Computers, Society, and the Law

Steven M. Bellovin
Department of Computer Science, Columbia University
https://www.cs.columbia.edu/~smb
The Space Shuttle Challenger

- NASA wanted to launch the shuttle on a cold January day
- The crucial O-rings had never been tested at low temperatures, but some Thiokol engineers suspected a problem
  - Roger Boisjoly had warned of it six months earlier
- Allan McDonald, director of the solid rocket program at Thiokol, opposed the launch
- NASA: “My God, Thiokol, when do you want me to launch, next April?”

*Engineers often know things that managers don’t know but need to*
Some Cases are Easy

- Volkswagen and the “defeat device” software to fool emissions tests
- Prenda Law and its bogus copyright infringement lawsuits
  - A judge hearing one case referred the matter to the FBI...
- Viruses, ransomware, and the like
Voting Machines

- There’s long been interest in computerized (“DRE”—Direct Recording Electronic) voting machines and Internet voting.

- Virtually all computer scientists oppose the idea: “Don’t use our technology!”

- But: “We bank online; why can’t we vote that way?”
Computer Scientists and Voting Systems

- We know how buggy and insecure software can be
- We know that ATMs, etc., can have log files and (in some cases) we can “unwind” problematic transactions
- But—anonymity and result integrity are extremely important in voting
- (Rerunning elections is problematic. If last year’s election were rerun a week later because of computer problems, what would the results have looked like?)

How do we communicate the software issues to legislators?
Encryption

- The FBI claims that they’re “going dark” because of increasing use of encryption

- They want some sort of “exceptional access” to let them get at the plaintext

- Most cryptologists think that this is dangerous, that cryptographic protocols and mechanisms are far too hard to get right

- Why?
Historical Example: The World War II Enigma Machine

Photo: public domain
Historical Example:
The World War II Enigma Machine

You select the proper rotors

Photo: public domain
Historical Example: The World War II Enigma Machine

Adjust the rotors to their “ground setting”
Historical Example: The World War II Enigma Machine

Set the plugboard

Photo: Bob Lord, via WikiMedia Commons
Historical Example: The World War II Enigma Machine

• Pick three random letters and encrypt them twice, and send those six letters as the start of the encrypted message
• Reset the rotors to those three letters

Photo: Paul Hudson, via Flickr
What Could Go Wrong?

- Sending the same, simple message every day was a fatal flaw
- Picking non-random letters was a fatal flaw
- Sending a message consisting of nothing but the letter “L” was a fatal flaw
- Encrypting the three letters twice was a fatal flaw
The Three Letters

• Imagine that “XJM” was encrypted to “AMRDTJ”

• The cryptanalysts realized that A and D represented the same letter, M and T were the same, and R and J were the same

• This gave away valuable clues to the rotor wiring and the rotor order!

Cryptography is hard...
Legal Issues

- Sometimes, there are legal issues involving computer technology
  - Today, almost everything involves computer technology...

- Most legislators and judges know nothing of computers

- How can they reach the right answer?

- We may know the answers—but we have to learn to speak *their* language: the law
Example: Wiretap Law and the Internet

- Under US law, phone and email conversations are strongly protected—police need a search warrant based on “probable cause” to obtain them.

- However, information that is voluntarily given to a “third party” is only weakly protected; it can be obtained if it is “likely to be relevant” to an ongoing criminal investigation.

- Phone numbers are third-party data, obtained by a “pen register” or “trap-and-trace device”.

- What about email addresses?
Sending Email

Outbound Mail Server

ISP

ISPs

Inbound Mail Server

ISP
Email (Simplified)

- Mail goes from a sender’s device to an “outbound mail server”
- From there, it is sent to the recipient’s “inbound mail server”
- The recipient downloads it from that machine
- The mail servers are generally ISP- or enterprise-operated
Sending Myself Email

220 machshav.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03 +0000
HELO eloi.cs.columbia.edu
MAIL FROM:<smb@eloi.cs.columbia.edu>
250 OK
RCPT TO:<smb@machshav.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: Barack Obama <president@whitehouse.gov>
To: <smb2132@columbia.edu>
Subject: Test
This is a test
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 machshav.com closing connection
Conversation With A Third Party

220 machshav.com ESMTP Exim 4.82 Tue, 11 Mar 2014 19:43:03 +0000
HELO eloi.cs.columbia.edu
MAIL FROM:<smb@eloi.cs.columbia.edu>
250 OK
RCPT TO:<smb@machshav.com>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
.
250 OK id=1WNSaS-0001z5-1d
QUIT
221 machshav.com closing connection
What the Recipient Sees

From: Barack Obama <president@whitehouse.gov>
To: <smb2132@columbia.edu>
Subject: Test

This is a test
Courts Have Gotten This Wrong

‘That portion of the “header” which contains the information placed in the header which reveals the e-mail addresses of the persons to whom the e-mail is sent, from whom the e-mail is sent and the e-mail address(es) of any person(s) “cc’d” on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device.’

(In re Application of United States, 396 F. Supp. 2d 45)

- But the “header” isn’t third-party data; it’s content, which cannot be obtained with a pen/trap order

- If you think that’s hard to explain to a judge, what about TCP port numbers?

Paper: http://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf
The Internet: A Layered Architecture
Is a Search Warrant Needed to Track Someone’s Location via their Cell Phone?

- Law enforcement: “No, you’re in public, and you’ve given your location to the phone company”

- But—the Fourth Amendment bars “unreasonable” searches

- Legal academics: if you track someone for too long, you can build up a very full picture of their life, which is unreasonable (called “mosaic theory”)

- Rejoinder: How long is “too long”? How will police know when they need a warrant?
Can Big Data Provide an Answer?

- Use machine learning to make predictions based on location data
- When predictions are accurate enough, a mosaic exists
- In other words, use computer science to answer the question
The technical literature supports the basic premise: with enough points, the whole is greater than the sum of its parts.

Note the jump in accuracy at 5 weeks and 28 weeks.

(Graph from Altshuler et al.)
One Week is the limit

- Experiments show that week-to-week movements are very predictable (Sadilek & Krumm)
- Weekend movements are *more* predictable, though of course different than weekday movement
- With seven days of observation, you have a very good picture of someone’s life
Where Are We?

- From a technical perspective, mosaic theory is correct: you really can build a very full picture of someone with enough data points.
- The limit should be about one week.
- But—movements are still in public.
- But—there are other legal issues that might arise in specific cases, such as the third party doctrine.
Results

- The science alone isn’t enough

- Fundamentally, this is a legal question, not a technical one. We can supply facts but the courts determine the law. Getting the right answer requires both kinds of input, legal and technical.

What Do We Do?

- First and foremost: *decide* to be involved
  - Be aware of societal issues
  - Make ethical choices about career paths and on-the-job behavior
- Learn the language of law and policy
  - You don’t have to be a lawyer—I’m not—but you do need to understand how to talk to policymakers
- Get involved—spend time in Trenton or Washington
- If you don’t speak, they can’t listen, even if they want to