Mass Surveillance and the Crisis of Social Responsibility

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

University of Auckland, NZ
9 December 2015

Radomes at RAF Menwith Hill, England

With thanks to
Steven Galbraith
for arranging this
talk and visit

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 ove
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)

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 defeat internet privacy and security

- NSA and GCHQ unlock encryption used to protect emails, banking and medical records

S program works covertly with tech companies to
into products
say programs 'undermine the fabric of the

t questions for our privacy experts

rger and Glenn Greenwald
day 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

some information on millions of ordinary Americans.

Regarded as the most secretive of the nation's intelligence agencies, the NSA is part of the military

TS//SI//REL to USA, FVEY

(S//REL) iPhone Location Services

(U) Who knew in 1984...

TS//SI//REL to USA, FVEY

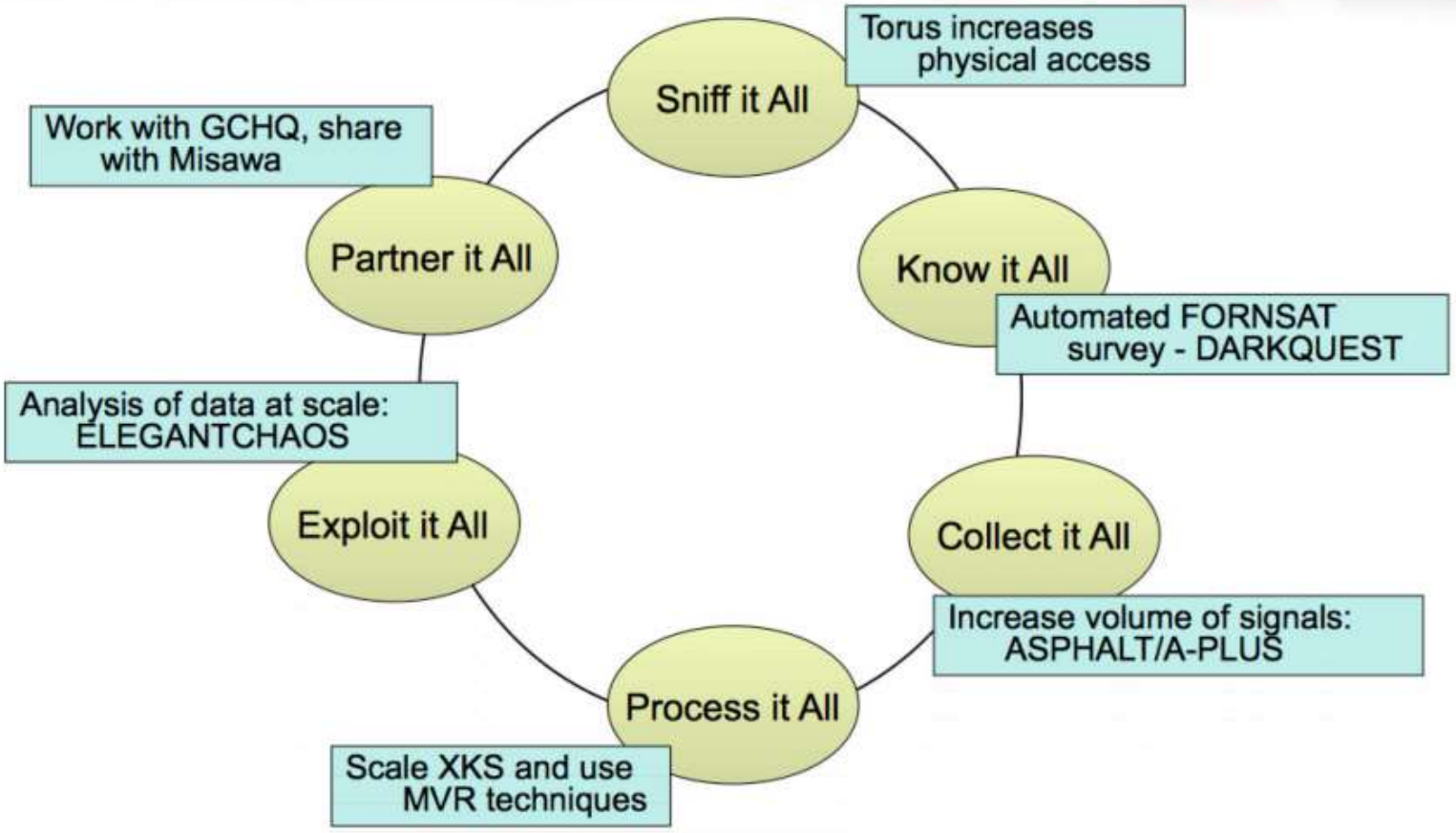
(S//REL) iPhone Location Services

(U) …that this would be big brother…

(S//REL) iPhone Location Services

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

New Collection Posture



Quotes from the “SIGINT Philosopher”

Jacob Weber, 2012

(U) I found myself wishing that my life would be constantly and completely monitored. It might seem odd that a self-professed libertarian would wish an Orwellian dystopia on himself, but here was my rationale: If people knew a few things about me, I might seem suspicious. But if people knew everything about me, they’d see they had nothing to fear.

