Crypto and the United States Constitution

Daniel J. Bernstein
University of Illinois at Chicago &
Technische Universiteit Eindhoven

Let's look at crypto
from the government perspective.

We're the government.
We have a long history
of trying hard to understand
what people are saying and
what people are thinking.
("We listen! We care!")

We've put serious time and money and effort into this goal. ("Collect it all.")

We've put serious time and money and effort into this goal. ("Collect it all.")

More and more progress.

But one big annoyance: crypto.

We've put serious time and
money and effort into this goal.
("Collect it all.")

More and more progress.
But one big annoyance: crypto.

What is crypto? Answer:
People using crypto are
people communicating using
a language we don't understand.

We've put serious time and
money and effort into this goal.
("Collect it all.")

More and more progress.
But one big annoyance: crypto.

What is crypto? Answer:
People using crypto are
people communicating using
a language we don't understand.

Sometimes we can't even figure
out *who* is talking to *whom*.
("Tor stinks.")

We've put serious time and
money and effort into this goal.
("Collect it all.")

More and more progress.
But one big annoyance: crypto.

What is crypto? Answer:
People using crypto are
people communicating using
a language we don't understand.

Sometimes we can't even figure
out *who* is talking to *whom*.
("Tor stinks.")

How should we respond?

Three important policy directions:

1. Ban communication that uses incomprehensible languages.
e.g. Iran bans encryption.

Three important policy directions:

1. Ban communication that uses incomprehensible languages.
e.g. Iran bans encryption.

2. Ban *instructions* that say how to speak incomprehensibly.
e.g. US Arms Export Control Act required NSA review and approval for any publication of crypto.

Three important policy directions:

1. Ban communication that uses incomprehensible languages.
e.g. Iran bans encryption.

2. Ban *instructions* that say how to speak incomprehensibly.
e.g. US Arms Export Control Act required NSA review and approval for any publication of crypto.

3. Demand translations of *some* communications.
e.g. UK RIP Act, Part III, lets police demand decryption keys.

Problem in the United States:

For many years
people have been complaining
about much more *limited* ways
that we try to understand them.

Problem in the United States:

For many years
people have been complaining
about much more *limited* ways
that we try to understand them.

The United States courts
keep saying that we're violating
the "United States Constitution"
and ignoring people's "rights".

Problem in the United States:

For many years
people have been complaining
about much more *limited* ways
that we try to understand them.

The United States courts
keep saying that we're violating
the "United States Constitution"
and ignoring people's "rights".

This talk: some examples
of the barriers we're facing—
constitutional court decisions
inconsistent with our policies.

Bill of Rights (excerpts)

First Amendment:
"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

Fourth Amendment:
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Fifth Amendment:

"No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

Bill of Rights is a
limitation on federal government.
Was (mostly) extended to states
after Civil War.

Fourteenth Amendment: "... No
State shall make or enforce
any law which shall abridge the
privileges or immunities of citizens
of the United States; nor shall any
State deprive any person of life,
liberty, or property, without due
process of law; nor deny to any
person within its jurisdiction the
equal protection of the laws. ..."

Judicial review

Classic "prior restraint":
before communicating you must
submit content to a censor
who decides whether
the communication is allowed.

Judicial review

Classic "prior restraint":
before communicating you must
submit content to a censor
who decides whether
the communication is allowed.

Freedman v. Maryland, 380 U.S. 51 (1965): Prior restraint must have procedural protections:
(1) *judge* deciding whether
the content is protected speech;
(2) burden of proof on censor;
(3) adversarial proceedings;
(4) brief time limits.

NSA review and approval
for publication of crypto:
classic prior restraint of
protected speech (instructions).
No procedural safeguards.
$\Rightarrow$ Unconstitutional.
See *Bernstein v. U.S.*
and in part *Junger v. Daley*.

NSA review and approval
for publication of crypto:
classic prior restraint of
protected speech (instructions).
No procedural safeguards.
$\Rightarrow$ Unconstitutional.
See *Bernstein v. U.S.*
and in part *Junger v. Daley*.

Lesson #1: Pesky judges
don't blindly trust us
to respect people's "rights".

NSA review and approval
for publication of crypto:
classic prior restraint of
protected speech (instructions).
No procedural safeguards.
$\Rightarrow$ Unconstitutional.
See *Bernstein v. U.S.*
and in part *Junger v. Daley*.

Lesson #1: Pesky judges
don't blindly trust us
to respect people's "rights".

Lesson #2: We should have
eliminated approval procedure,
simply banned everything.

Warrants for searches

Katz v. U.S., 389 U.S. 347 (1967) (internal quotes omitted): Eavesdropping requires warrant. Fourth Amendment "requires adherence to judicial processes . . . searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions."

Search must have
“precise limits established in
advance by a specific court order”
after “detached scrutiny
by a neutral magistrate”.
(Judicial review again!)

Search must have
"precise limits established in
advance by a specific court order"
after "detached scrutiny
by a neutral magistrate".
(Judicial review again!)

After search must "notify the
authorizing magistrate in detail
of all that had been seized".

Search must have
"precise limits established in
advance by a specific court order"
after "detached scrutiny
by a neutral magistrate".
(Judicial review again!)

After search must "notify the
authorizing magistrate in detail
of all that had been seized".

Serious problems for our goal
of understanding the people.

Search must have
"precise limits established in
advance by a specific court order"
after "detached scrutiny
by a neutral magistrate".
(Judicial review again!)

After search must "notify the
authorizing magistrate in detail
of all that had been seized".

Serious problems for our goal
of understanding the people.

The exceptions are narrow:
occasionally useful for us
but clearly not enough.

Example of an exception:
Police can search anyone
who they (validly) arrest.
Motivations for this exception:
concealment/destruction of
evidence; hidden weapons.

Example of an exception:
Police can search anyone
who they (validly) arrest.
Motivations for this exception:
concealment/destruction of
evidence; hidden weapons.

But see Riley v. California, 573 U.S. ___ (2014): "These two cases raise a common question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. . . . Our answer [is] simple—get a warrant."

Privacy of association

NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958): "State scrutiny of membership lists" of NAACP violates the Fourteenth Amendment.

Albertson v. Subversive Activities Control Board, 382 U.S. 70 (1965): Compelled registration of members of any "Communist action organization" violates the Fifth Amendment.

Anonymity

Talley v. California, 362 U.S. 60 (1960): Prohibition on distribution of anonymous leaflets violates the First Amendment. "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."

The way forward

We need to undermine
these court decisions.

Strategy: Accuse communicators
of being child pornographers,
drug dealers, terrorists, etc.

Clearly any incomprehensible
communication is something *bad*:
obscenity; copyright violation;
fraud; false advertising; libel;
conspiracy; aiding the enemy;
advocacy of unlawful conduct;
plotting a revolution; etc.

“Terrorism” has turned out
to be a fantastic word for us:
eliminates warrant requirements,
due-process requirements, etc.

"Terrorism" has turned out
to be a fantastic word for us:
eliminates warrant requirements,
due-process requirements, etc.

Public-relations problem: We've
been caught lying to drug judges;
spying on World of Warcraft,
Petrobras, Airbus, Merkel; etc.
So nobody believes that we're
simply fighting "terrorism".

"Terrorism" has turned out
to be a fantastic word for us:
eliminates warrant requirements,
due-process requirements, etc.

Public-relations problem: We've
been caught lying to drug judges;
spying on World of Warcraft,
Petrobras, Airbus, Merkel; etc.
So nobody believes that we're
simply fighting "terrorism".

Someone that FBI+NSA spied on
for activism, war opposition,
association with Communists
(picture credit: Wikipedia):