Cryptography *vs.* Mass Surveillance

Phillip Rogaway
Department of Computer Science
University of California, Davis, USA

Talk for
Crypto vs. Mass Surveillance:
The Uneasy Relationship workshop
14 November 2016
Trondheim, Norway

With thanks to
Stig Mjølsnes and
Britta Hale for
inviting me and
arranging my visit!

Cryptography *vs.* Mass Surveillance

The title imagines the two **standing in opposition**.
Do they?

From a **descriptive** standpoint: **no**.

Crypto has **not** been effective at curtailing mass surveillance …
and **most** cryptographers do **not** see this as our role.

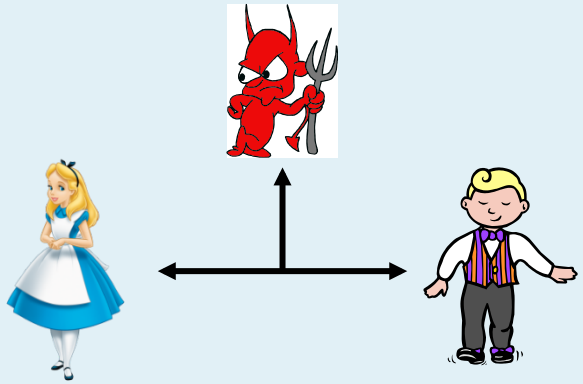
WHY hasn't crypto helped?

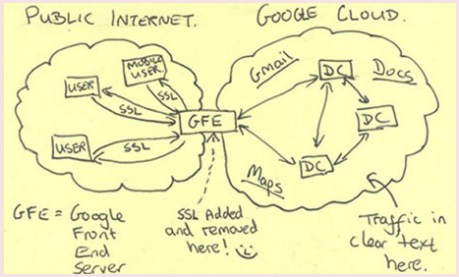
From a **normative** standpoint: **maybe**.

Many think cryptography **should** stand
in opposition to mass surveillance.
But not at all clear that it **could**.
Ought implies *can*.

CAN crypto help?

Cryptography – the science of **secure communications**.





Mass surveillance – the spectacular **failure** to secure communications.

You **would think**

- these would be in opposition, and that
- cryptographers would be **aghast** by mass surveillance revelations.

***You'd be wrong*.** Most of my community doesn't see a connection, and thinks things are going great.

A rosy assessment of CS

Computer science is marking an epical change in human history. We are conquering a new and vast scientific continent. …
Virtually all areas of human activity … [and]
virtually all areas all areas of human knowledge …
are benefitting from our conceptual and technical contributions. …
Long live computer science!

Cryptographer
Silvio Micali
Turing Award acceptance speech 15 June 2013

About a 1.5 weeks after the initial Snowden revelations (Verizon + PRISM)

Cryptographers don't care about mass surveillance

(work on)

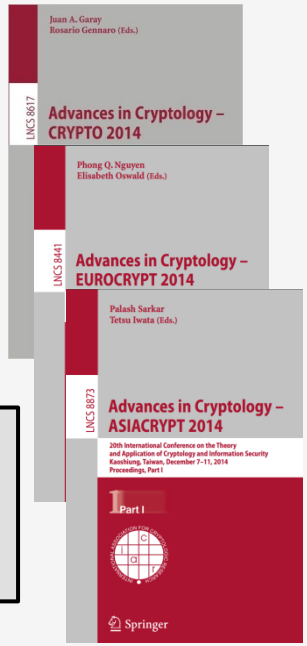
2011: 0 papers
2012: 0 papers

Before Snowden

2013 IACR-sponsored conferences

156 papers (3067 pages)

0 papers with the word "surveillance"



After Snowden

2014 IACR-sponsored conferences

155 papers (2910 pages)

1 paper with the word "surveillance" (mine)

2015: 1 paper
2016: 3 papers

The Summer of Snowden

2013

News › World news › NSA

Series: Glenn Greenwald on security and liberty

NSA collected US email records in bulk for more than two years under Obama

- Secret program launched by Bush continued 'until 2011'
- Fisa court renewed collection order every 90 days
- Current NSA programs still mine US internet metadata

Glenn Greenwald and Spencer Ackerman
The Guardian, Thursday 27 June 2013 11.20 EDT
Jump to comments (...)

News › World news › The NSA files

New NSA leaks show how US is bugging its European allies

Exclusive: Edward Snowden papers reveal 38 targets including EU, France and Italy

Berlin accuses Washington of cold war tactics

Follow Julian Borger by email BETA

Ewen MacAskill in Rio de Janeiro and Julian Borger
The Guardian, Sunday 30 June 2013 16.28 EDT

News › World news › US national security

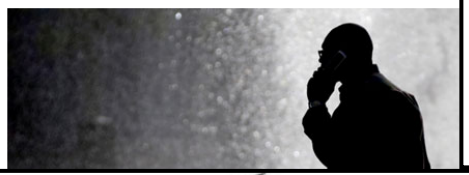
Series: Glenn Greenwald on security and liberty

NSA collecting phone records of millions of Verizon customers daily

Exclusive: Top secret court order requiring Verizon to hand ov
all call data shows scale of domestic surveillance under Obama

- Read the Verizon court order in full here
- Obama administration justifies surveillance

Glenn Greenwald
The Guardian, Wednesday 5 June 2013
Jump to comments (...)



News › World news › NSA

Series: Glenn Greenwald on security and liberty

Microsoft handed the NSA access to encrypted messages

- Secret files show scale of Silicon Valley co-operation on Prism
- Outlook.com encryption unlocked even before official launch
- Skype worked to enable Prism collection of video calls
- Company says it is legally compelled to comply

Follow Glenn Greenwald by email BETA

Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe
The Guardian, Thursday 11 July 2013
Jump to comments (4174)

NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'
The Guardian

theguardian

News | US | World | Sports | Comment | Culture | Business | Money

News › World news › The NSA files

Series: Glenn Greenwald on security and liberty

Revealed: how US and UK spy agencies ...et privacy and security

...lock encryption used to protect emails, ... records
...program works covertly with tech companies to ...to products
...y programs 'undermine the fabric of the ...

...uestions for our privacy experts

... and Glenn Greenwald
...y 5 September 2013

The Washington Post

FRIDAY, JUNE 7, 2013

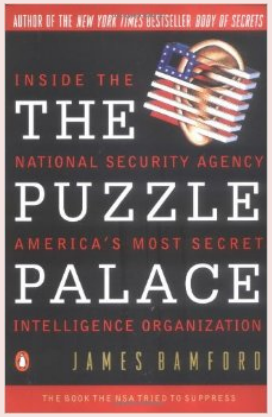
U.S. mines Internet firms' data, documents show

Google, Facebook, Apple, Yahoo deny giving NSA direct access to servers

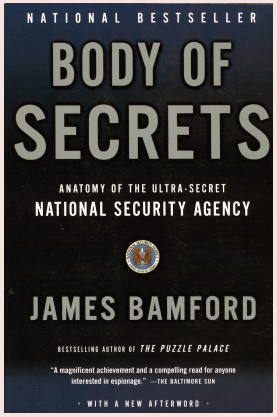
tion directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."

