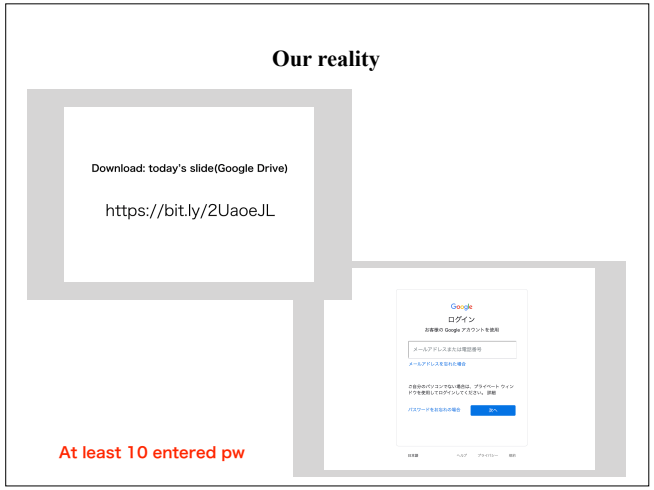
Digital Security in Japanese Journalism

19Q4 @ Hong Kong, 2019/12/12



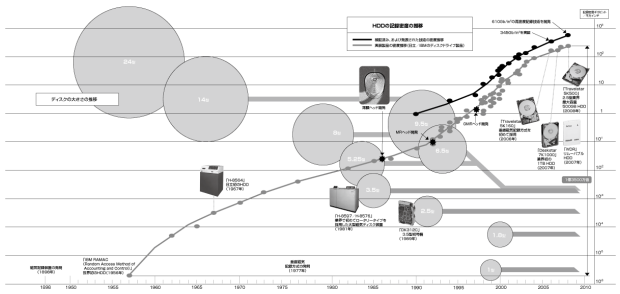
Last summer, I did a digital security workshop for Japanese journalists in Tokyo. I explained how internet works, what phishing is or what social engineering is. At the end of the workshop, I showed this URL for downloading “today’s material.” This URL was the link to my web page where I created a fake Google login page. At least 10 journalists entered their passwords. They are not stupid journalists. They were security-conscious enough to come voluntarily to the early morning session. This is the reality we have to face.

Journalists in US were wondering:

Prosecutions of whistleblowers increased under Obama administration.
He was a civil rights attorney and an academic teaching constitutional law.
Why?

Recent years, US journalists were wondering why prosecutions of whistleblowers increased under Obama administration. He was a civil rights attorney and an academic teaching constitutional law.

Traces abound in storages



1995 1GB 400USD 2019 4TB 100USD

It is not because of 9.11. In my opinion, there are so many traces left in data storages that “suspected whistleblowers” cannot deny the involvements and law enforcement officials have enough evidence to prosecute them. In their background is rapid and continuous improvement of hard disks.

Traces abound in storages

NSA Utah Data Center:2013,12EB,$1.4b

cf. Google, 15EB

NSA Utah Data Center is built around 2013 costed $1.4b. Reportedly it has capability to capture all in-coming communications and store it into 12EB storages. Recording all telephone communications in US needs 300PB, i.e. 0.3EB, 24h low-rate video recording of all Americans needs 2EB. NSA is not so audacious. Google is said to have 15EB worldwide. Maybe the building where you are working has CCTV system with terabyte disk. These inexpensive, massive data storage has changed the landscape of our information security and privacy.

Conventional protections are invalidated

1. **By workplace**

   No court order required for employer

   Office phones/Office PC/Mail/
   Internet access/Security gate/CCTV

1. **By private sector**

   MobilePhone/Credit card/Frequent user reward/
   Book purchase/Itenerary/Parking receipt/
   Google/Facebook/Twitter

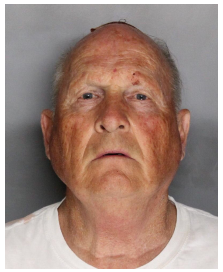
   For bill/improvement/marketing purposes
   Most companies are “cooperative” with investigators

1. **By cheap storage & search technology**

   Gather whatever can be acquired, devise applications afterwards
   retroactive surveillance