(U) I guess if we [the NSA] were a corporation, we could make our mission statement … this: “building informed decision makers – so that targets do not suffer our nation’s wrath unless they really deserve it – by exercising deity-like monitoring of the target.” Now <u>that’s</u> philosophy.

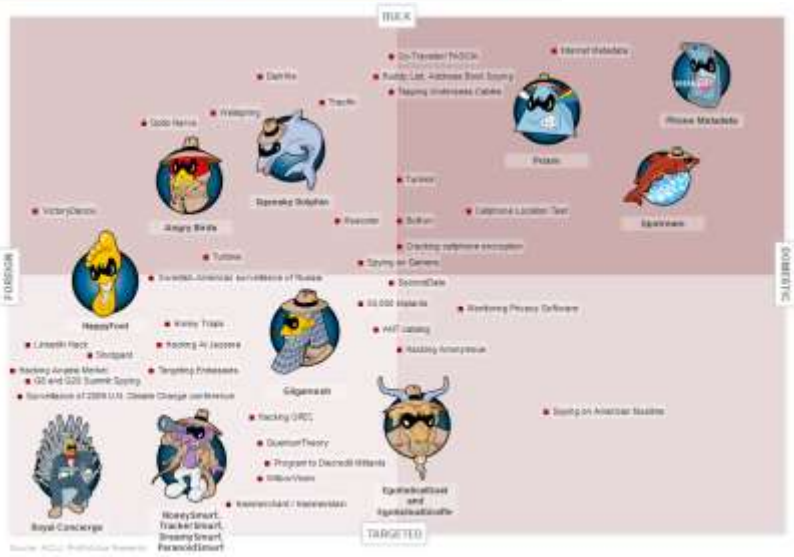
https://www.documentcloud.org/documents/2259077-the-sigint-philosopher-is-back-with-a-new-face.html

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 Undersea Cables	Companies - including BT, Vodafone, and Verizon Business - gave GCHQ access to their undersea 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 Massachusetts 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

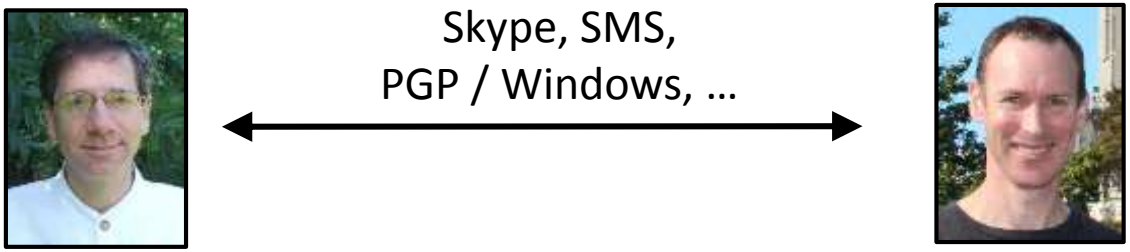
VictoryDance	The NSA tested a technique for using drones to map "the Wi-Fi fingerprint of nearly every major town in Yemen."	NSA
Hammerchant / Hammerstein	NSA programs to spy on data sent through voice over IP calls and Virtual Private Networks.	NSA
ANT catalog	Various techniques - with names like IronChef 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 a	
Wellspring	An NSA	
Spying on American Muslims	FBI mon a former leader o	
Upstream	The Ups commer	
50,000 implants	An NSA surveills	
G8 and G20 Summit Spying	The NS/ Canada	
Phone Metadata	The wel aka met	
HappyFoot	An NSA users' d	