Agency knows much about public, but we know little about it

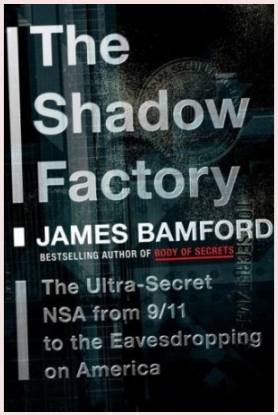
same information on millions of ordinary Americans.
Regarded as the most secretive of the nation's intelligence agencies, the NSA is part of the military



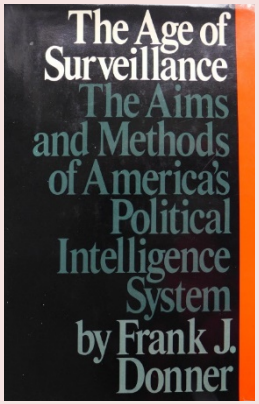
1983



2002



2009



1980

Clipper Chip 1993

Why wasn't I paying more attention to this earlier?

Thomas Drake

Bill Binney

Diane Roark

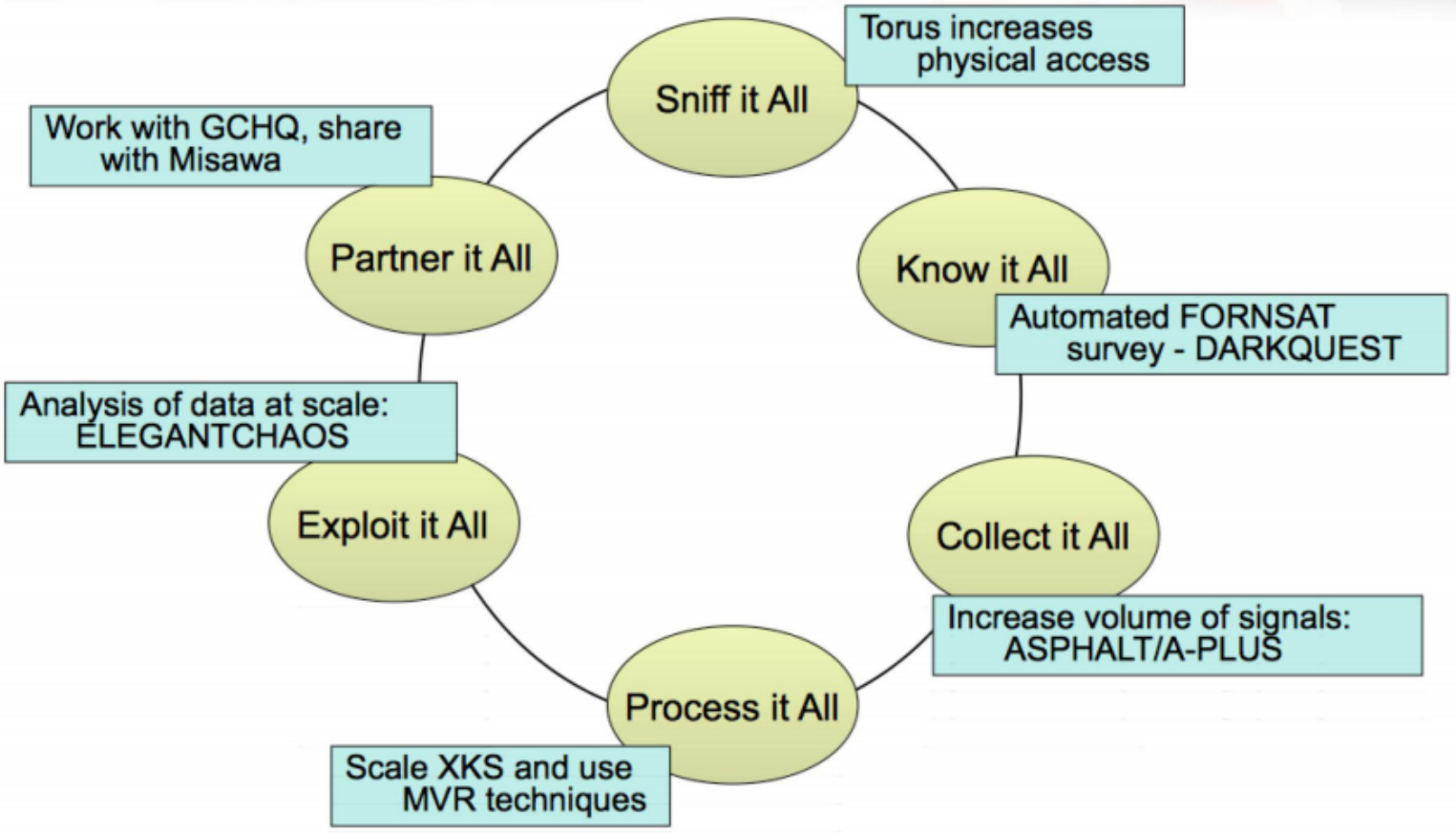
Mark Klein

Kirk Wiebe

2013/451 **Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits**
Sanjam Garg and Craig Gentry and Shai Halevi and Mariana Raykova and Amit Sahai and Brent Waters
2013/454 **How to Use Indistinguishability Obfuscation: Deniable Encryption, and More**
Amit Sahai and Brent Waters
2013/471 **Obfuscating Conjunctions**
Zvika Brakerski and Guy N. Rothblum
2013/500 **Obfuscating Branching Programs Using Black-Box Pseudo-Free Groups**
Ran Canetti and Vinod Vaikuntanathan
2013/509 **Replacing a Random Oracle: Full Domain Hash From Indistinguishability Obfuscation**
Susan Hohenberger and Amit Sahai and Brent Waters
2013/557 **Black-Box Obfuscation for d-CNFs**
Zvika Brakerski and Guy N. Rothblum
2013/563 **Virtual Black-Box Obfuscation for All Circuits via Generic Graded Encoding**
Zvika Brakerski and Guy N. Rothblum
2013/601 **Two-round secure MPC from Indistinguishability Obfuscation**
Sanjam Garg and Craig Gentry and Shai Halevi and Mariana Raykova
2013/631 **Protecting Obfuscation Against Algebraic Attacks**
Boaz Barak and Sanjam Garg and Yael Tauman Kalai and Omer Paneth and Amit Sahai
2013/641 **Indistinguishability Obfuscation vs. Auxiliary-Input Extractable Functions: One Must Fall**
Nir Bitansky and Ran Canetti and Omer Paneth and Alon Rosen
2013/642 **Multiparty Key Exchange, Efficient Traitor Tracing, and More from Indistinguishability Obfuscation**
Dan Boneh and Mark Zhandry
2013/643 **There is no Indistinguishability Obfuscation in Pessiland**
Tal Moran and Alon Rosen
2013/650 **On Extractability (a.k.a. Differing-Inputs) Obfuscation**
Elette Boyle and Kai-Min Chung and Rafael Pass
2013/665 **The Impossibility of Obfuscation with a Universal Simulator**
Henry Cohn and Shafi Goldwasser and Yael Tauman Kalai
2013/668 **Obfuscation for Evasive Functions**
Boaz Barak and Nir Bitansky and Ran Canetti and Yael Tauman Kalai and Omer Paneth and Amit Sahai

Cryptographers – too busy with iO to notice Snowden?

