SECURITY OF COMMUNICATIONS BREAK-OUT SESSION

INTRODUCTION

A small note on why a session on 'security' exists separate from 'online identity' or 'privacy' sessions:

The idea is to understand security aspects of the internet that are more concerned **with managing risks of all kinds**. It is not about privacy – or data protection and management from new privacy invasion- nor is it about forms of identity and anonymity or digital presence. It is about managing the risks to business efficiency and effectiveness, to (critical and non-critical) infrastructures, to financial stability, and to personal security and trust. **Security is about risk management.**

DISCUSSION

I. KEY NEW TECHNOLOGIES & POSSIBLE THREATS

The team tackled two particular examples where security is an issue and through which attempted to answer the key questions challenges to security:

A. EXAMPLE ONE: CLOUDS AND SECURITY

While cloud computing could provide access to great resources, they raise concerns about the risks they could put users and societies under. Clouds provide their customers with instant access to large-scale data storage and processing facilities. But **what type of risks do clouds pose: to society, to individuals and to businesses?**

1. **What if cloud providers or their customers were malicious? For instance:**
   - because they have been compromised by criminals?
   - because they are criminals?
   - because they don't care about some potential threats?

2. **Possible Threats**
   - DDoS attack using a public cloud (possibly procured using stolen credit card details)
   - The mobile (in IP space) casino, child pornography site, phishing site, etc.

   For instance, someone renting a cloud with a stolen credit card, or using a cloud to create a virtual casino to evade taxing. Can pornography or fishing sites be moved around using clouds?

B. Example Two: Sensor Networks and Security

Another example of security potential risks is sensor networks. They can be used in services that expand from traffic management and health warnings to advice on best routes for cyclists. Reusable sensor networks can enable applications such as:

- pollution monitoring and environmental management
- public safety and emergency response management
- traffic monitoring and optimization, etc

1. **But what if a malicious agent could spoof the sensor data?**

2. **Possible threats**
   - farmer corrupts humidity sensors to increase the irrigation of his fields
   - faking a traffic jam to divert customers from a rival store
   - terrorist corrupts humidity sensors to reduce irrigation and kill crops

These are all security threats (as opposed to privacy or identity issues). So **how can we block these potential abuses?**

C. Typical Non-Technical Issues

We are concerned with the **non-technical** questions, issues and challenges around clouds:

1. **Who is (or should be) <u>responsible</u> for meeting clouds security threats?**

   - The operator of the cloud or sensor network?
   - The developer of applications that use them?
   - The customer for those applications?
   - The bystanders affected by them? (e.g. the victims)
   - Social agents (e.g. police, social networks, etc)?

2. **Socio-economics of <u>risk management</u>**

   And in such cases, how can responsibility be imposed? Do you impose responsibility by regulations, or self-regulations or market forces? There is no easy way. There are major concerns of what could happen if you impose responsibility to protect from security risks. One extreme scenario could be that the cloud provider becomes the key party responsible for the cloud. This could have serious implications on the degree of freedom users could have. In contrast, the implications of not having any regulations could lead to risks of outlawing part of the innovation.

   - Will the responsibility and potential liability deter anyone from offering innovative future Internet services?
   - Will the potential impact lead society to outlaw them?

   There are no easy and general solutions. But starting with getting all parties involved together and bringing them to understand the risks involved is the first step.

II. TECHNOLOGY DEVELOPMENT AND CHALLENGES

Some of the key legal, technical and financial challenges raised by team:

i. LEGAL

The first question to ask is who should be responsible for providing counter-measures in case the clouds are being misused?

Option 1 (users): It could be through convincing the users to install malware, the attack in such case can be scaled up very quickly. **Does that mean people must have a driving licence before using a cloud? If we needed a license for owning a PC, that would have stopped the PC market, but now what do we do with owning a cloud given the risks involved?**

The users' ability can vary, and there could be so many ways into a cloud or a sensor network. Most of the protective measures can be putting precautions to the users to take. But because there are so many ways, some attacks would always work.

Option 2 (Service Operators): **Another scenario is to ask service operators to do a cloud isolation of suspected users.** If the cloud provider has a hacker or password cracker, can the cloud provider take responsibility to prevent the attack from happening? If for instance, suddenly one user is using the cloud very strangely and it turns out a hacker is using their stolen credit details. **The cloud provider, in principle, could detect abnormality; but should they have a responsibility to protect the user?** The cloud provider has to make that choice for the user.

Another question was: does the cloud provider want to have any responsibility for what they do?

The issue of variations of legal measures between countries was particularly raised. In Italy, for instance, the law was putting liability on the service provider of Youtube- Google. You would have the same problem with clouds. If the service providers are not using measures that match the laws in the countries they are operating in, it might be discouraging for them to work altogether in that country. At the moment no cloud providers accept responsibility.

ii. TECHNICAL/NON-TECHNICAL

It is difficult to really discuss security risks without a scenario. Perhaps we should start with the assumption that sensors are mis-configured on purpose, then, we can deduct a number of consequences and scenarios.

Technically it is possible to detect a cloud abnormality but it is not that straightforward. The outbound and inbound traffic may have statistical information that can ensure that the user is not behaving differently compared to the past. In such case, it would be possible for Cloud providers to use the 'credit limit' of the user as a way to stop any abnormal behavior. However, it would not be possible to detect the scale (except for password cracking). But what if users don't have a long history? Also, typically, if someone wants to do something wrong with the cloud, they will not be planning to stay for long - they would quickly do something to the system, then, move out. So how can we technically address these behavioral differences?