In democratic societies, communication and privacy are closely related to its value of liberty and are protected by constitutional laws. For eg, Interception, wiretapping of telephone, by law enforcement agencies has been selectively allowed with court orders.
But, by massive data storage, these conventional protections are invalidated. Not only governmental agencies but also telephone networks are accumulating massive data for daily monitoring, billing, technical improvements or marketing. Every aspect of data are being kept digitally in our workplace for management, quality control, streamlining or automation. With cheaper disks, companies tend to record everything to analyze it afterwards. (explain slide here)

Conventional protections are invalidated



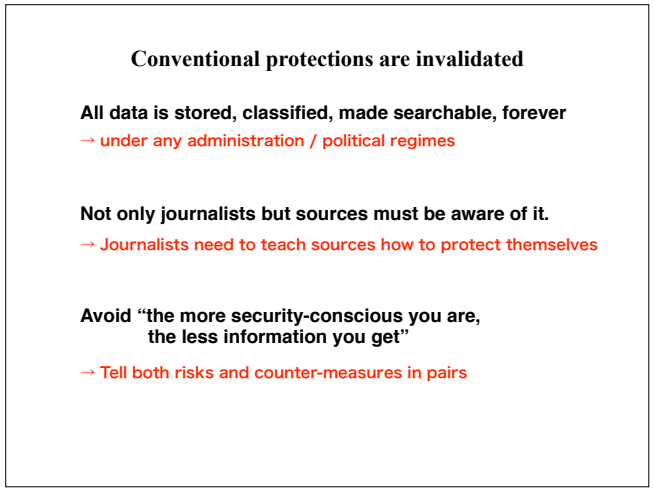
Golden State Killer

At least 10 relatives of Golden State Killer had uploaded their DNA data. Can we consent to use of DNA information that is shared with future relatives?

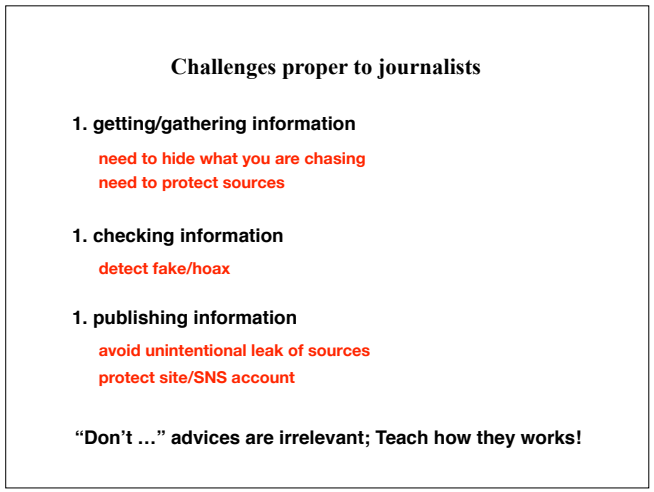
In April 2018, California officers arrested Joseph DeAngelo. He is allegedly the Golden State Killer, a serial killer who committed at least 13 murders, more than 50 rapes, and over 100 burglaries in California from 1974 to 1986. To chase him down, the investigative officials uploaded the killer's DNA profile to the website GEDmatch, an open DNA database which is used by adoptees searching for birth parents. They found at least 10 potential relatives with the killer. Of course Joseph DeAngelo did not upload his DNA information but these 10 relatives did. Did these 10 people gave consent to use their DNA in such a manner? More basically, can we consent to the use of DNA which is not exclusively yours? your consent may affect your grand-grand-sons' escape from police or their health insurance premium.

Conventional protections are invalidated

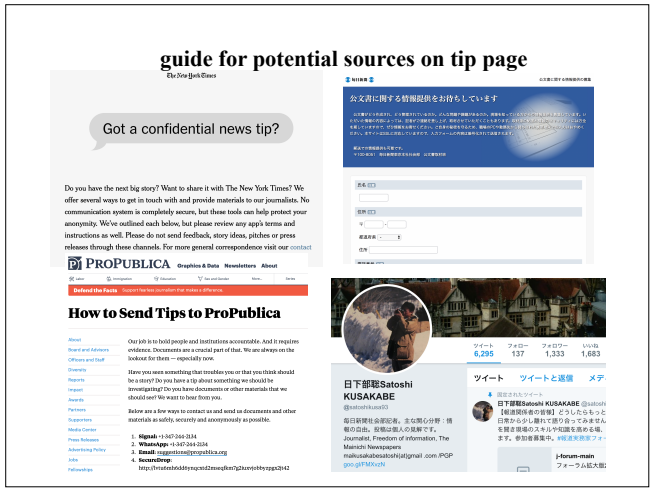
By the same token, how can we consent to the access to mobile phone's directory which is not about ourselves but about our friends' ?
This is my facebook page. I have never used my real name, birthday, school history. But these "friend requests" shows my friends exactly. Probably these people had allowed FB to access to their directories and the app had extracted my mail address, phone number or physical address from it. FB matched my sole real information, mail address, to the extracted data and, probably, FB has already known my real name, real phone number and real address without my consent. Are we aware that the consent to access to the directory means the disclosure of friends' data without their consent?