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

ECPA | Executive order 12333 | PATRIOT Act | FISA

The basics are not known

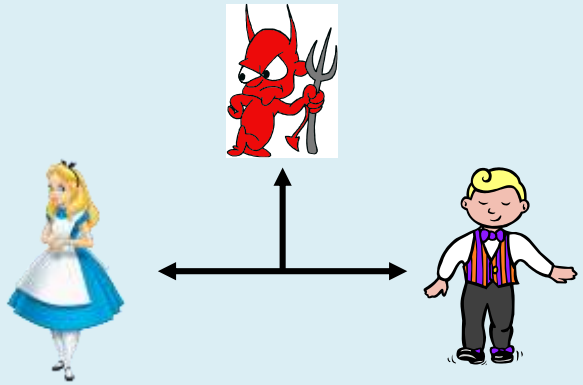


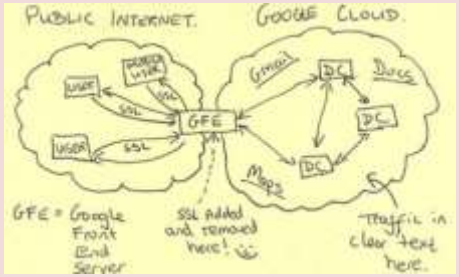
How many copies of the communications are archived, by whom, for how long?
What algorithms are applied– or will be applied – to the data?
What is the data combined with?
When might a human analyst become involved?
What consequences might stem from the communications content?

Secrecy + Complexity

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

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





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

So you might **think** that **cryptographers** would be **aghast** and **embarrassed** about **mass surveillance** revelations.

You'd be utterly wrong.

My community 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 June 15, 2013

A different assessment

- Yes, computer science **is** at the center of major scientific and societal changes.
- But the chances of **dystopian** outcomes are **large**.
- Computer science is at the center of **transforming the Internet** into a frightening tool for **total surveillance**, but few of us say a thing, and many help out.
- **Cryptographers** could play a significant role in resisting this change, but we don't.

WHY?

Answering the QUESTION

Provisos

- **Academic** + **cryptographic** + **personal** perspective
  Inside-the-discipline view; I'm not a technology-studies scholar
- **Communities are *not* monolithic**
  There *are* computer scientists who care deeply about mass surveillance, privacy, and security.
- **I know nothing about the situation in New Zealand**
- **There's not *one* answer to the QUESTION**

An answer. Gets dropped in a box.