New Collection Posture



TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...

TS//SI//REL to USA, FVEY

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) …that this would be big brother...

TS//SI//REL to USA, FVEY

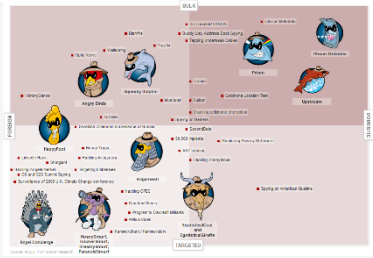
TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) ...and the zombies would be paying customers?

TS//SI//REL to USA, FVEY

No human understands what's going on



ACLU + ProPublica

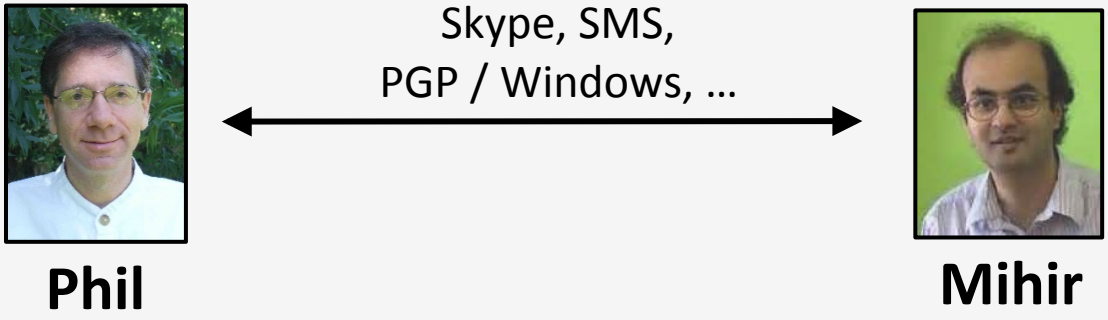
Honey Traps	A British spy effort to conduct covert Internet investigations, including sexual "honey-traps."	NSA
Surveillance of 2009 U.N. Climate Change conference	NSA surveillance of the 2009 U.N. Climate Change conference.	NSA
Spying on Gamers	The NSA and GCHQ monitored games including World of Warcraft.	NSA and GCHQ
Targeting Embassies	An NSA operation targeting the Italian embassy in Washington D.C.	NSA
Dishfire	An NSA program to collect up to 200 million text messages a day worldwide.	NSA
QuantumTheory	NSA programs that inject spyware onto targets' computers through so-called "man on the side" attacks. Variants include QuantumInsert, QuantumBiscuit, and QuantumSmackdown.	NSA
Muscular	The NSA and GCHQ have jointly operated a program to intercept data from Yahoo and Google networks.	NSA and GCHQ
Prism	The Prism program collects data from the servers of U.S. technology companies.	NSA
Hacking Angela Merkel	The NSA targeted German Chancellor Angela Merkel's cellphone.	NSA
Hacking Al Jazeera	NSA hacked into Al Jazeera's internal communications system.	NSA
Cellphone Location Test	In 2010 and 2011, the NSA tested bulk collection of location data from Americans cellphones.	NSA
Tapping Underseas Cables	Companies - including BT, Vodafone, and Verizon Business - gave GCHQ access to their underseas cables.	NSA
Angry Birds	NSA and GCHQ efforts to intercept information transmitted by phone apps, including Angry Birds.	NSA and GCHQ
Royal Concierge	A GCHQ program to monitor hotel reservations for "governmental hard targets."	NSA
Monitoring Privacy Software	The NSA collected information about users of privacy software including visitors to two Massachussetts Institute of Technology computers.	NSA
SecondDate	A so-called man-in-the-middle attack for "mass exploitation" of traffic "passing through network choke points" as well as "surgical target selection."	NSA
NoseySmurf, TrackerSmurf, DreamySmurf, ParanoidSmurf	The Smurf programs get inside iPhones and Android devices, turning on microphones, tracking location, and managing power.	NSA
Internet Metadata	A program, ended in 2011, to sweep up domestic Internet metadata such as the To and From fields in emails.	NSA
EgotisticalGoat and EgotisticalGiraffe	The Egotistical animal programs are techniques to track users of Tor anonymizing software.	NSA
Program to Discredit Militants	An NSA effort to spy on targets' online sexual activity.	NSA
LinkedIn Hack	Engineers at a Belgian telcom were infected with malware, via a technique called QuantumInsert, when they pulled up their LinkedIn profiles.	NSA
Bullrun	Joint NSA and GCHQ effort to undermine and weaken cryptography standards and tools.	NSA and GCHQ
Shotgiant	An NSA program to break into Chinese-owned Huawei networks and products.	NSA
WillowVixen	An NSA technique to deploy malware by sending out emails that trick targets into clicking a malicious link.	NSA
Turmoil	A large network of clandestine surveillance "sensors" to collect data from satellites, cables, and microwave communications around the world.	NSA
Turbine	A network of active command and control servers around the world that can be used for "industrial scale exploitation."	NSA
Squeaky Dolphin	A British effort to monitor YouTube video views, URLS "liked" on Facebook and Blogger visits.	NSA

VictoryDance	The NSA tested a technique for using drones to map "the Wi-Fi fingerprint of nearly every major town in Yemen."	NSA
Hammerchant / Hammerstein	NSA programs to spy on data sent through voice over IP calls and Virtual Private Networks.	NSA
ANT catalog	Various techniques - with names like IronChef and DropoutJeep - used to inject surveillance software into Apple, Cisco, Dell and other products.	NSA
Cracking cellphone encryption	The NSA has the capability to defeat a widely-used cellphone encryption technology.	NSA
Optic Nerve	A British program to bulk collect images from Yahoo webcam chats: "It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person."	NSA
Swedish-American surveillance of Russia	A Swedish-American effort to spy on Russian leadership.	NSA
Gilgamesh	An NSA program to geolocate people's SIM cards via Predator drones.	NSA
Buddy List, Address Book Spying	An NSA effort to collect hundreds of millions of contact lists from email and instant messaging accounts.	NSA
Hacking Anonymous	A British spy unit to monitor hacktivists such as the group Anonymous.	NSA
Co-Traveler/ FASCIA	The NSA collected 5 billion records a day of cellphone locations worldwide.	NSA
Hacking OPEC	NSA and GCHQ programs to infiltrate the OPEC oil cartel	NSA and GCHQ
Tracfin	Tracfin amasses gigabytes of data about credit card purchases.	NSA
Wellspring	An NSA program to collect images from emails for facial recognition.	NSA
Spying on American Muslims	FBI monitored e-mail of 200 Americans including prominent Muslims such as a former Bush Administration official, two professors, an attorney and the leader of a Muslim civil rights group.	NSA
Upstream	The Upstream program collects communications transiting the Internet via commercial partners codenamed Fairview, Stormbrew, Blarney, and Oakstar.	NSA
50,000 implants	An NSA map of the 50,000 computers worldwide it has implanted with surveillance malware.	NSA
G8 and G20 Summit Spying	The NSA conducted surveillance during the 2010 G8 and G20 summits in Canada.	NSA
Phone Metadata	The well-known and controversial program to collect phone call records - aka metadata - of nearly all Americans.	NSA
HappyFoot	An NSA effort to use Web cookies and data from phone apps to identify users' devices and physical locations.	NSA