Now that we live in a society where all data is stored forever, classified afterwards, made searchable at any time. Protecting sources is getting more difficult where even the very first contact between reporters and sources might be recorded. It has nothing to do with political regime, government policy. Journalists need to teach potential sources how to protect themselves before the first contact. At the same time, we must avoid "the more security-conscious you are, the less information you get" situation for journalists.
So the workshop I did emphasized the explanation of how digital tools work and told both risks and counter-measures in pairs.



Moreover, There are many challenge proper to journalists. Some companies have system to monitor website access from news organizations and potentially adversarial NGOs. You might have need to hide what you are chasing.



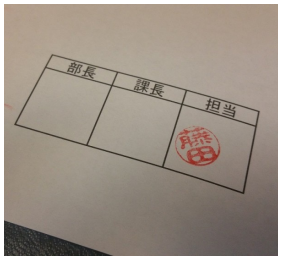
News organizations now have “tips” pages written in educational languages.
A personal SNS profile with PGP fingerprint serves as a good indicator of security-trained journalist.

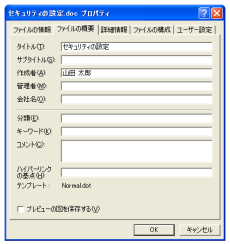
CryptoParty, 2012-
by Australian journos

documentary, 2017
by German/French journos

Pressing need to educate sources gave birth to these activities.
CryptoParty is a open meetup to think about cybersecurity, emphasizing practical hands-ons about digital securities such as PGP or introduction of secure texting app.
It was conceived in 2012 by the Australian journalist following the passing of the Cybercrime Legislation Amendment Bill.
Nothing to Hide was a documentary film about mass surveillance. It was made by French and German video journalists in 2017. It was dealing with surveillance and its acceptance by the general public through the "I have nothing to hide" argument.

Document might have tracking cues



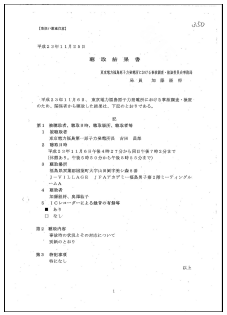


The most important thing in digital security training for journalists is unintentional leakage of sources in published materials.

In 1971, Takichi Nishiyama, a political reporter for Mainichi newspaper, published a story based on the leaked documents about secret bargaining over Okinawa reversion between US and Japan. As the story did not caused wide controversy, he handed over the the copy of the documents to politicians of opposition party. The copies circulated and the ruling governments found who leaked the document from the red seals that senior officials stamps when they had read it. (In Japanese bureaucracy documents circulate from bottom to top with stamps). This is why journalists usually do not publish the leaked documents in its self or entirely.

In digital age, the informations about the author might be left in document property.