The issue of protecting the Data was raised as another challenge. When we look at the security challenges, we are – by defaults- getting in the problem of data protection. If we cannot protect the data how can we guarantee that the services can be protected?

Moreover, the service operator might have a mechanism for detecting a micro hotspot, to detect when something is hot (e.g. a data fusion system); but then someone could use the data from this network to advise a GP on what to expect with their surgery the following morning. It brings a new challenge dimension of how the data can impact others - or conversely - how the sensors corruption risks should be managed.

Security can be addressed through technical needs, but the harder rising challenges are the socio-economic: how does it affect the obligations of those who didn't expect to be supporting these services?

Example: In India , there are sensing networks that measure humidity of the field. If you were a farmer would you be able to use this and would it increase your crops? It really depends on whether you will use it for agriculture, finance..etc? And what if someone goes there and changes something? How will it affect the farmers business?

One suggested solution was having a **multiplication of sensors to avoid misinterpretation of one sensor** (e.g. if one gets attacked, the effect will be annulled by the total number). But the economic implication is important to consider. Having one hundred sensors is more costly than having just one. We also have to have a number of different monitoring points.

iii. Capacity to access risk expertise & to manage risk

The cloud provider has a team of security analysts or Information security analysts, and large corporations employ large defense companies. You have to have a team of legal, security, technical experts. If you are developing the technology, you ought to be the expert already.

However, **not everyone has access to risk experts or to cope with security threats**. Most medium and small scale companies cannot afford to hire technical risk analysts (on top of lawyers and other experts). Similarly, home users just trust the information they are given. The user wouldn't hire a technical expert to analyze the risk situation at home. What will they do? Shall they just trust the information they get?

Another issue is the **lack of human capacity to handle all monitored detections.** The example of Swiss banks and money laundry detection was given as a similar case to Clouds fraud detection. The bank created a system for detecting money laundry potential frauds. Within the first few days, thousands of cases were detected by the system but nobody had the resources to look at them. The speed and volume of data can cause a challenge to manage.

The issue of providing technical advice as part of the service provision of clouds was also raised. Swiss com offered a security package for a fee to its customers, in which many people subscribed. But users ended up having merely software updates to ensure security. **For some kind of stakeholders, it might be a solution to just have an add-on security feature.** But for bigger operations like a company or universities, getting technical expertise from the service provider would be difficult.

III. Strategies to bridge gap & potential solutions

A. Policy makers: change the regulatory framework

One possible strategy is to allow policy makers to anticipate what could go wrong and analyze frameworks of detection. This is the same way Bank systems detect money laundry. It would only work if you have a mechanism of anomaly detection. But there are certain issues worth considering:

1. **Where there is a risk, could one impose an obligation on (say) service providers – similar to Anti-Money Laundering regulations?**

- The problem with legislation as a solution is that cloud providers might not operate in that country, and different countries have different laws. Also even though they have to comply with existing EU legislatives on handling storage, privacy.. etc the nature of the cloud bring new risks.
- Many SMEs are thinking to move their regular jobs into a cloud. For a smaller company it might be better NOT to have many policies and regulations. Often regulations move into a direction at least five years later after the technology has been invented.
- You could regulate, but on the other hand, you have got to deal with the possibility that it might be going on all the time. And you should be ready for the risks, and that this could create a huge amount of work.
- **You can make service providers manage the risks.** Customers need to trust the cloud provider, but if users feel they are closely monitored, they might not feel comfortable with the service. We have to be careful about what can or can be detected.

2. We need to **keep up with the technical developments (and monitoring it) but not be ahead of it**. And we need to **avoid creating new problems** or unexpected side effects by technology. Like in the case of the Swiss bank attempt to detect money laundry cases, the system showed thousands of small cases that they did not have the capacity to monitor.

B. LEGAL AND TECHNICAL ANALYSTS, OR FORUMS LIKE CSA

1. One solution could be bringing technical and legal analysts to understand risks and assess new risks. We can only address risks within the current framework– assessing new risks is always harder. Also, not everyone has access to risk experts. **You need more than just a lawyer, but someone who can understand the technical aspect of it** at a higher threshold of the game.

2. Service providers' technical assistance could be one solution, but can it be enough? Currently, the best thing that could be provided is a set of best practices and guidelines shared with users.

C. Market forces: will customers reject services that are bad for society?

One possible solution would be to leave the security to the market: customers may not use services that they find too risky. But the example of *laissez-faire* of a total free market style, like what happened with the financial crisis, cannot be enough to manage security risks. There should be some regulations and rules informing the market. One simple approach could **be to force cloud service providers to publish statistics about the health of their activities and their monthly attacks**. To that, it could be checked by a government authority or a third party.

1. **Would providers publish data on this (or could they be forced to)?** Incentives could also be given to service providers to publish periodically health reports.
2. But since security is very sensitive information, service providers might not be willing to reveal those data so as not to lose customers (similar to the way Banks hiding their cases of money laundry). **We therefore need metrics for comparison of 'trustworthiness'** and of the anti-risk health. **They must be** publically available to allow users to compare between service providers.
3. Some auditing standards must also be established, to ensure that what service providers published is credible.
4. **It is also possible to allow a community of users – who are not the police or regulators or individual customers but networks with common interests - to help work together to monitor services and improve the cloud systems. This is through enabling platforms for peer to peer interaction.**
5. **Are there any risk analysis models that cloud operators use?** Service providers probably have some but they also must look at the integrity of their network – and what it can do. But they might not look at the risk they might run as a result of exploiting their customers. You can analyze their risks for them, but as soon as you do that, you expand your scope and add to your cost of analysis.