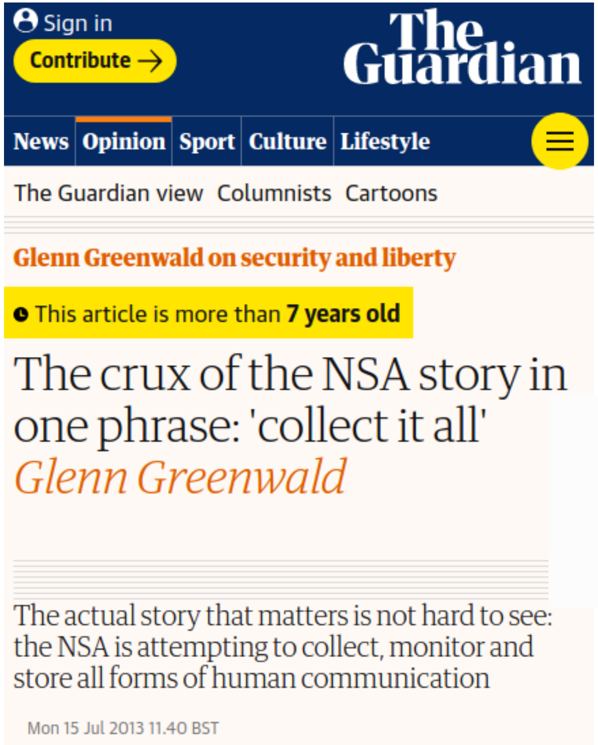
Privacy, mass-surveillance, and cryptography



Glenn Greenwald on security and liberty

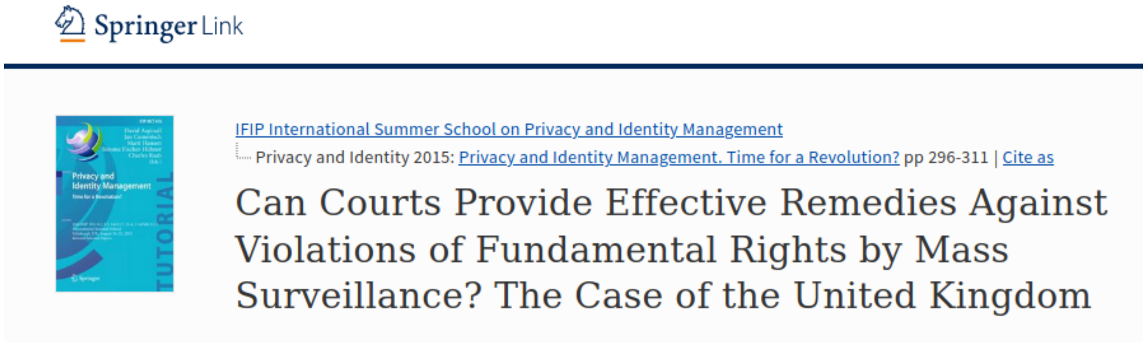
This article is more than **7 years old**

The crux of the NSA story in one phrase: 'collect it all'

Glenn Greenwald

The actual story that matters is not hard to see: the NSA is attempting to collect, monitor and store all forms of human communication