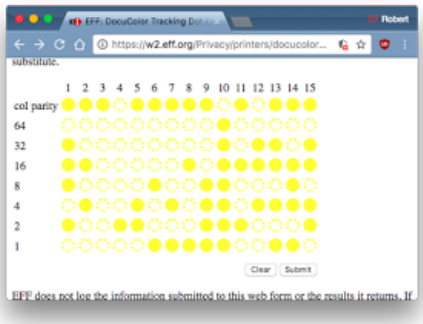
Document might have tracking cues



RGB(254,254,254)でフィルター

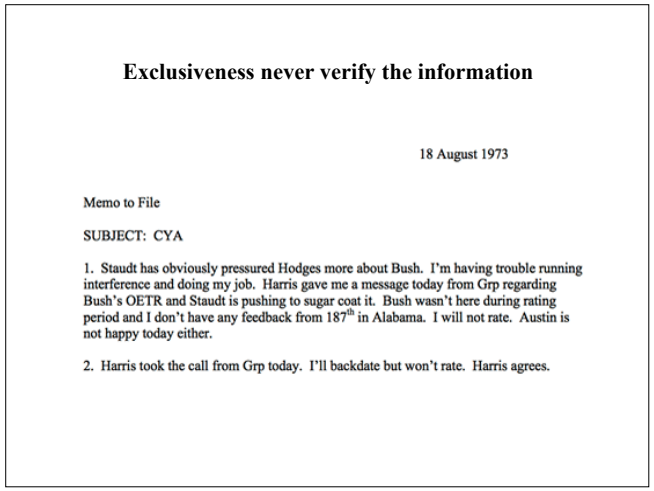
Seemingly simple documents might be stamped invisible to humans but clear to computers.
This document has a serial number on it with RGB(254,254,254). Frequently updated documents are, in a sense, serial-numbered automatically. Adobe PDF documents have a capabilities to track who opened the file by sending a signal to the verification server. Don't open PDF when your PC is online.

Reality Winner case



In June 2017, Reality Winner, an American intelligence specialist, was arrested on suspicion of leaking an intelligence report about Russian interference in US elections to the news website The Intercept. She sent to the Intercept, startup news organization, confidential documents printed by laser printers in office. The reporter is said to have showed the documents to the NSA officials. Now almost all laser printers have capability to stamp almost-invisible tiny yellow dots which records printer's ip-address and time.

With traditional media diminishing and start-up news media hiring more and more young reporters, Journalism are losing hard-earned wisdom of battle field; Never show naked documents to anyone except your editor.



Exclusiveness never verify the information

18 August 1973

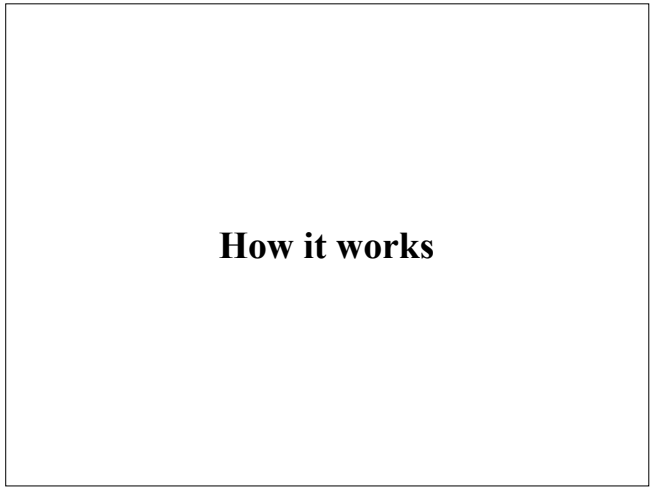
Memo to File

SUBJECT: CYA

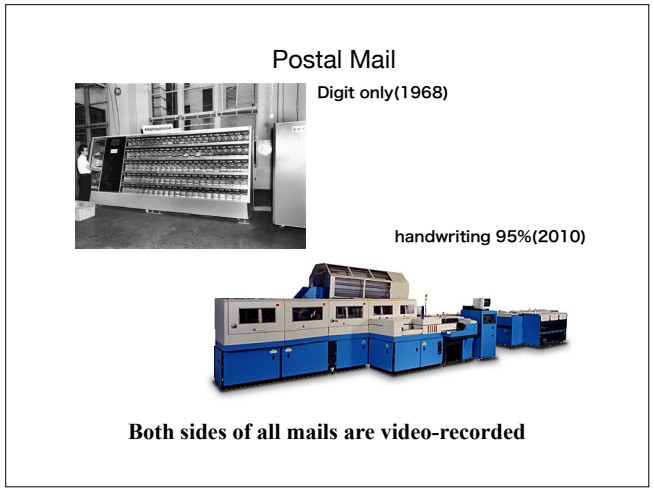
1. Staudt has obviously pressured Hodges more about Bush. I'm having trouble running interference and doing my job. Harris gave me a message today from Grp regarding Bush's OETR and Staudt is pushing to sugar coat it. Bush wasn't here during rating period and I don't have any feedback from 187th in Alabama. I will not rate. Austin is not happy today either.