FISAAA | PPD-20 | HSPD-23 | Freedom Act | CALEA

ECPA | Executive order 12333 | PATRIOT Act | FISA

The basics are not known



How many copies of the communications are archived, by whom, for how long?
What algorithms are applied– or will be applied – to the data?
What is the data combined with?
When might a human analyst become involved?
What consequences might stem from the communications content?

Secrecy + Complexity

- Reduces the possibility of effective reform.
- Is *itself* an exercise of tradecraft.

So cryptographers have been disinclined to work on mass surveillance, and don't see crypto as relevant.

But WHY ?

While there's no one answer,
there is one theme explaining the *disinclination* to help:

It's the culture, stupid.

A more specific answer. With a bit of an explanation.

From where did this disciplinary culture come?

MIT Lab for Computer Science
Theory of Computation Group
Cryptography – mid-1980's



Ron Rivest Shafi Goldwasser Silvio Micali

- **Youthful**
- **Iconic, paradigmatic works that captured the imagination**

[GM] Goldwasser, Micali – STOC 1982 (JCSS 84) Probabilistic encryption
and how to play mental poker keeping secret all partial information

[GMR] Goldwasser, Micali, Rivest – FOCS 84 (SIAM 88)
A "paradoxical" solution to the signature problem

[GMR] Goldwasser, Micali, Rackoff – STOC 85 (SIAM 89)
The knowledge complexity of interactive proof systems

[GMW1] Goldreich, Micali, Wigderson – FOCS 86 (JACM 91)
Proofs that yield nothing but their validity and a methodology of cryptographic protocol design

[GMW2] Goldreich, Micali, Wigderson – STOC 87
How to play any mental game or A completeness theorem for protocols with honest majority

- **A branch of theory**
- **Problem selection: aesthetics, philosophy**

Founding ethos. Crypto is theory, philosophy, and imagination.

Embedded ethos. This ethos remains dominant, continually renewed by technical and nontechnical choices.

What is cryptography?

Philosophically … Sociologically …

"The Science Wars" as projected onto my corner of the world

Scientific realism

C = modern cryptography

C is as it is because of the nature of reality
C is inevitable
C is objective, ahistorical, and politically neutral
C is but superficially shaped by the disciplinary culture
C is a science. We discover it.

cryptographic research is indeed part of science. This assertion is empirical and it refers to the current sociology of the discipline; that is, we believe that the vast majority of the members of this research community identify themselves as scientists …

On Post-Modern Cryptography, Oded Goldreich, 2006

What is cryptography?

Philosophically … Sociologically …

"The Science Wars" as projected onto my corner of the world

Social constructionism

C need not be as it is. It is not inevitable
C is not determined by the nature of things.
C looks like it does due to social and historical forces
C is shaped by the disciplinary culture
C is a technology. We invent it.

C = modern cryptography

the body of work our community has produced is less the inevitable consequence of what we aim to study than the contingent consequence of sensibilities and assumptions within our disciplinary culture… I would claim that cryptography, even in its most pure and scientific persona, is quite strongly constructed.

Practice-Oriented Provable-Security and the Social Construction of Cryptography, P. Rogaway, 2009

When most cryptographers are blue …

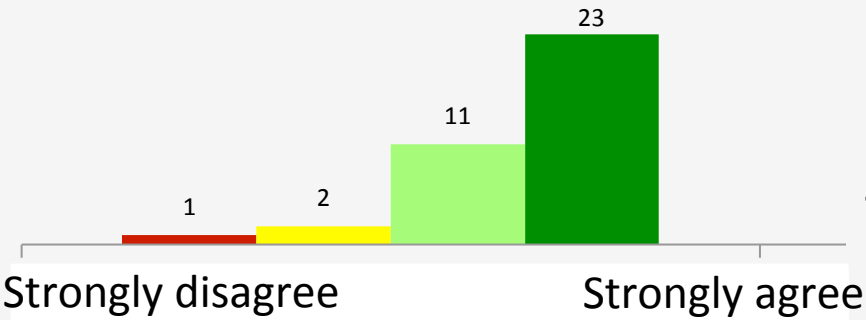
Here for fun. Intellectuality as sport — pragmatism as small-mindedness.

Irrelevance. Imagination-genesis work can't actually find a route to practice.

Distanced from security. Cryptographers don't see even prominent security problems because of community structure.

Standardization non-participation. Crypto standards without the cryptographers.

Value-neutral view. The myth that science and technology is value-neutral.



Beginning-of term survey data from my class ECS 188 "Ethics in an Age of Technology", W13

"Technology itself is value-neutral: it is what humans do with technology that is right or wrong."

Spawned Disjoint Communities

D. Chaum,
Untraceable electronic mail, return addresses, and digital pseudonyms
CACM 1981 (4368 citations)

→ Grew into the PETS community

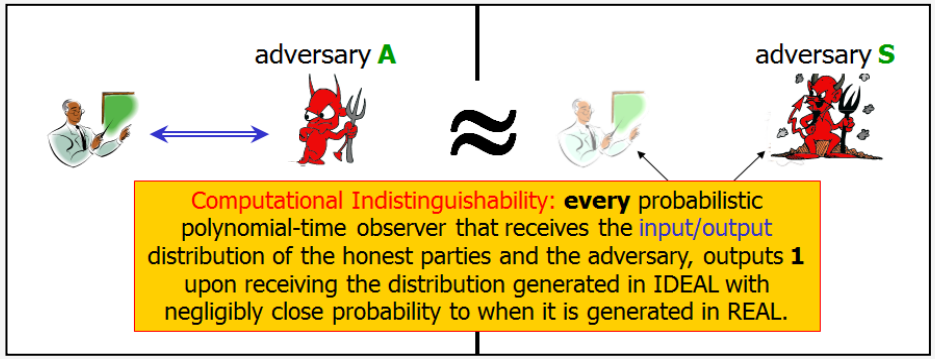
S. Goldwasser and S. Micali,
Probabilistic encryption
STOC82+JCSS 1984 (3733 citations)