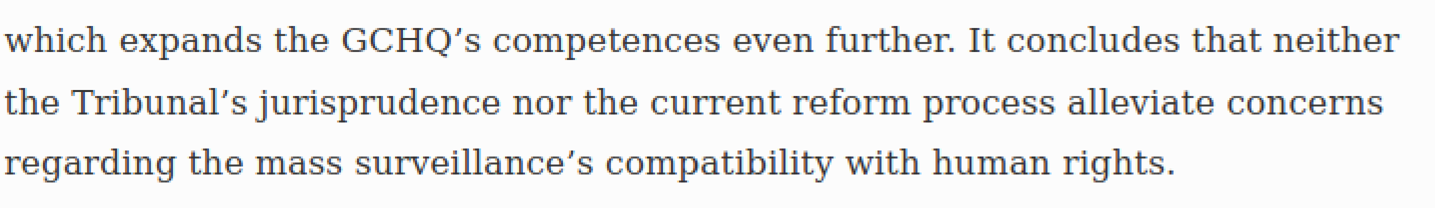
Mon 15 Jul 2013 11.40 BST



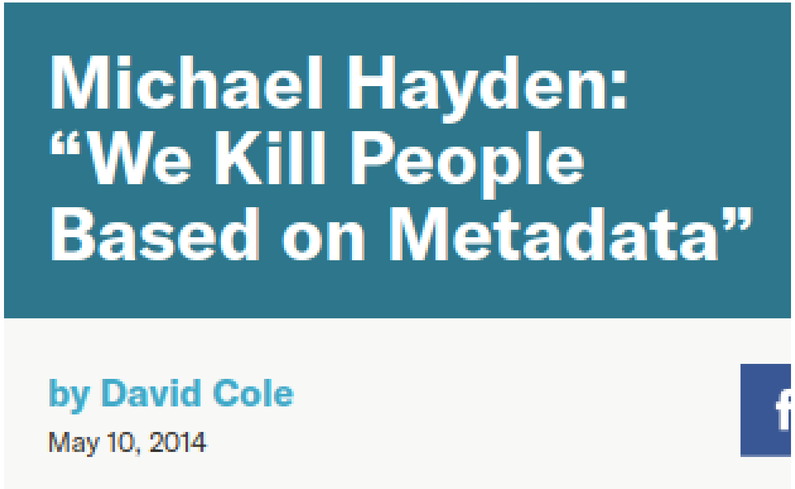
IFIP International Summer School on Privacy and Identity Management

Privacy and Identity 2015: Privacy and Identity Management. Time for a Revolution? pp 296-311 | Cite as

Can Courts Provide Effective Remedies Against Violations of Fundamental Rights by Mass Surveillance? The Case of the United Kingdom


which expands the GCHQ's competences even further. It concludes that neither the Tribunal's jurisprudence nor the current reform process alleviate concerns regarding the mass surveillance's compatibility with human rights.

https://youtu.be/kV2HDM86XgI?t=1026



Michael Hayden: "We Kill People Based on Metadata"

by David Cole

May 10, 2014

Cryptography:

- Attempts to give everyone the option of privacy

- How? Secure communication over an insecure channel

Viewers of the insecure channel: **Adversaries**

Not all adversaries are made equal!

Large-scale adversaries

Examples:

- Powerful governments.
- Large data collection companies (like Google or Facebook).

Some abilities:

- Ability to store and/or access large amounts of (meta)data long-term.
- Access to much higher computing power than users.
- Influence over encryption standards (c.f. backdoors).
- Influence over potential ‘Trusted Third Parties’.

Small-scale adversaries

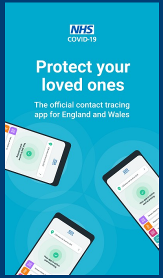
Limitations:

- Cannot store large amounts of (meta)data long-term.
- No option for ‘legal’ acquisition of data stored by others.
- Weaker assumptions on computing power.
- ‘Trusted Third Parties’ can be reasonably used to aid against small-scale adversaries.

Use-cases for secure communication

- Encrypted messaging.