2. Harris took the call from Grp today. I'll backdate but won't rate. Harris agrees.

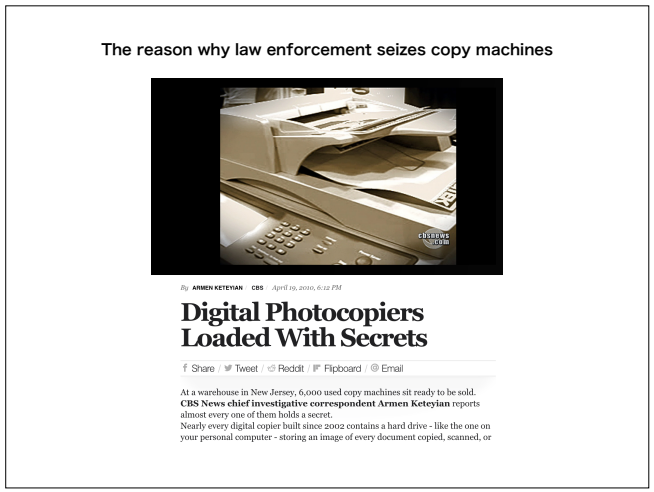
The Killian documents are said to be harsh allegations about President Bush's service in the Texas Air National Guard in 1972–73. The famous 60 Minutes of CBS presented these documents as authentic during 2004 presidential election campaign, but it was later found fake. The font used in the documents was the same as Microsoft Word 2004. I don't know whether this was an hoax against mainstream media or fake documents against President Bush. Getting documents through secure, exclusive route does not mean the documents are authentic.



How it works



In Japan zip code was introduced in 1968 to automate sorting out post cards. At first the machines can read only 5 digits in predefined area. Now manufacturers are boasting of the these machines that can read 95% of the handwritten addresses in 50 languages. The machines video-record both sides of all mails. In US, keeping records of all mails is required by law. About 160 billion mails are recorded every year. In japan, it is not required by law but privatized Japan Post are streamlining the structure of the delivery. Now almost all mails are processed by machines. Even your Christmas cards to your friends living next door travels to the regional distribution center to be video-recorded.

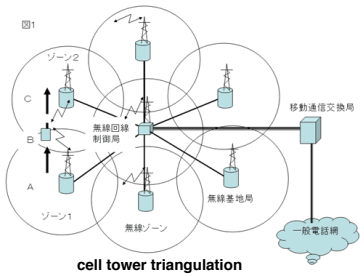


Copying machines are now digital archive machines. All documents are scanned and stored in disks and the data stays forever unless you did not change the initial settings. This news is by CBS reporter who bought secondhand copying machines and checked the stored documents in the disks. This is the reason why law enforcement seizes copy machines in the office when someone is arrested.

ANPR（Automatic number-plate recognition,1987）

Automatic number-plate recognition cameras are so prevalent. In Japan, this system is under loose control of the police so that every law enforcement officials can access to these data. Haven't you read news stories about fugitive criminals, detected by CCTV and ANPR?
The same is true to reporters. Don't use your car when you have to meet someone confidentially. Use Taxi and pay in cash.

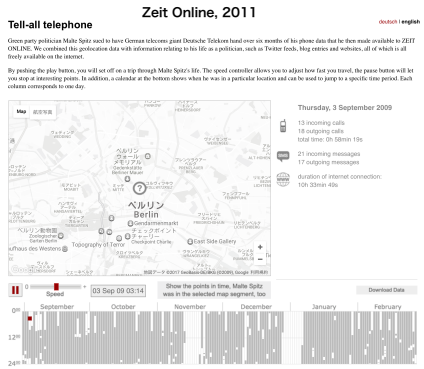
Phone



cell tower triangulation

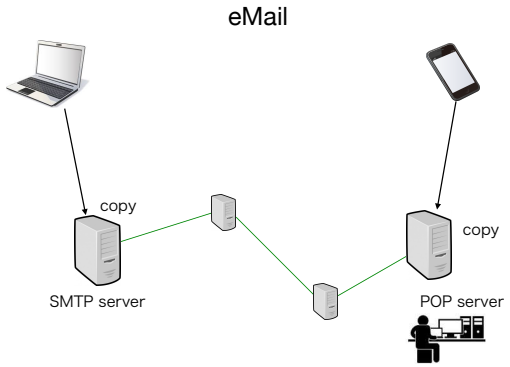
1. **Telephone exchanges have wiretapping capabilities; system requirement**