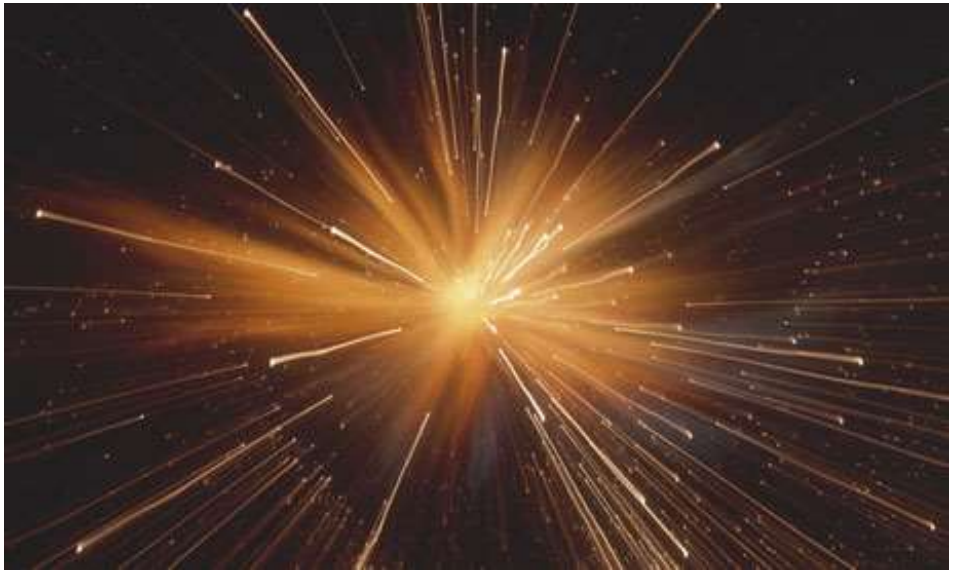
While there's no one answer,

there is one theme:

It's the culture, stupid.

the crypto community
modern computer science
scientific & technical people
contemporary consumer society

From where did cryptographers' 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, 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.

When this ethos dominates …

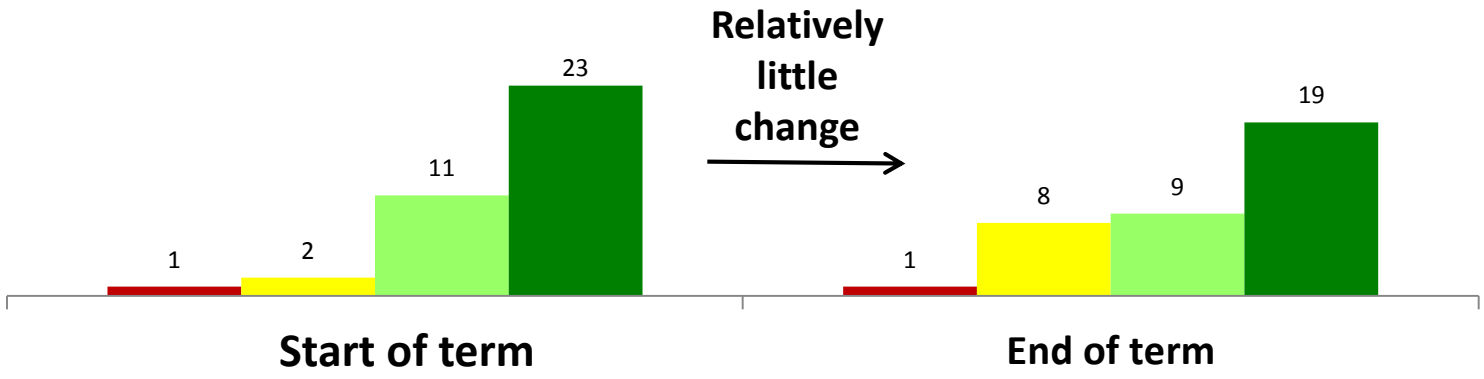
Here for fun. Intellectuality as sport — pragmatism as small-mindedness.

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

Standardization non-participation. Crypto standards without the cryptographers.

And when this ethos dominates …

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



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

Survey data from UC Davis ECS 188, *Ethics in an Age of Technology*, Winger 2013

Artifacts and Ideas are Routinely Political

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.

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

Top reasons given for not signing:

53 signatories
58% acceptance rate

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

Getting political as unprofessional. An unwillingness to engage in anything "political" connected to ones work.

Changing Motivations

The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a 'chilling effect,' causing people to alter their observable activities.

David Chaum
Security without identification: transaction systems to make big brother obsolete
CACM 1985

Nowadays, most computer scientists would be *uncomfortable* by such speech

Changing motivations. Very few current-generation cryptographers and computer scientists are in it for moral or political reasons.