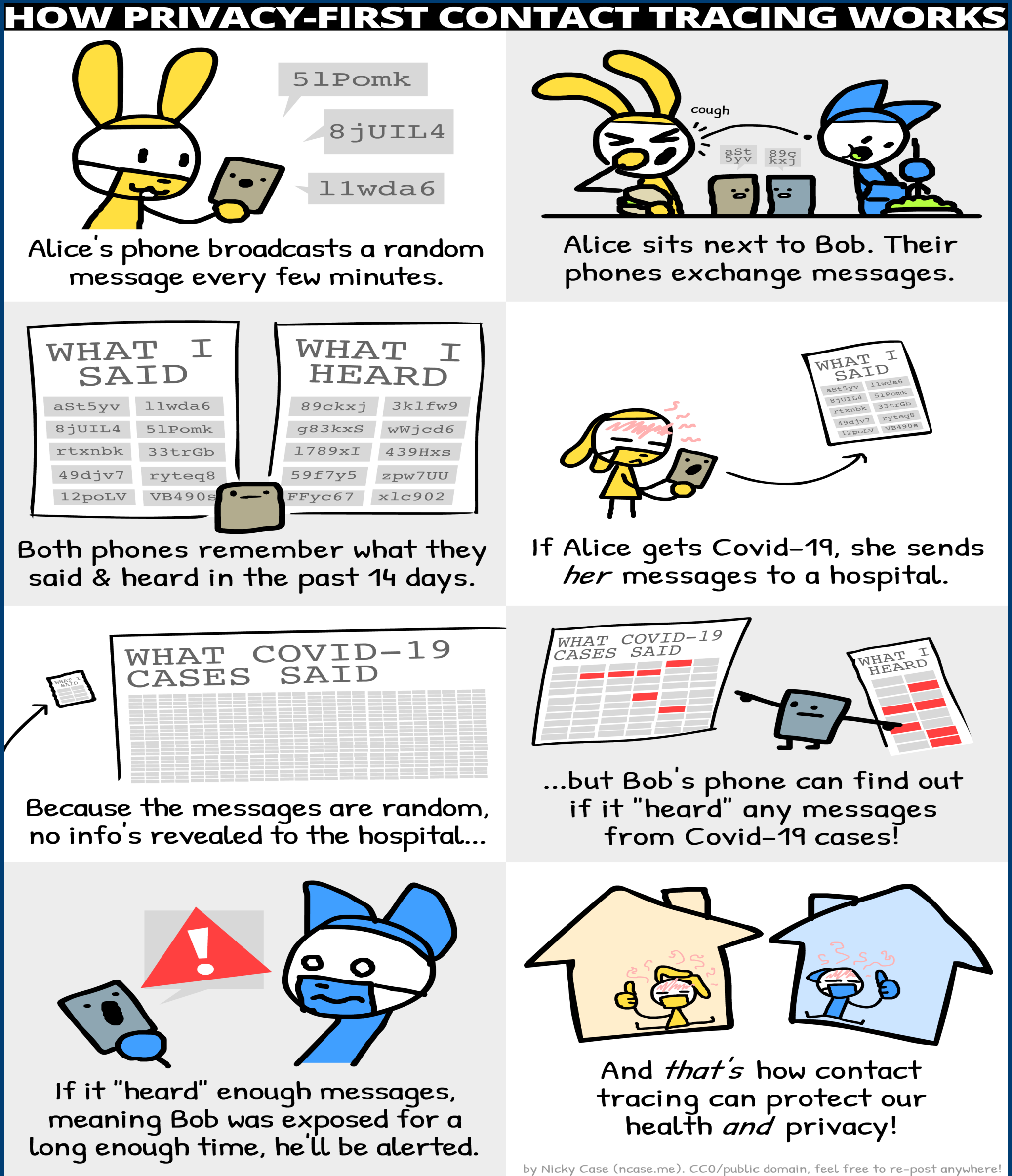
- Authentication of your identity (e.g. so people can’t impersonate you).
- Preserving anonymity online.
- Preserving anonymity with contact tracing.



- (etc.)

Image due to Nicky Case.

Describes DP-3T.



HOW PRIVACY-FIRST CONTACT TRACING WORKS

Alice's phone broadcasts a random message every few minutes.

Alice sits next to Bob. Their phones exchange messages.

WHAT I SAID

aSt5yv	l1wda6
8jUIL4	51Pomk
rtxnbk	33trGb
49djv7	ryteq8
12poLV	VB490s

WHAT I HEARD

89ckxj	3klfw9
g83kxS	wWjcd6
1789xI	439Hxs
59f7y5	zpw7UU
FFyc67	x1c902

Both phones remember what they said & heard in the past 14 days.

If Alice gets Covid-19, she sends *her* messages to a hospital.

Because the messages are random, no info's revealed to the hospital...

...but Bob's phone can find out if it "heard" any messages from Covid-19 cases!

