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.")

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.")

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

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.")

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.

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.")

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.")

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.")

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?

and the
States Constitution

. Bernstein
ty of Illinois at Chicago &
che Universiteit Eindhoven

---

ok at crypto
e government perspective.

he government.
e a long history
g hard to understand
ople are saying and
ople are thinking.
ten! We care!")

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 in

1. Ban c
incompr
e.g. Iran

stitution

n
is at Chicago &
siteit Eindhoven

---

to
ent perspective.

nent.
story
understand
aying and
hinking.
care!")

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 p

1. Ban communic
incomprehensible l
e.g. Iran bans encr

ago &
hoven

ective.

l

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 direc

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

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.

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.

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.

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.

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.

ut serious time and
nd effort into this goal.
t it all.")

d more progress.
big annoyance: crypto.

crypto? Answer:
using crypto are
ommunicating using
ge we don't understand.

nes we can't even figure
is talking to *whom*.
inks.")

ould we respond?

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

For man
people h
about m
that we

time and
into this goal.

ogress.
vance: crypto.

Answer:
to are
ating using
n't understand.

n't even figure
to *whom*.

spond?

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 Un

For many years
people have been
about much more
that we try to und

oal.

pto.

g
tand.

gure
.

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 State

For many years
people have been complainin
about much more *limited* w
that we try to understand th

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.

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.

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

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.

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.

nportant policy directions:

communication that uses
ehensible languages.
bans encryption.

instructions that say
speak incomprehensibly.
Arms Export Control Act
NSA review and approval
oublication of crypto.

and translations
communications.
RIP Act, Part III, lets
emand 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.

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 R

First Am
"Congre
respectir
religion,
exercise
the freed
press; or
peaceab
petition
redress c

policy directions:

ation that uses
anguages.
ryption.

ns that say
mprehensibly.
ort Control Act
ew and approval
n of crypto.

ations
cations.
Part III, lets
cryption keys.

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 (exc

First Amendment:
"Congress shall ma
respecting an esta
religion, or prohibi
exercise thereof; o
the freedom of spe
press; or the right
peaceably to asser
petition the Gover
redress of grievanc

ctions:

uses

y

bly.

ol Act

proval

o.

ts

eys.

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
religion, or prohibiting the fr
exercise thereof; or abridging
the freedom of speech, or of
press; or the right of the peo
peaceably to assemble, and
petition the Government for
redress of grievances."

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."

in the United States:

y years
have been complaining
nuch more *limited* ways
try to understand them.

ted States courts
ving that we're violating
ited States Constitution"
oring people's "rights".

k: some examples
arriers we're facing—
tional court decisions
tent 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 A
"The rig
secure ir
papers, a
unreason
seizures,
and no W
upon pro
by Oath
particula
to be sea
things to

nited States:

complaining
limited ways
lerstand them.

s courts
we're violating
s Constitution"
le's "rights".

xamples
re facing—
rt decisions
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 Amendmen
"The right of the
secure in their per
papers, and effects
unreasonable searc
seizures, shall not
and no Warrants s
upon probable cau
by Oath or affirma
particularly describ
to be searched, an
things to be seizec

es:

ng
ays
hem.

ting
tion"
s".

_
s
s.

<u>Bill of Rights (excerpts)</u>

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
secure in their persons, hous
papers, and effects, against
unreasonable searches and
seizures, shall not be violate
and no Warrants shall issue,
upon probable cause, suppor
by Oath or affirmation, and
particularly describing the pl
to be searched, and the pers
things to be seized."

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.”

Rights (excerpts)

nendment:
ss shall make no law
ng an establishment of
or prohibiting the free
thereof; or abridging
dom of speech, or of the
r the right of the people
ly to assemble, and to
the Government for a
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 Am
“No pers
in any cr
witness
be depriv
property
law; nor
taken fo
compens

erpts)

ake no law
blishment of
ting the free
r abridging
eech, or of the
of the people
mble, and to
nment for a
ces.”

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 . . . sh
in any criminal cas
witness against hi
be deprived of life
property, without
law; nor shall priva
taken for public us
compensation.”

v
of
ree
g
f the
ople
to
a

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 com
in any criminal case to be a
witness against himself, nor
be deprived of life, liberty, o
property, without due proces
law; nor shall private proper
taken for public use, withou
compensation."

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.”

Amendment:
ght of the people to be
n their persons, houses,
and effects, against
nable searches and
shall not be violated,
Warrants shall issue, but
obable cause, supported
or affirmation, and
rly describing the place
arched, and the persons or
o 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 R
limitatio
Was (mo
after Civ

Fourteen
State sh
any law
privilege
of the U
State de
liberty, c
process c
person w
equal pr

nt:
people to be
sons, houses,
s, against
ches and
be violated,
shall issue, but
use, supported
ation, and
bing the place
d the persons or
d.”