The strongest advocates of cryptography

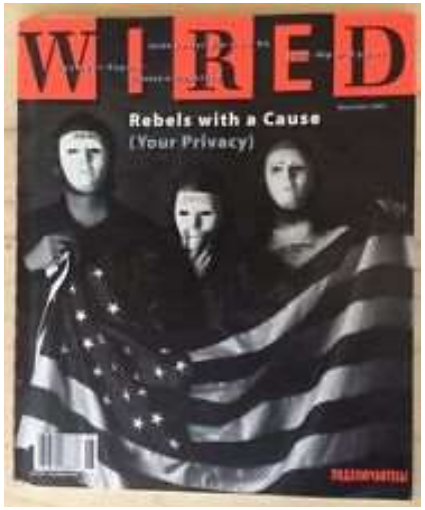
The Cypherpunks

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.

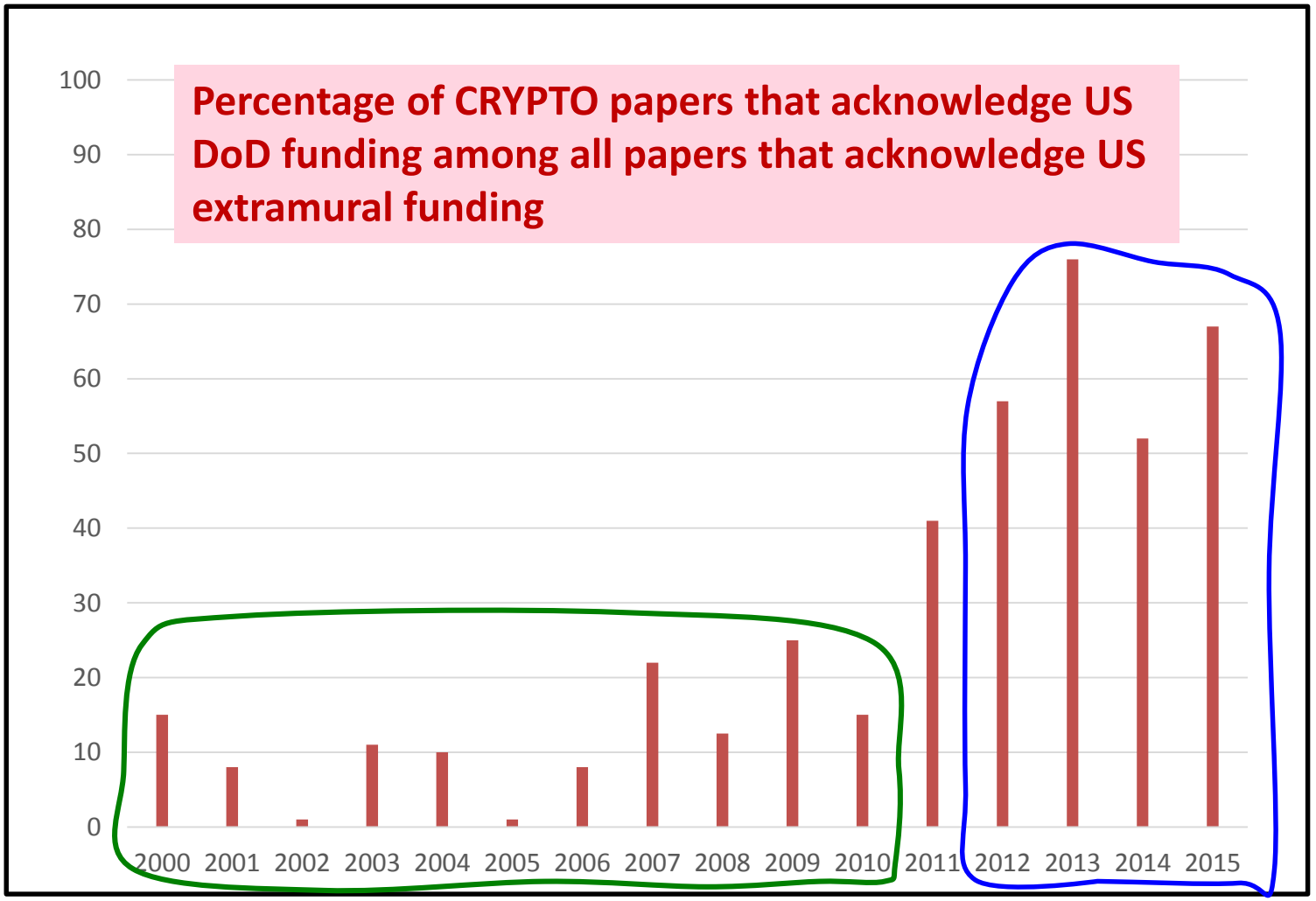
E. Snowden, 2014.



