Lecture 24: Ethical, moral, and policy dimensions to cryptography

Boaz Barak

This will not be a lecture but rather a discussion on some of the questions that arise from cryptography. I would like you to read some of the sources below (and maybe others) and reflect on the following questions:

The discussion is often framed as weighing privacy against security, but I encourage you to look critically at both issues. It is often instructive to try to compare the current situation with both the historical past as well as some ideal desired world. It is also worthwhile to consider cryptography in the broader contexts. Some people on both the pro regulation and anti regulation camps exeggarate the role of cryptography.
On one hand, cryptography is likely not to bring about the "crypto anarchy" regime hoped for in the crypto anarchist manifesto. For example, more than the growth of bitcoin, we are seeing a turn away from cash into credit cards and other forms of much more traceable and *less* anonymous forms of payments (interestingly, these forms of payments are often enabled by cryptography). On the other hand, despite the fears raised by government agencies of "going dark" there are powerful commercial incentives to collect vast amounts of data and store them at search-warrant friendly servers. Clearly technology is shifting the landscape of relationships among individuals, as well as between individuals and large organizations and governments. Cryptography is an important component in these technologies but not the only one, and more than that, the ways technologies end up *used* often has more to do with social and commercial factors than with the technologies themselves.

All that said, significant changes often pose non trivial dangers, and it is important to have an informed and reasoned discussion of the ways cryptography can help or harm the general and private good.

Some questions that are worth considering are:

- Is communicating privately a basic human right? Should it extend to communicating at a distance? Should this be absolute privacy that cannot be violated even with a legal warrant? If there was a secure way to implement wiretapping only with a legal warrant, would it be morally just?
- Is privacy a basic good in its own right? Or a necessary condition for the

freedom of expression, and peaceful assembly and association?

- Are we less or more secure today than in the past? In what ways did the balance between government and individuals shift in the last few decades? Do governments have more or less data and tools for monitoring individuals at their disposal? Do individuals and non-governmental groups have more or less ability to inflict harm (and hence need to be protected against)?
- Do we have more or less privacy today than in the past? Do cryptography regulation play a big part in that?
- What would be the balance between security and privacy in an ideal world?
- Is the focus on encryption misguided in that the main issue affecting privacy and security is the so called *meta data*? Can cryptographic techniques protect such meta data? Even if they could, is there a commercial interest in doing so?
- One argument against the regulation of cryptography is that, given the mathematics of cryptography is not secret, the "bad guys" will always be able to access it. Is this a valid argument? Note that similar arguments are made in the context of gun control. Also, perhaps the "true dissidents" will also be able to access cryptography as well and so regulation will effect the masses or "run of the mill" private good and not-so-good citizens?
- What would be the practical impact of regulations forbidding the use of end-to-end crypto without access by governments?
- Rogaway argues that cryptography is inherently political, and research should acknowledge this and be directed at achieving beneficial political goals. Has cryptography research failed the public? What more could be done?
- Are some cryptographic (or crypto related) tools inherently morally problematic? Rogaway suggests that this may be true for fully homomorphic encryption and differential privacy- do you agree?
- What are the most significant scenarios where cryptography can impact positively or negatively? Large scale terror attacks? "Ordinary" crimes (that still claim the lives of many more people than terror attacks)? Attacks against cyber infrastructure or personal data? Political dissidents in opressive regimes? Mass government or corporate surveilance?
- How are these issues different in the U.S. as opposed to other countries? Is the debate too U.S. centric?

Reading prior to lecture:

- Moral Character of Cryptographic Work - please read at least parts 1-3 (pages 1-30 in the footnoted version) - it's long and should not be taken

uncritically, but is a very good and thought provoking read.
- "Going Dark" Berkman report - this is a report written by a committee, and as such not as exciting (though arguably more sober) than Rogaway's paper. Please read at least the introduction and you might also find the personal statements in Appendix A interesting.
- Digital Equilibrium project - optional reading - this is a group of very senior current and former officials, in particular in government, and as such would tend to fall on the more "establishment" or "pro regulation" side. Their "foundational paper" has even more of a "written by committee" feel but is still worthwhile reading.
- Crypto anarchist manifesto - optional reading - very much not "written by committee" can be an interesting read even if it sounds more like science fiction than describing actual current or near future reality.