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 feder
Was (mostly) exte
after Civil War.

Fourteenth Amend
State shall make o
any law which sha
privileges or immu
of the United Stat
State deprive any
liberty, or property
process of law; nor
person within its j
equal protection o

be

ses,

d,

but

rted

ace

sons or

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 governn
Was (mostly) extended to st
after Civil War.

Fourteenth Amendment: ".
State shall make or enforce
any law which shall abridge
privileges or immunities of c
of the United States; nor sha
State deprive any person of
liberty, or property, without
process of law; nor deny to a
person within its jurisdiction
equal protection of the laws.

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. . . .”

nendment:

son . . . shall be compelled riminal case to be a against himself, nor ved of life, liberty, or , without due process of shall private property be r public use, without just sation."

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

Classic " before co submit o who dec the com

all be compelled
se to be a
mself, nor
, liberty, or
due process of
ate property be
se, without just

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 restr
before communica
submit content to
who decides wheth
the communicatio

npelled

r
ss of
ty be
t just

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 m submit content to a censor who decides whether the communication is allowe

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.

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.

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.

ights is a
n on federal government.
ostly) extended to states
vil War.

nth Amendment: "… No
all make or enforce
which shall abridge the
s or immunities of citizens
nited States; nor shall any
eprive any person of life,
or property, without due
of law; nor deny to any
within its jurisdiction the
otection of the laws. …"

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 rev
for publi
classic p
protecte
No proc
⇒ Unco
See *Ber*
and in p

ral government.
ended to states

dment: "... No
or enforce
ll abridge the
nities of citizens
tes; nor shall any
person of life,
, without due
r deny to any
urisdiction the
f the laws. ..."

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 a
for publication of
classic prior restra
protected speech (
No procedural safe
⇒ Unconstitution
See *Bernstein v. U*
and in part *Junge*

ment.
tates

. . No

the
itizens
all any
life,
due
any
the
. . . .”

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 (instructio
No procedural safeguards.
⇒ Unconstitutional.
See *Bernstein v. U.S.*
and in part *Junger v. Daley*.

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.
⇒ Unconstitutional.
See *Bernstein v. U.S.* and in part *Junger v. Daley*.

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.
⇒ 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”.

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.
⇒ 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.

review

‘prior restraint”:
ommunicating you must
content to a censor
ides whether
munication is allowed.

an v. Maryland, 380 U.S.
5): Prior restraint must
ocedural protections:
re deciding whether
tent is protected speech;
en of proof on censor;
ersarial proceedings;
f time limits.

NSA review and approval
for publication of crypto:
classic prior restraint of
protected speech (instructions).
No procedural safeguards.
⇒ 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.

Warrant

Katz v.
(1967) (
Eavesdro
Fourth A
adherenc
processe
outside t
without
judge or
unreasor
Amendm
few spec
well deli

raint":
ting you must
a censor
her
n is allowed.

yland, 380 U.S.
estraint must
rotections:
g whether
tected speech;
of on censor;
ceedings;
ts.

NSA review and approval
for publication of crypto:
classic prior restraint of
protected speech (instructions).
No procedural safeguards.
⇒ 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 searc

Katz v. U.S., 389
(1967) (internal q
Eavesdropping req
Fourth Amendmen
adherence to judic
processes . . . searc
outside the judicia
without prior appr
judge or magistrat
unreasonable unde
Amendment—subj
few specifically est
well delineated exc

must

ed.

U.S.

ust

ech;

or;

NSA review and approval
for publication of crypto:
classic prior restraint of
protected speech (instructions).
No procedural safeguards.
⇒ 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 omit
Eavesdropping requires warr
Fourth Amendment "require
adherence to judicial
processes . . . searches condu
outside the judicial process,
without prior approval by
judge or magistrate, are per
unreasonable under the Four
Amendment—subject only t
few specifically established a
well delineated exceptions."

NSA review and approval for publication of crypto: classic prior restraint of protected speech (instructions). No procedural safeguards. ⇒ 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."

view and approval
cation of crypto:
rior restraint of
d speech (instructions).
edural safeguards.
onstitutional.
nstein v. U.S.
art *Junger v. Daley*.

#1: Pesky judges
ndly trust us
ct people's "rights".

#2: We should have
ed approval procedure,
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 r
"precise
advance
after "de
by a neu
(Judicial

pproval
crypto:
int of
(instructions).
eguards.
al.
J.S.
r v. Daley.

judges
us
s “rights”.

hould have
al procedure,
erything.

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 esta
advance by a spec
after “detached sc
by a neutral magis
(Judicial review ag

ns).

e

re,

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 o after "detached scrutiny by a neutral magistrate". (Judicial review again!)

