LET PRIVACY BE THE BRAND
Ho Ming-Syuan
Project Manager
Taiwan Association for Human Rights
Business Model v.s. Human Rights Problems
Human Rights Problems Caused by Data Processing

- Data breach
- Restrict freedom of expression, especially in right to receive and send information
- Algorithm’s discrimination or bias
- Government surveillance & company’s surveillance
- Democracy crisis
Business and human rights

The growing reach and impact of business enterprises have given rise to a debate about the roles and responsibilities of such actors with regard to human rights, and have led to the placement of business and human rights on the UN agenda.

In 2005, the UN Commission on Human Rights adopted resolution E/HRC/RES/2005/3 on Business and Human Rights. This was followed by the UN Guiding Principles on Business and Human Rights in 2011. These principles have been further developed and adapted by the private sector, civil society, and intergovernmental organisations.

Highlights

- OHCHR Accountability and Remedy Project
- ARP I: Judicial Mechanisms
- ARP II: State-based non-judicial mechanisms
Got many good responses, but, is there anything changed?
Why “Privacy”?

Of course, these service providers are reasonable to pay attention on privacy.

But, how about other service provider?

Or, even these service providers will face the problem whether they should protect the privacy.
Privacy has an image problem. Over and over again, regardless of the forum in which it is debated, it is cast as old-fashioned at best and downright harmful at worst — anti-progressive, overly costly, and inimical to the welfare of the body politic. Yet the perception of privacy as antiquated and socially retrograde is wrong.

-- Julie Cohen, 2013, *What is Privacy for?*
Is “privacy” not a social norm anymore?
Some Good Reasons for Company to Respect Privacy
R1: International Society says Company has the Responsibility.
“Guideline” Point 13:

- The responsibility to respect human rights requires that business enterprises:
  - (b) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

“GDPR” Article 25, Article 35: Privacy by design/default, data protection impact assessment.
R2: Easier to Refuse illegitimate Government Surveillance


● Not all Surveillance is legitimate. Sometimes the law is bad, so the surveillance is legal but not legitimate.

● Be partner of illegitimate surveillance would harm companies reputation.

● After Snowden leaks, almost everyone know that company has the capability to be the partner of government surveillance.

● Government would put more pressure to company in the future.
The Pressures Company Faced related to Government Surveillance

- Request company to provide more user’s data
  - to cooperate with more crime investigation
  - to provide more users’ data.
  - to provide more different kinds of data about each user.

- Request company to provide the encryption key

- Request company to provide the “backdoor”
How could Company Fight back?
TRANSPARENCY REPORTING INDEX

Transparency reporting is one of the strongest ways for technology companies to disclose threats to user privacy and free expression. Such reports educate the public about company policies and safeguards against government abuses, and contribute to an understanding of the scope and scale of online surveillance, network disruptions, content removal, and a host of other practices impacting our fundamental rights.

IN 2010
Google released the first transparency report
70 companies have released transparency reports to date
95 countries are covered in all released reports

6900% increase in the number of reports over the past 8 years

... and more regional diversity in transparency reporting
Three Advantages for Making Transparency Report

- Tell the users that company do care about their privacy.
- Make the company accountable.
- The report could become the tool for company to negotiate with government and civil society.
If I can’t see the data, I can’t help you.

End-to-end encryption

End-to-end encryption ensures that a message is turned into a secret message by its original sender, and decoded only by its final recipient. Other forms of encryption may depend on encryption performed by third-parties. That means that those parties have to be trusted with the original text. End-to-end encryption is generally regarded as safer, because it reduces the number of parties who might be able to interfere or break the encryption.
Collaborate with Multi-Stakeholders: GNI as Example

GLOBAL NETWORK INITIATIVE

PROTECTING AND ADVANCING FREEDOM OF EXPRESSION AND PRIVACY IN THE ICT SECTOR

OUR WORK
GNI helps companies respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications.

OUR MEMBERS
We are a growing alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions from around the world.

OUR IMPACT
From advancing accountability to advocating for laws and policies that protect free expression and privacy rights worldwide, our members are working together to get results.
R3: Protect Privacy is not Opponent to Make Profits.

Good practice in protecting privacy could:

- save money in facing unnecessary dispute, unnecessary lawsuit, and high penalties.
- get free advertising from multi-stakeholders, like civil society
- keep the good talented staff
- get good reputation to get more orders.
Thank You

Ho Ming-Syuan

hmsyuan@tahr.org.tw