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

Missing attitude. We lack the philosophical drive, and verve, of the cypherpunks.

DoD Funding in Cryptography, 2000-2015



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

The “ethic of responsibility” – the “doctrinal norm” for scientists and engineers

- Do **not** contribute with your work to **social harm.**
  A **negative** right. Obliges **inaction**.

- Contribute with your work to the **social good.**
  A **positive** right. Obliges **action**.

- These obligations stem from your **professional role.**
  For us: as a **cryptographer**, **computer scientist**, and **scientist.**

A norm that never was

- Easy to find scientists for military work
- UC runs WMD labs. Universities run on federal/military funding
- Social-utility of work nearly unconsidered by students
- In academia, having a normative vision deprecated:

do your job; don't try to do someone else's job ... and don't let anyone else do your job. In other words, don't confuse your academic obligations with the obligation to save the world; that's not your job as an academic

Marx famously said that our job is not to interpret the world, but to change it. In the academy, however, it is exactly the reverse: our job is not to change the world, but to interpret it. Stanly Fish, 2004

False norm. The "doctrine of responsibility" was never embraced.

Anti-norm. Taking a moral stance is routinely seen as *un*-academic.

Two-Cultures Explanation

I think much of the problem we face today represents the culmination of a problem diagnosed 55 years ago by C.P. Snow in his essay "The Two Cultures": the absence of dialogue between the ***scientific-technological*** *and the* ***humanist*** *traditions. When Snow wrote his classic essay, he bemoaned that neither culture understood or impinged [upon] the other. Today,* ***bereft of understanding of fundamental issues and writings in the development of liberal democracy, computer geeks devise ever better ways to track people... simply because they can and it's cool****. Humanists on the other hand do not understand the underlying technology and are convinced, for example, that tracking meta-data means the government reads their emails. C.P. Snow's two cultures not only do not talk to each other, they simply act as if the other doesn't exist.*

Two-cultures. Computer scientists are inadequately grounded in humanistic concerns.

Estonian Pres. Toomas Hendrik Ilves (2014)

Radical Individualism

The belief that ones personal interests are more important society's.

Michael Douglas as Gordon Gekko in *Wall Street* (Oliver Stone, 1987)

***Greed**, for lack of a better word, is **good**. Greed is **right**. Greed **works**. Greed clarifies, cuts through, and captures, the essence of the evolutionary spirit. Greed, in all of its forms; greed for life, for money, for love, knowledge, has marked the upward surge of mankind and greed, you mark my words, will … save … that other malfunctioning corporation called the U.S.A.*

Radical individualism. Makes ethical-based motivations seem antiquarian.

Compartmentalization and dissociation

Could you describe your personal view on the social responsibilities of computer scientists?

Phil

I'm a body without a soul

Data-mining faculty candidate

Compartmentalization & dissociation. Life is lived in separated realms. Ethics and work are far apart.

Technological optimism

Technological contextualism

Technological pessimism

Technological optimism. Makes the exertion of moral agency pointless.

Misframing: Law-Enforcement Narrative

U.S. FBI Director
James Comey

Privacy is a **personal good**

Security is a **collective good**

Inherently in **conflict**

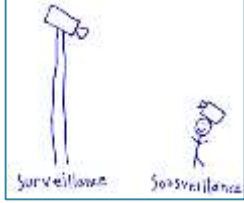
Encryption has destroyed the **balance.** Privacy wins

The **bad guys** may win

Risk of **Going Dark**.