When someone call you up, All cell towers on the globe emit signal ?
Now almost all young, newly-grad, apprentice reporters can not answer this question. Ask your friends "Fiber-optic internet access is much much faster than mobile phone. Which travels faster, light or radio signal?"
Mobile phones are ALWAYS located by its nature. All telephone exchanges have "taps" for wiretapping. In good old fairytale, FBI is said to stop wiretapping when the phone is picked up by target's family. Now every conversation is recorded in small countries like Afghanistan and Bahrain. I have no idea about Japan but some journalist behave just as they are eavesdropped on.



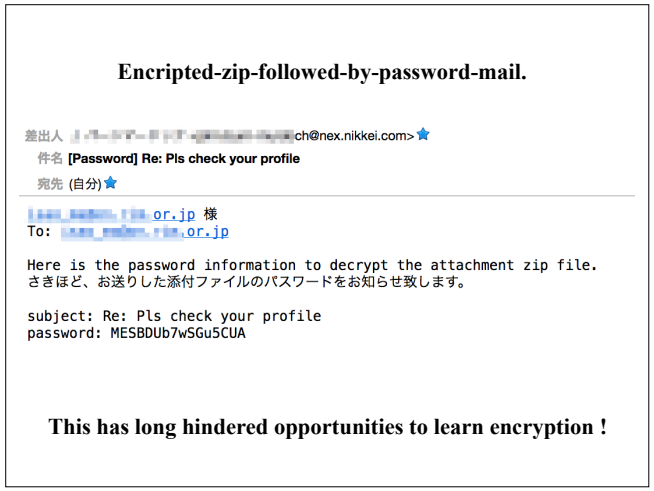
2. anonymous/false name phone + public appearances can spot the targeted device.

It is not secret that metadata of telephones is kept in all countries. In 2011, German Green party politician Malte Spitz sued to have Deutsche Telekom hand over six months of his phone data. ZEIT ONLINE made this map by combining data with his activities that were scraped from the internet. (Some reporters believe in anonymous/corporate name phone. But several public appearances will reveal which device targeted journalist are using.)

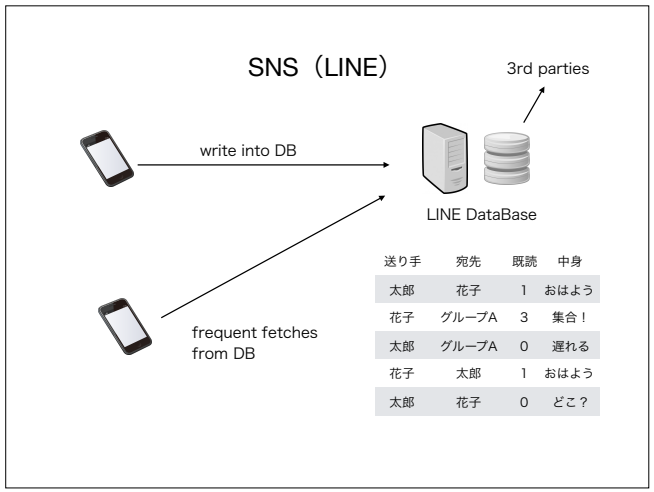


POP server stores plain-text mails, if possible, forever

Many journalist knows how e-mail works but rarely use PGP encryption. Frankly e-mail is the most vulnerable tool for journalists. Once the account is compromised or POP server administrator become evil, all communications will be leaked.

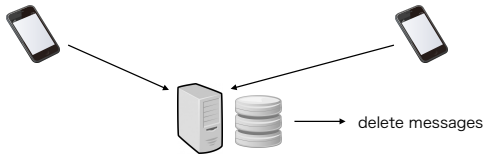


Some news media use this automatic encripted-zip-followed-by-password-mail system. This has long hindered opportunities for journalists to learn encryption. Of course PGP has a weak point; sources must use PGP too and the very existence of communication is not concealed. So I did PGP workshop in Japan, but my focus is not on how to use it but general information around digital security. However, generally speaking, mastering PGP is a good indicator of security-conscious reporters.