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!)

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!)

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

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!)

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

Serious problems for our goal of understanding the people.

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!)

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.

s for searches

U.S., 389 U.S. 347
(internal quotes omitted):
opping requires warrant.
Amendment "requires
ce to judicial
s . . . searches conducted
the judicial process,
prior approval by
magistrate, are per se
nable under the Fourth
nent—subject only to a
cifically established and
neated exceptions."

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
Police ca
who they
Motivati
concealn
evidence

ches

U.S. 347
uotes omitted):
uires warrant.
nt "requires
cial
ches conducted
l process,
oval by
te, are per se
er the Fourth
ject only to a
tablished and
ceptions."

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 exc
Police can search
who they (validly)
Motivations for th
concealment/destr
evidence; hidden w

cted):
ant.
es

ucted

se
rth
o a
nd

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 exceptio
concealment/destruction of
evidence; hidden weapons.

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.

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.

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.”

must have
limits established in
by a specific court order"
etached scrutiny
tral magistrate".
review again!)

arch must "notify the
ing magistrate in detail
at had been seized".

problems for our goal
standing the people.

eptions are narrow:
ally useful for us
rly not enough.

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

NAACP
rel. Patt
(1958):
member
violates
Amendm

Alberts
Control
(1965):
registrat
"Commu
violates

ablished in
ific court order"
rutiny
strate".
gain!)

"notify the
rate in detail
en seized".

for our goal
the people.

e narrow:
l for us
ough.

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."

<u>Privacy of associat</u>

NAACP v. Alaban
rel. Patterson, 357
(1958): "State scr
membership lists"
violates the Fourte
Amendment.

Albertson v. Subve
Control Board, 38
(1965): Compelle
registration of me
"Communist actio
violates the Fifth

n
order”

ne
tail
.
al
.

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 NAAC violates the Fourteenth Amendment.

Albertson v. Subversive Acti Control Board, 382 U.S. 70 (1965): Compelled registration of members of a “Communist action organiza violates the Fifth Amendmen

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.

e of an exception:
an search anyone
y (validly) arrest.
ions for this exception:
ment/destruction of
e; hidden weapons.

Riley v. California, 573
_ (2014): “These two
ise a common question:
the police may, without a
search digital information
l phone seized from
idual who has been
. . . . Our answer [is]
-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.

Anonym

Talley v.
60 (1960
distribut
violates
“Anony
brochure
have pla
in the pr
Persecut
from tim
history h
oppressiv
either ar

ception:
anyone
arrest.
is exception:
ruction of
veapons.

California, 573
"These two
mon question:
e may, without a
gital information
ized from
has been
answer [is]
rant."

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. Californi
60 (1960): Prohib
distribution of ano
violates the First A
"Anonymous pam
brochures and eve
have played an im
in the progress of
Persecuted groups
from time to time
history have been
oppressive practice
either anonymousl

on:

573

vo

ion:

hout a

mation

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 le
violates the First Amendmer
"Anonymous pamphlets, lea
brochures and even books
have played an important ro
in the progress of mankind.
Persecuted groups and sects
from time to time throughou
history have been able to cri
oppressive practices and law
either anonymously or not a

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."

of association

v. Alabama ex
rerson, 357 U.S. 449
“State scrutiny of
ship lists” of NAACP
the Fourteenth
nent.

on v. Subversive Activities
Board, 382 U.S. 70
Compelled
ion of members of any
unist action organization”
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

We need
these co

Strategy
of being
drug dea

Clearly a
commun
obscenit
fraud; fa
conspira
advocac
plotting

tion

na ex
7 U.S. 449
rutiny of
of NAACP
eenth

ersive Activities
2 U.S. 70
d
mbers of any
n organization"
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 under
these court decisio

Strategy: Accuse
of being child porn
drug dealers, terro

Clearly any incom
communication is
obscenity; copyrig
fraud; false advert
conspiracy; aiding
advocacy of unlaw
plotting a revoluti

P

ivities

ny
ation"
nt.

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 communic
of being child pornographers
drug dealers, terrorists, etc.

Clearly any incomprehensible
communication is something
obscenity; copyright violatio
fraud; false advertising; libel
conspiracy; aiding the enemy
advocacy of unlawful conduc
plotting a revolution; etc.

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.

ity

California, 362 U.S. 0): Prohibition on ion of anonymous leaflets the First Amendment. mous pamphlets, leaflets, es and even books yed an important role rogress of mankind. ted groups and sects ne to time throughout have been able to criticize ve practices and laws nonymously 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.

