• Special focus on Computer Science and Law
• Let’s form a WG on CS+Law and run a workshop in 2020.
• NSF Program Solicitation 19-612: Law and Science
• “The Law & Science Program considers proposals that address social scientific studies of law and law-like systems of rules, as well as studies of how science and technology are applied in legal contexts. The Program is inherently interdisciplinary and multi-methodological.”