→ Grew into the IACR community

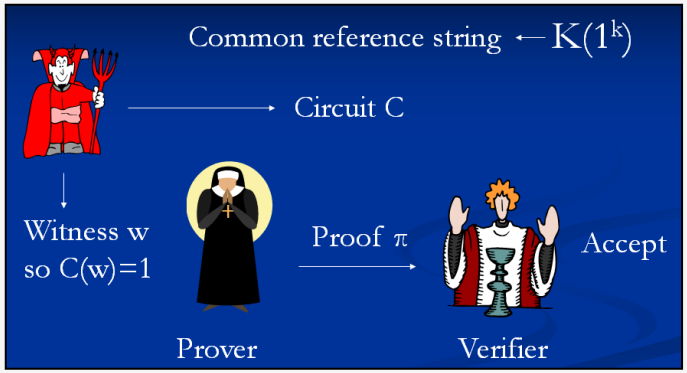
Community fracture. Splitting off of PETS, symbolic approaches to crypto, …

For most cryptographers …

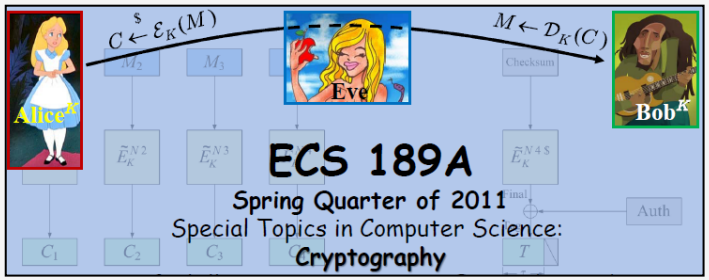
Adversaries are **notional**.
We **joke** about them.
We see crypto as a **game**.



Y. Lindell



J. Groth

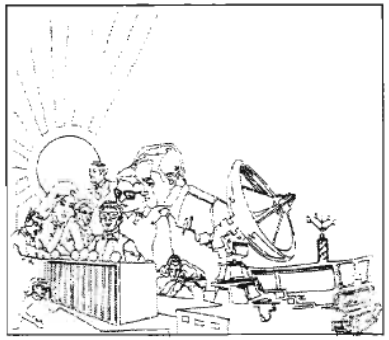


P. Rogaway

1

Adversarial abstraction. Treating the adversary notionally.

Our irrelevance hasn't been lost on power



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

NATIONAL SECURITY AGENCY

CRYPTOLOG

1st Issue 1994

EUROCRYPT '92 report:

(U) Three of the last four sessions were of no value whatever, and indeed there was almost nothing at Eurocrypt to interest us (*this is good news!*).

(U) There were no proposals of cryptosystems, no novel cryptanalysis of old designs, even very little on hardware design. *I really don't see how things could have been better for our purposes*.

(U) The conference again offered an interesting view into the thought processes of the world's leading "cryptologists." *It is indeed remarkable how far the Agency has strayed from the True Path.*

[*emphasis mine*]

Unthreateningly engaged. We're *happy* to do stuff irrelevant to power.

Why no reaction?

53 signatories 58% acceptance rate 4.5 months >900 emails

http://masssurveillance.info/

An Open Letter from US Researchers in Cryptography and Information Security
January 24, 2014

Media reports since last June have revealed that the US government conducts domestic and international surveillance on a massive scale, that it engages in deliberate and covert weakening of Internet security standards, and that it pressures US technology companies to deploy backdoors and other data-collection features. As leading members of the US cryptography and information-security research communities, we deplore these practices and urge that they be changed.

Indiscriminate collection, storage, and processing of unprecedented amounts of personal information chill free speech and invite many types of abuse, ranging from mission creep to identity theft. These are not hypothetical problems; they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-center links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities.

The value of society-wide surveillance in preventing terrorism is unclear, but the threat that such surveillance poses to privacy, democracy, and the US technology sector is readily apparent. Because transparency and public consent are at the core of our democracy, we call upon the US government to subject all mass-surveillance activities to public scrutiny and to resist the deployment of mass-surveillance programs in advance of sound technical and social controls. In finding a way forward, the five principles promulgated at http://reformgovernmentsurveillance.com/ provide a good starting point.

The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users. Every country, including our own, must give intelligence and law-enforcement authorities the means to pursue terrorists and criminals, but we can do so without fundamentally undermining the security that enables commerce, entertainment, personal communication, and other aspects of 21st-century life. We urge the US government to reject society-wide surveillance and the subversion of security technology, to adopt state-of-the-art, privacy-preserving technology, and to ensure that new policies, guided by enunciated principles, support human rights, trustworthy commerce, and technical innovation.

Top reasons stated for *not* signing:

- *Nothing I know is relevant*.
- *These are political issues; I am not an expert on public-policy; this is not our professional concern*.

If one's technical work isn't even relevant to security, how is it supposed to be relevant to a socio-technical problem like this?

Extreme specialization. Can rob scientists of any sense of agency.

No politics. An unwillingness to engage in anything "political" connected to ones work.

A big-data candidate we recently interviewed

Some of your work could have troubling applications. Could you describe your personal view on the social responsibilities of computer scientists?

I'm a body without a soul.

Dissociation. A belief that it is *reasonable* to dissociate ones ethical being from ones work.

Ralph Merkle – Martin Hellman -- Whit Diffie

Changing motivations

"I told her [my wife, circa 1976] that we were headed into a world where people would have important, intimate, long-term relationships with people they had never met face to face. I was worried about privacy in that world, and that's why I was working on cryptography."

