Cryptography, law, ethics

Eerke Boiten, Nov 2014 update
Why talk about this?

- Important and frequently badly understood area in CS/maths
- Need to have awareness: lots of relevant law
- Ethics, maybe
- Professional: big risk area
- Crypto wars may be back on
Why cryptography?

- Cryptographic technologies, which have been essential to the success of e-commerce and online businesses, have various uses:
  - **Authentication** – guaranteeing that the originator or recipient of data is the person they claim to be;
  - **Availability** – assurance that the systems responsible for delivering, storing and processing data are accessible when needed, by those who need them;
  - **Confidentiality** – protecting data to ensure that its contents cannot be read by anyone other than an intended recipient;
  - **Integrity** – guaranteeing that data has not been accidentally or deliberately corrupted;
  - **Non-repudiation** – preventing the denial of previous commitments or actions;

- “If you haven’t done anything wrong, you have nothing to hide.” [Dr Bob Keim, CO643 lecture, 2009]
1. with the exception of the quote at the bottom, of course
I would describe my knowledge of the RIP Act 2000 as ...

1. Confident legal
2. Good awareness
3. Some idea
4. Requiescat In Pace
Cryptographic encryption in the UK

1. Is illegal
2. Is legal as long as you give keys to the government
3. Is legal as long as it’s not too strong
4. Is legal, but be prepared to hand in keys on government request
5. Is legal, no constraints
And it goes on to say ...

- Primarily it is application of cryptography to the confidentiality of data which is exploited by terrorists and criminals to protect their data, whether it is stored data, on a disk or other storage device, or data being communicated from one to another or from one to many others.

- The measures in Part III are intended to ensure that the ability of public authorities to protect the public and the effectiveness of their other statutory powers are not undermined by the use of technologies to protect electronic information.
So what is RIPA?

• Regulation of Investigatory Powers Act 2000
• Government can demand that a public telecoms service (incl ISP) intercepts an individual’s communications ...
• Without telling anyone ...
• Warrant can be granted for
  – National security
  – Serious crime prevention/detection
  – Economic well-being of the UK (!)
RIP Act continued

• Various government agencies have powers too
• Mass electronic surveillance possible too
• Technology: ISPs may have to install “black boxes” to monitor (US: Carnivore), government may contribute to cost (“as much as needed”)
• Whose black boxes, ideally & potentially!?
• Not admissible in court ... so ...
• http://www.magnacartaplus.org/bills/rip/
Recent changes

• DRIP: July 2014
• Firmed up a few things, in particular foreign companies operating in UK can be given warrants to hand over data
• Presented as “no additional powers” but
• Rushed through parliament at start of summer
RIP Part III: “Investigation of Protected Electronic Information”

- May be forced to hand over encryption key (or else 2 years in prison)
- Secrecy may be imposed (or else 5 years!)
- May need to prove you lost key
- Issues: self-incrimination argument rejected, reverse burden of proof denied.
Cryptography: short unserious history

• It’s really old, long before computers (Spartan *scytale*, Caesar shift cypher)
• Mary, Queen of Scots, allegedly paid with her life for trusting in it
• Save Bletchley Park! (More seriously, the need to deal with it probably had a big impact on the development of CS and computers in UK, and elsewhere)
• Modern computers make strong cryptography accessible to everyone, not just ...
• (The power of the one-time pad.)
Some landmark oddities

• 1981 US: suggestion all manuscripts on cryptography to be cleared by National Security Agency
• 1994: The Dutch try to outlaw cryptography
• 1995 Dan Bernstein vs US: free speech vs export controls. “Can put it on the internet as long as it doesn’t go abroad”
• 1997 “Teaching cryptography in universities violates export controls if overseas students”
• 1998 Dan Brown publishes “Digital Fortress”
• 2014 FBI; Cameron “prepared to legislate” against methods of communication that resist surveillance
But seriously ...

- Cryptography classified as “dual-use” good: can be used for military and civil purposes
- As a consequence, is subject to export restrictions (Wassenaar)
- Many exemptions: public domain, over the counter, short keys, signatures, ...
- Some countries also import restrictions
- See Bert-Jaap Koops’ maps
- Key recovery, key escrow
The ethics of strong cryptography

• Governments need it for law enforcement and security
• Individuals need it to protect privacy (avoiding the “panopticon”), and for many other apps
• Terrorists and criminals and spies use it, but governments need to negate this
• Some compromises since 90s, but fundamental divide remains
• (“Digital watermarking is as evil as arms trade”)
Resources: crypto legal and ethics

- Cryptography, data retention and the panopticon society by Blanchette & Johnson
- Wassenaar list of export control goods
- Crypto Law Survey by Bert-Jaap Koops
- The Crypto Controversy by Bert-Jaap Koops
- RIPA Section 71 Code of Practice
- RIPA
- Godzilla crypto tutorial (esp part 9, P. Guttman, bit old and feisty)
Using cryptography: the professional angle

- Relying on P≠NP is *not* unprofessional
- It’s just very complicated, in particular:
  - textbook descriptions (e.g. RSA) oversimplified, leaving security holes
  - accounting for the right attacks, no overkill and risks of weakest links

See Wenbo Mao: “Modern Cryptography” (Prentice Hall 2003)

So don’t reinvent it, take expert advice and apply it.
Choose the statement that best describes your attitude re: privacy vs RIPA and constraints on crypto

1. Paranoid (and that doesn’t mean ...)
2. Dubious erosion of civil liberties
3. Compromise is possible
4. Ineffective legislation
5. If you haven’t done anything wrong, you have nothing to hide