Surveillance-Studies Framing

Drawing by the six-year-old **daughter of** surveillance-studies scholar **Steve Mann**



Surveillance is an **instrument of power**

Technology makes it **cheap**

Tied to **cyberwar** and **conventional war**

Privacy and security usually **not** in conflict

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

Hard to stop. **Cryptography** offers (limited) hope

Mass surveillance always becomes **political surveillance**

KING,

In view of your low grade, abnormal personal behavoir I will not dignify your name with either a Mr. or a Reverend or a Dr. And, your last name calls to mind only the type of King such as King Henry the VIII and his countless acts of adultery and immoral conduct lower than that of a beast.

King, look into your heart. You know you are a complete fraud and a great liability to all of us Negroes. White people in this country have enough frauds of their own but I am sure they don't have one at this time that is any where near your equal. You are no clergyman and you know it. I repeat you are a colossal fraud and an evil, vicious one at that. You could not believe in God and act as you do. Clearly you don't believe in any personal moral principles.

King, like all frauds your end is approaching. You could have been our greatest leader. You, even at an early age have turned out to be not a leader but a dissolute, abnormal moral imbecile. We will now have to depend on our older leaders like Wilkins a man of character and thank God we have others like him. But you are done. Your "honorary" degrees, your Nobel Prize (what a grim farce) and other awards will not save you. King, I repeat you are done.

No person can overcome facts, not even a fraud like yourself. Lend your sexually psychotic ear to the enclosure. You will find yourself and in all your dirt, filth, evil and moronic talk exposed on the record for all time. I repeat - no person can argue successfully against facts. You are finished. You will find on the record for all time your filthy, dirty, evil companions, male and females giving expression with you to your hideous abnormalities. And some of them to pretend to be ministers of the Gospel. Satan could not do more. What incredible evilness. It is all there on the record, your sexual orgies. Listen to yourself you filthy, abnormal animal. You are on the record. You have been on the record - all your adulterous acts, your sexual orgies extending far into the past. This one is but a tiny sample. You will understand this. Yes, from your various evil playmates on the east coast to [redacted] and others on the west coast and outside the country you are on the record. King you are done.

The American public, the church organizations that have been helping - Protestant, Catholic and Jews will know you for what you are - an evil, abnormal beast. So will others who have backed you. You are done.

King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do (this exact number has been selected for a specific reason, it has definite practical significant. You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation.

FBI's "suicide letter" to civil rights leader Martin Luther King, Jr 1964

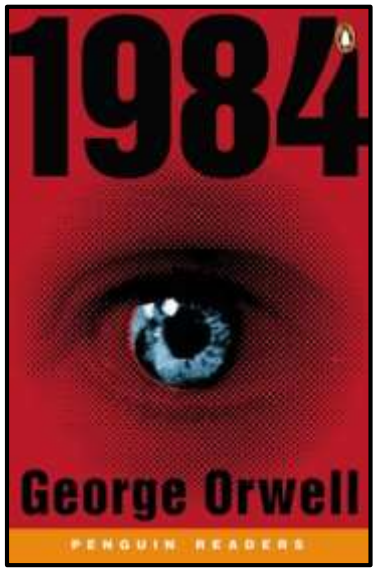
Student activists at UC Berkeley, 1964

Activist Abdul Ghani Al Khanjar

Free Trade Area of the Americas summit Miami, 2003

Misframing. Accepting a fictitious storyline of what mass surveillance is for. The correct framing emphasizes human rights and liberal democracy.