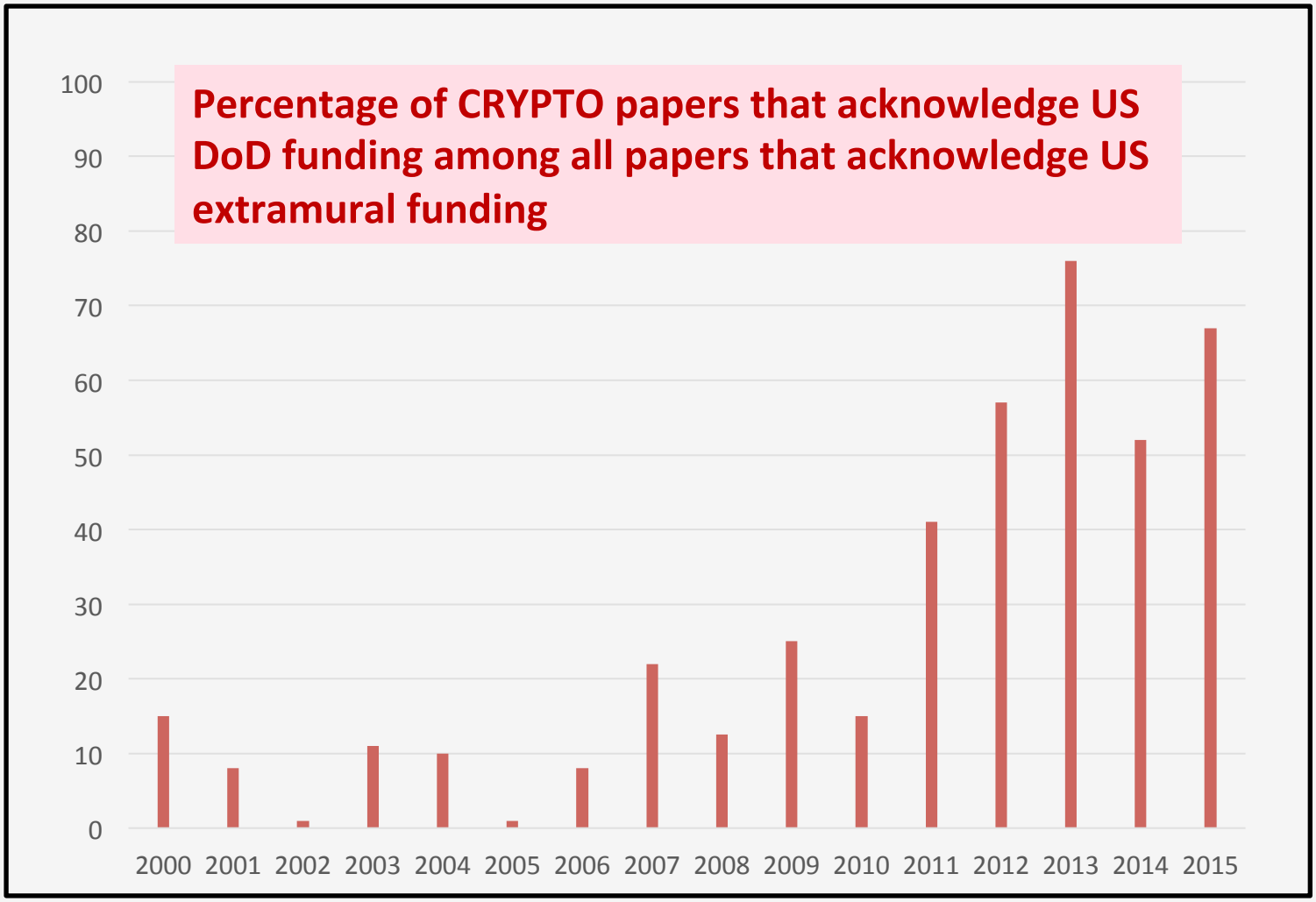
Whit Diffie, testifying at the Newegg vs. TQP patent trial, 21 November 2014

Changing motivations. Current-generation cryptographers aren't in it for moral or socio-political reasons.

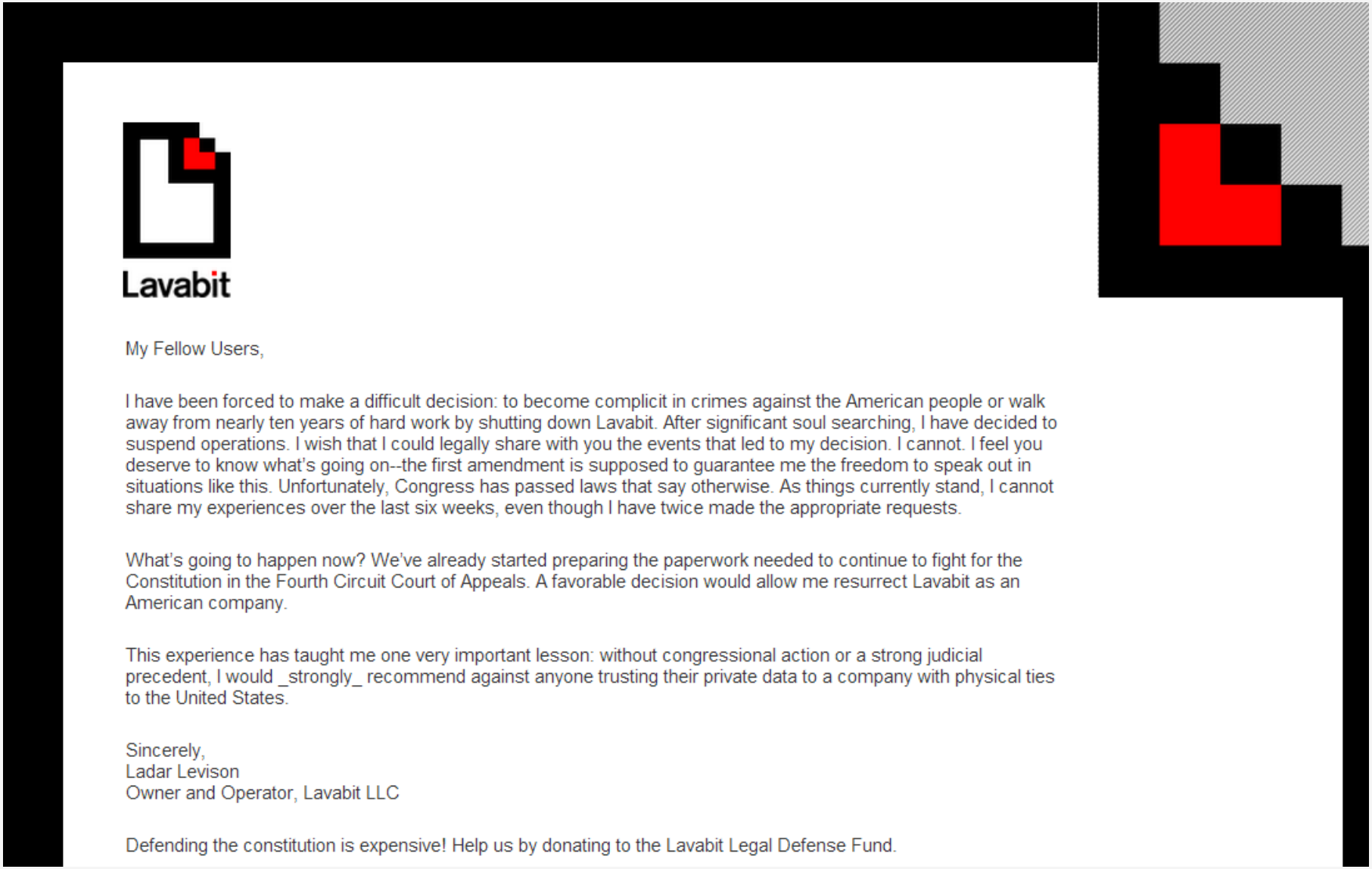
Careerism. What we do aligns with the academic reward system.

(Write **lots** of papers **appreciated enough** to get into tier-1 venues. Bring in plenty of **money**.)