"Terroris to be a eliminat due-proc

a, 362 U.S.
ition on
onymous leaflets
Amendment.
phlets, leaflets,
n books
portant role
mankind.
and sects
throughout
able to criticize
es and laws
y 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 tu
to be a fantastic w
eliminates warrant
due-process requir

.

eaflets
nt.
flets,

le

s
ut
iticize
s
t 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 requireme
due-process requirements, et

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.

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.

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".

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.

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):

y forward

d to undermine
urt decisions.

y: Accuse communicators
child pornographers,
alers, terrorists, etc.

any incomprehensible
nication is something *bad*:
y; copyright violation;
alse advertising; libel;
cy; aiding the enemy;
y of unlawful conduct;
a revolution; 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”.

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

mine
ons.

communicators
nographers,
orists, etc.

prehensible
something *bad*:
nt violation;
ising; libel;
the enemy;
vful conduct;
on; 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".

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

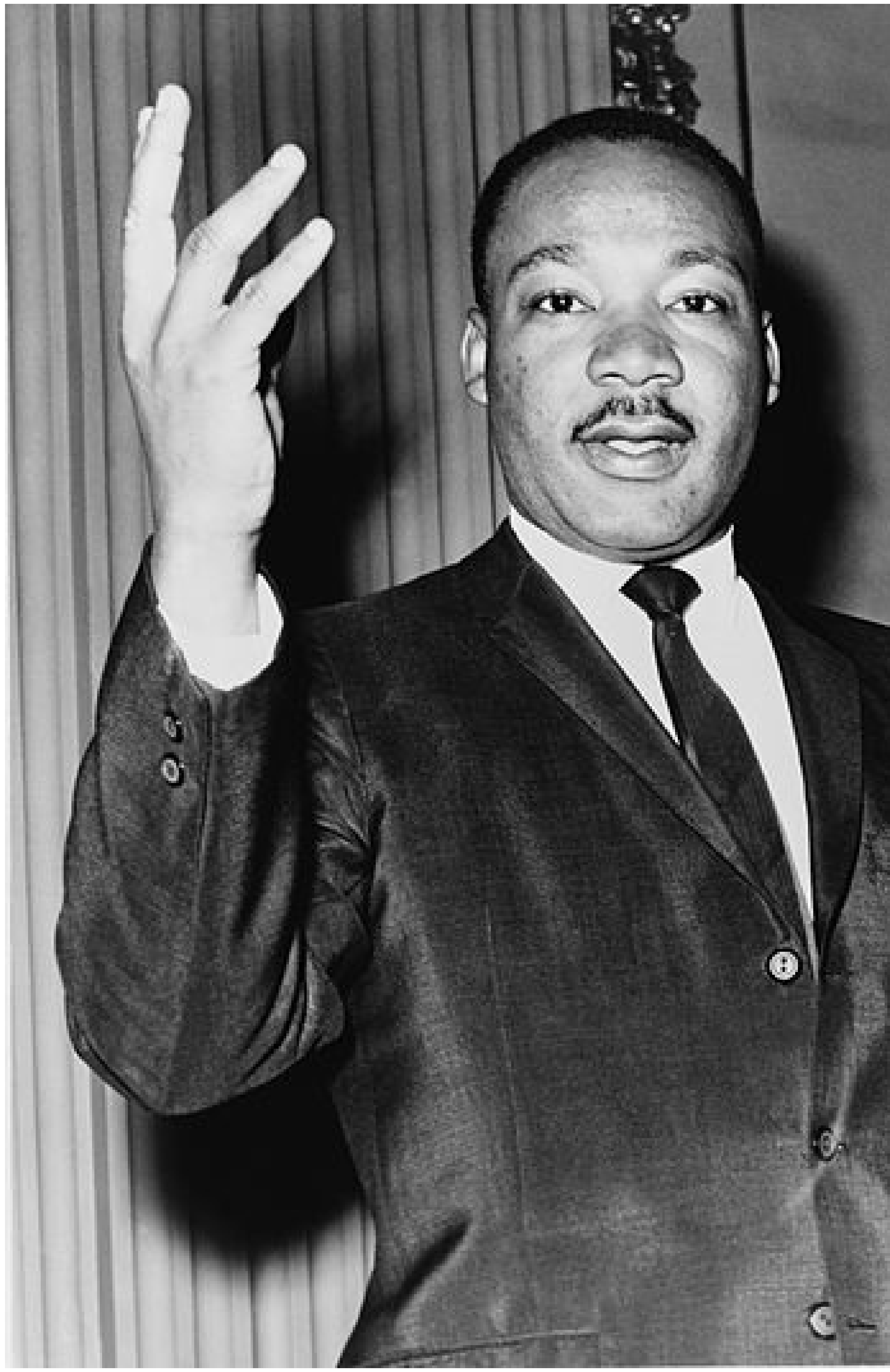
ators
s,

e
g *bad*:
n;
;
y;
ct;

“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):



“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):