Sanitization of a dystopia



1949

WAR IS PEACE
FREEDOM IS SLAVERY
IGNORANCE IS STRENGTH

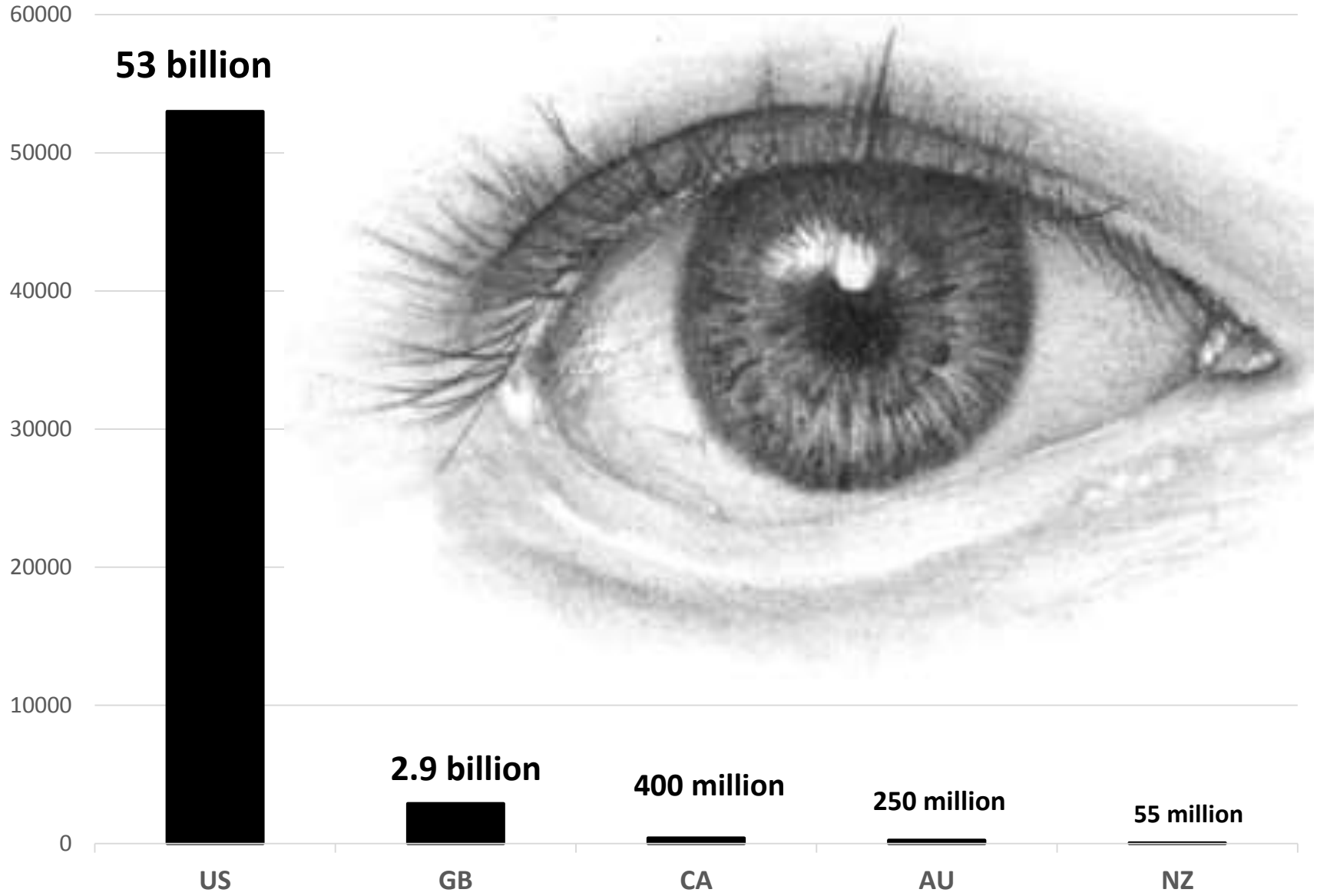
1999 – present

Yevgeny Zamyatin
(1921)

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

Closing Comments

Five-Eyes = one ENORMOUS eye, one small eye, and some noise



Closing Comments

"Truth is Coming and Cannot be Stopped" (2013)
Sarah Lynn Mayhew & D606
Street art in Manchester, UK

Our failure to avert mass surveillance
isn't just a social curiosity,
but an ethical failure of technologists,
as well as governments, worldwide.

It portends, I fear, a broad failure of
liberal democracy.

I am not optimistic, although there is *some* cause for hope:

Disciplinary culture is mutable.
Communications technology is mutable.
The surveillance net is not yet complete.
It is never easy to predict how things will play out.