DoD Funding in Cryptography, 2000-2015



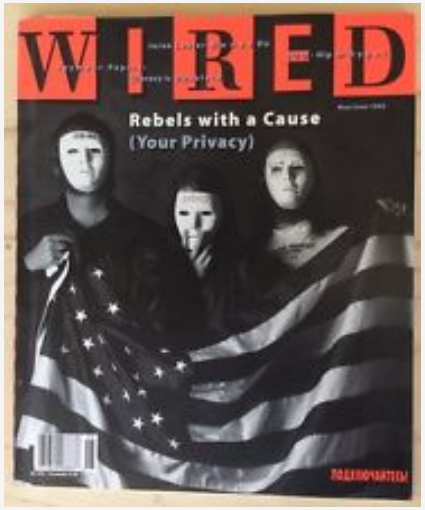
Sensibilities for sale. You don't bite the hand that feeds you.



Fear. You want to attract *more* attention to yourself!?

Why are the strongest crypto-advocates non-cryptographers?

A missing *attitude* – that of the **cypherpunks**.



… We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. … ¶ We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.
Eric Hughes, 1993

even Levy, "Crypto Rebels", *Wired*, May/June 1993.
Tim May – Eric Hughes – John Gilmore

But we discovered something. Our one hope against total domination. A hope that with courage, insight and solidarity we could use to resist. A strange property of the physical universe that we live in. ¶ The universe believes in encryption. ¶ It is easier to encrypt information than it is to decrypt it.
Julian Assange, 2012

In words form history, let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography.
Edward Snowden, 2013

Missing attitude. We lack the energy and sense of purpose of the cypherpunks.

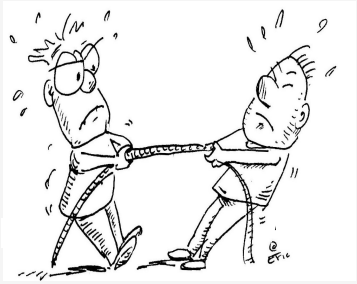
“Going-Dark” Framing

U.S. FBI Director
James Comey

Privacy is a **personal good**

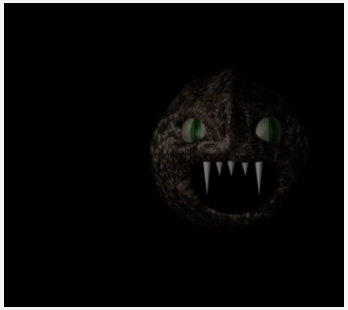
Security is a **collective good**

Inherently in **conflict**



Encryption has destroyed the **balance.** Privacy wins

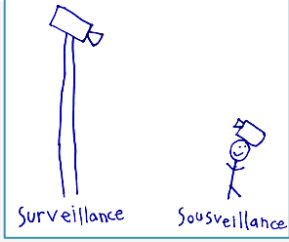
The **bad guys** may win



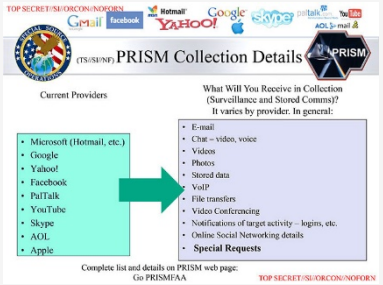
Risk of **Going Dark**.

“Golden-Age of Surveillance” Framing

Drawing by six year old daughter of Steve Mann



Surveillance is an **instrument of power**



Technology makes it **cheap**

Tied to **cyberwar** and **assassinations**

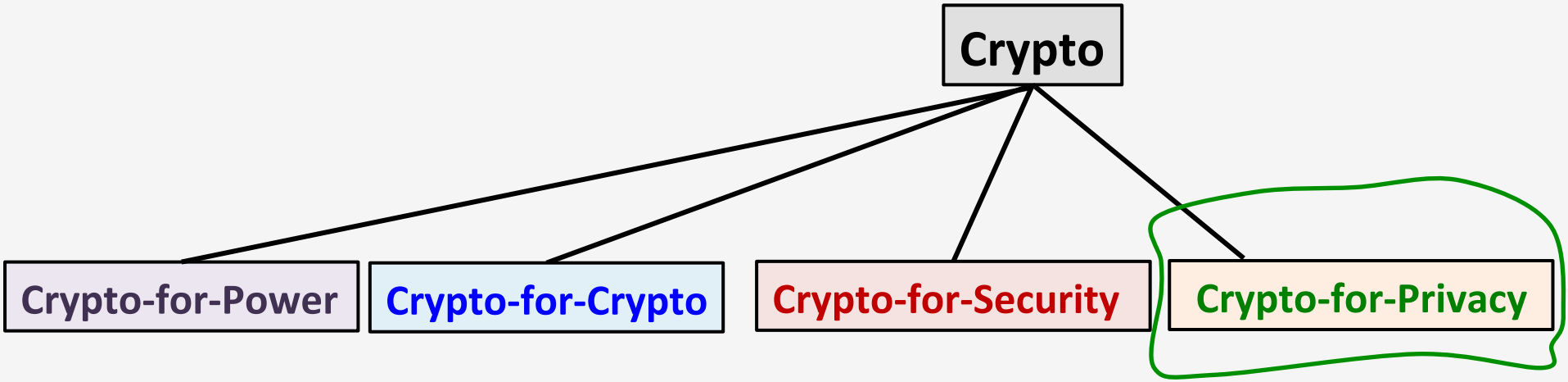
Privacy is a **social** good **rarely** in conflict with security

Makes people **conforming**, **fearful**, **boring**. Stifles **dissent**

The **costs** of surveillance are not born equally

Misframing. Accepting a fictitious storyline of what surveillance is for.

Maybe crypto will save us



Maybe crypto will save us

1. Encryption works, and has a natural democratizing tendency.
2. Cryptographers and developers are smart,
3. And the work can be relevant.
4. Metadata concealment is possible, and is already done (in Tor).
5. End-to-end and device encryption is becoming popular.
6. Open-source, open-hardware movement offers promise.
7. More cryptographers are becoming interested in privacy.
8. And are attending to the political implications of our work.
9. We can rebalance what we do to put more emphasis on crypto-for-privacy.

But probably not

1. Most of the crypto community is busy thinking about other things.
2. Architecture can make crypto support the powerful **or** the powerless.
3. Endpoints are insecure, code is buggy.
4. Security is a "weak-link" property, and crypto is rarely that link.
5. Usable security has proven elusive.
6. No moral compunction among computer scientists, engineers.
7. Privacy-enhancing add-ons add complexity and reduce utility. Economic incentives often wrong. Enormous value gained by mining information flows. Value flows to corporations and governments.
8. Legal protections are weak, legal instruments (eg, NSLs) are strong, most judges don't understand technology.
9. Intelligence agencies have enormous budgets, operate beyond the reach of law. Anything-goes mentality (even, eg, subverting standardization process). Shielded by complexity, secrecy, partnerships, legal invention, linguistic invention.
10. Open source is no panacea (Linus's law: "given enough eyeballs, all bugs are shallow". NO)
11. Monitoring in physical space: facial recognition, license-plate readers, …
12. It's all in the metadata – and concealing metadata hard.
13. Decline of the general-purpose computer.
14. Successful framing by government
15. Technology matters, but policy, law, adherence to law matter more.
16. Corporatism / Public-private "partnership" has never been stronger.