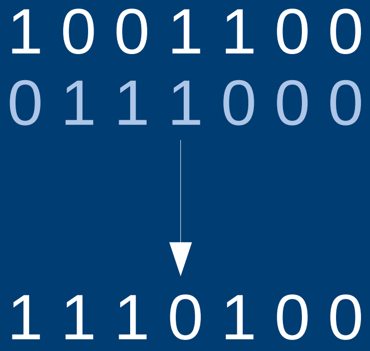
If it "heard" enough messages, meaning Bob was exposed for a long enough time, he'll be alerted.

And *that's* how contact tracing can protect our health *and* privacy!

by Nicky Case (ncase.me). CC0/public domain, feel free to re-post anywhere!

Encrypted messages: One Time Pads

- Message: a bit string (e.g. m = 1001100)
- OTP: also a bit string (e.g. k = 0111000)
- Encrypted message: line up m and k, and flip the bit of m if corresponding bit in k is 1.



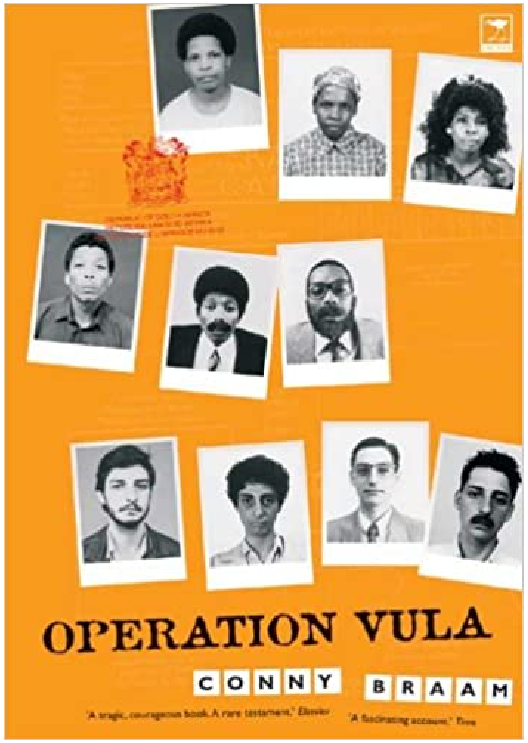
1 0 0 1 1 0 0

0 1 1 1 0 0 0

1 1 1 0 1 0 0

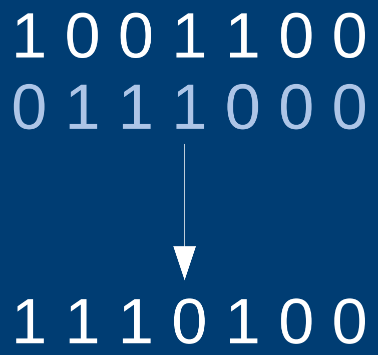
Anti-Apartheid Movement
REMEMBER BOIPATONG

THE
VULA CONNECTION


OPERATION VULA
CONNY BRAAM
'A tragic, courageous book. A rare testament.' Elsevier
'A fascinating account.' Time

Encrypted messages: One Time Pads

- Message: a bit string (e.g. m = 1001100)
- OTP: also a bit string (e.g. k = 0111000)
- Encrypted message: line up m and k, and flip the bit of m if corresponding bit in k is 1.



1 0 0 1 1 0 0

0 1 1 1 0 0 0

1 1 1 0 1 0 0

Public Key Encryption (PKE)

User

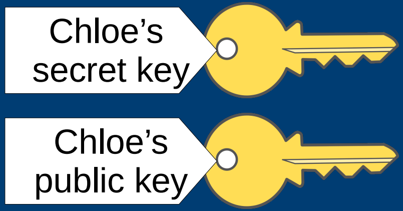
I need people to be able to send me encrypted messages

Public Key Encryption (PKE)

User

I need people to be able to send me encrypted messages

1. **KeyGen**



Chloe’s secret key

Chloe’s public key

Public Key Encryption (PKE)

User

1. **KeyGen**

Chloe's secret key

Public database

Chloe's public key

Public Key Encryption (PKE)