Social networks store everything you do on the platform. On Twitter and Line, both popular platforms in Japan, you might feel that you are sending or receiving messages but actually you are writing a message into platform's database and fetching messages very frequently from that database. Nothing is sent from you to your friend directly. When you delete your message, platforms never delete the record but just flagged as deleted. Data is platforms' precious property sold to third parties.

Secure SNS（Signal）



sender	receiver	message
太郎	花子	ITqQRdAAzKnSLX58pw5CqriHFjO6mYAe
花子	太郎	7YPLDW+yHP69BwkcmSRyT6ZPUFrj
太郎	花子	2ENi5X1JmV+AJ9r3cEW286p7JxOj
花子	太郎	F4qB8b1+7tgY+bCxrSze55mZK08b
太郎	花子	X9//jG/WrMFZOM4ZXX136jhx

Signal Database

By the way, so-called “secure” messaging services such as Signal, Telegram, work like this. All messages are encrypted end-to-end. Messages stored in the database are already encrypted so none has incentive to make use of these data. Most recent version of Signal has capability to anonymously send message. In this slide, the column “sender” will become anonymous in the next version.
My advice is simple; use Signal with colleagues / invite your sources to use it.

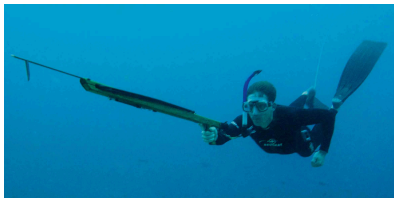
Social Engineering

Never tell someone your password

Manage your PC by yourself !!!

Most journalists, except those covering security, probably don’t know the word, social engineering, nor its meaning either. But it is no exaggeration to day that half of the Japanese reporters had never installed any softwares by himself. Large news organizations have the IT service stations to serve these non-IT guys.
It is said that 85% of data breaches are caused by social engineering. Don’t call IT service station everytime you install something or you need to change something. Try to manage your PC by yourself.

Spear Phishing



Spear phishing is carried out by email or instant messaging to obtain sensitive information such as usernames, passwords. According to Snowden, NSA sent to executive members of OPEC emails with link to computer virus. 80% of their accounts were compromised. Someone sent a direct message to AP social editor and took over the account. He tweeted this fake breaking news when the market was open.

Social Network / IT companies

PRISM

NSA has access to designated user informations from Google, Facebook, Microsoft, Apple, Yahoo, Skype..

Russia — Almost everything is under surveillance

China — TOM-Skype : messages that contains sensitive words are automatically stored.

Social network companies have no intentions to protect user informations from law enforcement agencies. PRISM is the most famous codename Snowden revealed. 9 companies such as Google, Facebook, Microsoft and Apple are offering informations about the users NSA requested. This was treated as a scandal because it was in US. In Russia all activities are under surveillance. TOM-Skype is a special version of Skype for China , made by Microsoft. It is said 30000 humans are monitoring the contents. (In HK this is like teaching fish how to swin)

U.S. Tracking Phones, Google Is a Dragnet for the Police

Tracking Phones, Google Is a Dragnet for the Police

The tech giant records people's locations worldwide. Now, investigators are using it to find suspects and witnesses near crimes, running the risk of snaring the innocent.

By JENNIFER VALENTINO-DeVRIES APRIL 13, 2019

When detectives in a Phoenix suburb arrested a warehouse worker in a murder investigation last December, they credited a new technique with breaking open the case after other leads went cold.

The police told the suspect, Jorge Molina, they had data tracking h phone to the site where a man was shot nine months earlier. They had made the discovery after obtaining a search warrant that required Google to provide information on all devices it recorded near the killing, potentially capturing the whereabouts of anyone ir the area.

捜査ツール実態 闇の中

核心

顧客情報 令状なく取得

検察「思い立ったら照会」

Last April, NY Times published a story about the police detectives using Google's Sensorvault, database of user locations, in their investigations. According to the article, which is follow-up story to another local TV station, Google is asked from investigative agencies as many as 180 requests now. In this case written in the articles, a man who lent his car to the actual killer was wrongly arrested. In Japan, Kyodo News revealed that Japan's prosecutor's office has a list of newly one hundred "cooperative" companies which includes railway, e-cash, telephone operators. It reads inquiries to these companies amounts to several dozens per day. Former prosecutor is quoted "Once new idea occurred in mind, make inquiries immediately." In a sense, they are doing what data journalists do without legal authority.