Case studies.

Since such a discussion might be sometimes hard to hold in the abstract, let us consider some actual cases:

The Snowden revelations

The impetus for the current iteration of the security vs privacy debate were the Snowden revelations on the massive scale of surveillance by the NSA on citizens in the U.S. and around the globe. Concurrently, in plain sight, companies such as Apple, Google, Facebook, and others are also collecting massive amounts of information on their users. Some of the backlash to the Snowden revelations was increased pressure on companies to support stronger "end-to-end" encryption such as some data does not reside on companies' servers, that have become suspect. We're now seeing some "backlash to the backlash" with law enforcement and government officials around the globe trying to ban such encryption technlogoy or mandate government backdoors.

FBI vs Apple case

We've mentioned this case in the past. (I also blogged about it.) The short summary is that an iPhone belonging to one of the San Bernardino terrorists was found by the FBI. The iPhone's memory was encrypted by a key k that is obtained as $H(uid \| passcode)$ where $passcode$ is the six digit passcode of the user and uid is a secret 128 bit key that is hardwired into the processor. The processor will only allow ten attempts at guessing the passcode before erasing all memory. The FBI wanted Apple's help in creating a digitally signed software update that essentially run a brute force search over the 10^6 passcodes and output the key k. The software update could be restricted to run only on that

particular iPhone. Eventually, the FBI managed to extract the information out of the iPhone without Apple's help. The method they used is unknown, but it may be possible to physically extract the *uid* from the processor. It might also be possible to prevent erasure of the memory by disconnecting it from the processor, or rewriting it after erasure. Would such cases change your position on this question?

Some questions that one could ask:

- Given that the FBI had a legal warrant for the information on the iPhone, was it wrong of Apple to refuse to provide the help required?
- Was it wrong for Apple to have designed their iPhone so that they are unable to easily extract information out of it? Should they be required to make sure that such devices can be searched as a result of a legal warrant?
- If the only way for the FBI to get the information was to get Apple's master signature key (that allows to completely break into any iPhone, and even turn it into a recording/surveillance device), would it have been OK for them to do it? Should Apple design their device in a way that even their master signature key cannot break them? Is that even possible, given that software updates are crucial for proper functioning of such devices? (It was recently claimed that Canadian police has had access to the master decryption key of Blackberry since 2010.)

In the San Bernardino case, the utility of breaking into the phone was questioned, given that both perpetrators were killed and there was no evidence of them receiving any assistance. But there are cases where things are more complicated. Brittney Mills was 29 years old and 8 months pregnant when she was shot and killed in April 2015 in Baton Rouge, Louisiana. Her baby was delivered via emergency C section but also died a week later. There was no sign of forced entry and so it is quite likely she knew her assailant. Her family believes that the clues to her murderer's identity could be found in her iPhone, but since it is locked they have no way of extracting this information. One can imagine other cases as well. Recently a mother found her kidnapped daughter using the Find my iPhone procedure. It is not hard to concieve of a case where unlocking a phone is the key to saving someone's life. Would such cases change your view of the above questions?

Juniper backdoor case and the OPM break-in

We've also mentioned the case of the Juniper backdoor case. This was a break in to the firewalls of Juniper networks by an unknown party that was crucially enabled by backdoor allegedly inserted by the NSA into the Dual EC pseudorandom generator. (see also here and here for more).

Because of the nature of this break in, whomever is responsible for it could have decrypted much of the traffic without leaving any traces, and so we don't know

the damage caused, but such hacks can have much more significant consequences than forcing people to change their credit card numbers. When the federal office of personell management was hacked sensitive information about millions of people who have gone through the security clearance was extracted. This includes fingerprints, extensive personal information from interviews and polygraph sessions, and much more. Such information can help then gain access to more information, whether it's using the fingerprint to unlock a phone or using the extensive knowledge of social connections, habits and interests to launch very targeted attacks to extract information from particular individuals.

Here one could ask if stronger cryptography, and in particular cryptographic tools that would have enabled an individual to control access to his or her own data, would have helped prevent such attacks.