WHY hasn't crypto helped?

Cryptographers have been disinclined to help.
The reasons for this are rooted in the disciplinary culture.

CAN crypto help?

On some matters – *yes*.
How much of a dent can we realistically make??
We won't know without trying.

Authoritarianism

Fearmongering

Jingoism

Corporatism

Militarism

Racism

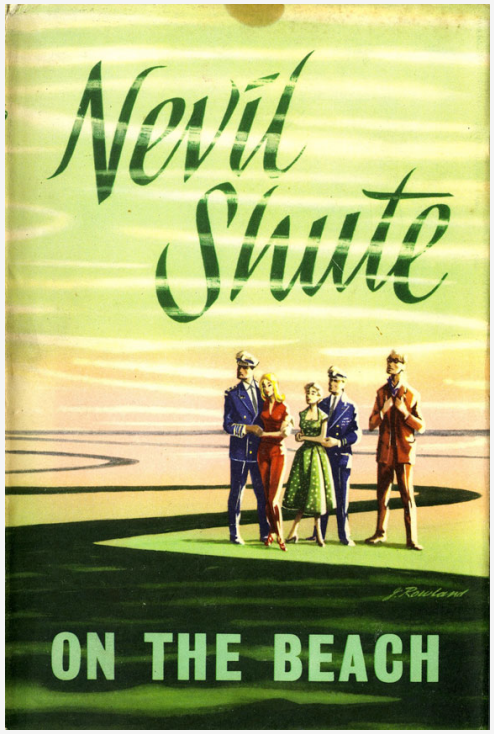
Incarcerations

Assassinations

Fascism

"eventually there will be a time where policies will change, because the *only* thing that restricts the activities of the surveillance state are policy.... And because of that, a new leader will be elected, they'll flip the switch, … and there will be nothing the people can do at that point to oppose it, and it'll be turnkey tyranny. –**E. Snowden**, June 6, 2013

Safely ensconced at the top of the world?



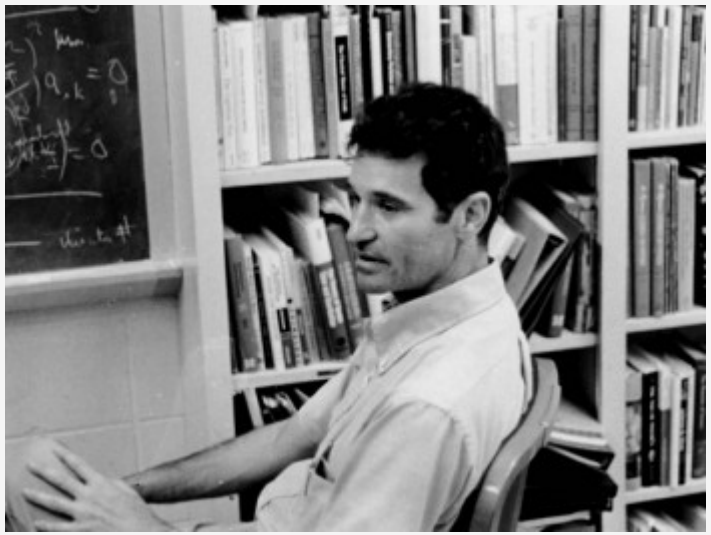
No way.

WHY disinclined to help

1. **Founding ethos.** Crypto is theory, philosophy, and imagination.
2. **Embedded ethos.** This ethos remains dominant, continually renewed by technical/nontechnical choices.
3. **Here for fun.** Intellectuality as sport — pragmatism as small-mindedness.
4. **Irrelevance.** Imagination-genesis work can't actually find a route to practice.
5. **Distanced from security.** Because of community structure.
6. **Standardization non-participation.** Cryptographic standards without the cryptographers.
7. **Value-neutral view.** The myth that science and technology is value-neutral.
8. **Community fracture**. Splitting off of PETS, symbolic approaches to crypto, …
9. **Adversarial abstraction.** Treating the adversary notionally.
10. **Unthreateningly engaged.** We're happy to do stuff irrelevant to power.
11. **Extreme specialization**. Can rob scientists of any sense of agency.
12. **No politics.** An unwillingness to engage in anything "political" connected to ones work.
13. **Dissociation**. A belief that it is reasonable to dissociate ones ethical being from ones work.
14. **Changing motivations.** Current-generation cryptographers aren't in it for moral or political reasons.
15. **Careerism.** What we do aligns with the academic reward system.
16. **Sensibilities for sale.** You don't bite the hand that feeds you.
17. **Institutional amorality.** The prominence of *economic* narratives to crowd out all others
18. **Fear**. You want to attract even *more* attention to yourself?
19. **Missing attitude.** We lack the energy and sense of purpose of the cypherpunks.
20. **Misframing**. Accepting a fictitious storyline of what mass surveillance is for.
21. **Routinization**. People quickly accept their new reality, and even come to think it's good.

The end of dissent

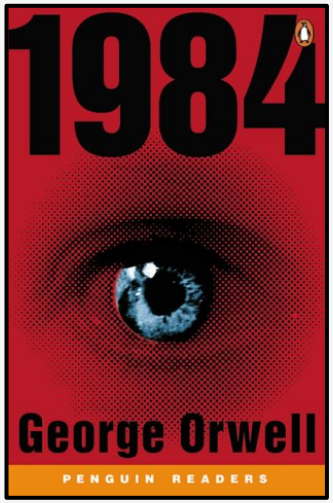
FBI branch office in Media, Pennsylvania.
Burglarized in 1971 by the team headed up by



William Davidon, 1927 - 2013
Professor of Physics
Haverford College, 1961-1991

See Betty Metsger, *The Burglary*, 2014

Sanitization of a dystopia

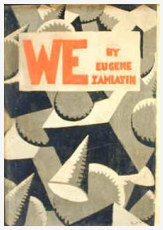


1949

WAR IS PEACE
FREEDOM IS SLAVERY
IGNORANCE IS STRENGTH

1999 – present

Routinization. People quickly accept their new reality, and even come to think it's good.



Yevgeny Zamyatin (1921)

Institutional amorality

Engineering has the Highest Rate of Return for all degrees

The Value of a Degree

Return on investment by college major, 2012

Source: Federal Reserve Bank of New York

- A recent study by the Federal Bank of New York determined that Engineering has the highest return on investment for students at 21% per year. This is also true for the underemployed

UC Engineering Deans, "UC Engineering Analysis, Outcomes and Proposal for Future Growth" (2014). Presentation to J. Napolitano

Institutional amorality. The tendency of economic narratives to crowd out all others, and individual to mirror the amoral stances of their organizations.