User

1. **KeyGen**

Chloe's
secret key

Public database

Chloe's
public key

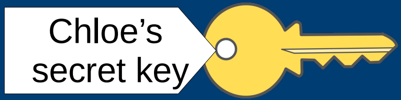
Second party

I need to
send Chloe
an encrypted
message

Public Key Encryption (PKE)

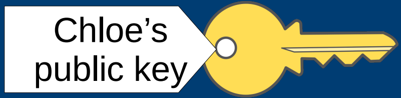
User

1. **KeyGen**



Chloe’s secret key

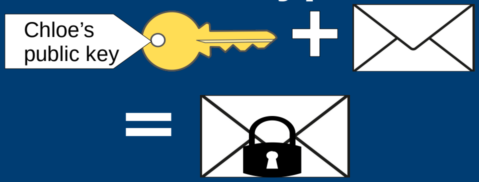
Public database



Chloe’s public key

Second party

2. **Encrypt**



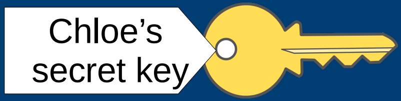
Chloe’s public key +

=

Public Key Encryption (PKE)

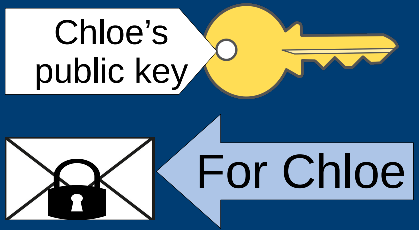
User

1. **KeyGen**



Chloe's secret key

Public database

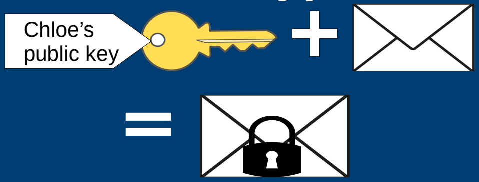


Chloe's public key

For Chloe

Second party

2. **Encrypt**

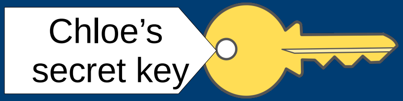


Chloe's public key + =

Public Key Encryption (PKE)

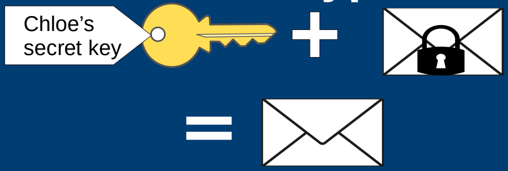
User

1. **KeyGen**



Chloe’s secret key

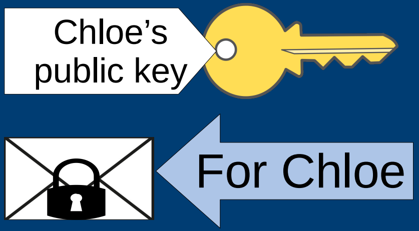
3. **Decrypt**



Chloe’s secret key +

=

Public database

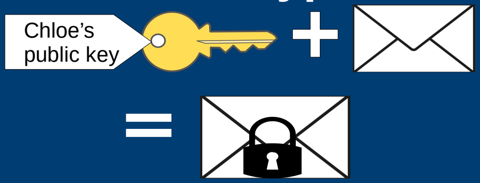


Chloe’s public key

For Chloe

Second party

2. **Encrypt**



Chloe’s public key +

=

- WhatsApp, Signal, Google etc. use PKE
- Medical and criminal records are secured with PKE

- New method of computing uses quantum physics
- This will break (almost) all PKE currently in use

- Large-scale adversaries store data long-term
- With a quantum computer, can decrypt all private data

QUANTUM COMPUTING
Disney
~~RALPH~~
BREAKS THE
INTERNET
© 2019 Disney

- My research: creating PKE resistant to quantum computers

- All current ideas are slow or big and mostly untested

- Big challenge: convince companies to make the switch

- Other challenges: humans, side-channels...