

Social media

Terry Yin

November 23, 2014

We wouldn't call the internal communication applications within a company "social media". For example, if a company uses Microsoft Lync as their internal point-to-point communication tool, and uses wiki as internal information sharing tool, we won't call them social medias. Social media is based on the Web2.0 technology, but it has an emphasize on a virtual community [Wikipedia \(2014b\)](#). In the physical communities, or the society, laws and regulations have been formed and evolved for centuries. But the virtual community enabled by the new technology is still new. Although it's still a community formed by humans, but because of the technology there are quite a lot of differences. Some of the differences are never expected by the humans before.

Before we explore the responsibilities of the security of the social media providers and users, we need to define what does it mean to be secure. In The Universal Declaration of Human Rights [Lauterpacht \(1948\)](#), I found these articles:

Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 19

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 22

Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.

1 Security Challenges of Social Media

1.1 Privacy

The privacy could belong to the person him/herself, other people, or the entity like a company. It's important to protect the privacy in social media.

1.1.1 Provider

Social media provider is responsible for protecting the privacy of the media participants. From technology perspective, social media provider is responsible for trying their best to eliminate the risk of leaking privacy, from the root. From the root, there are several layers they can do (from the best to worse):

- **Do not collect it.** If social media don't collect private information, then the private information will not leak because of the media itself.
- **Do not keep it.** If they collected the information, but don't keep it anywhere, nobody can get it in the future.
- **Do not keep it too long.** If they have to keep the information, then don't keep it too long. Technically, breaking any protected information is just a matter of time.
- **Keep it with strong protection.** And let the users know about their risks.

1.1.2 User

First, user need to know what is his/her privacy. There are also a few layers a user could achieve:

- Do not share
- Share with trusted device & connection
- Share with trusted application
- Share with trusted group

1.2 Abusing

Just like what happened in a real-world community, there are people with bad wills and abusing the social media. One way of abusing the social media is Social engineering. Social engineering means to psychological manipulate people to perform some actions. In social media, since it's easy to collect people's information and interact with them, social engineering is very common.

1.2.1 Provider

- Detect social engineering [Wikipedia \(2014a\)](#).
- Prevent non-human participants.

1.2.2 User

- Protect your account. Because when your account is compromised, it can be used to harm you, and also can be used to harm the others.
- Don't forget the link between the information you share. For instance, if you shared somewhere than you have a daughter and then shared somewhere else a picture of yourself with a young girl in the background, they people could guess that she's your daughter and use that information.

1.3 Social Responsibility

Another area of social media security is the society security and national security. This is an area beyond my knowledge. One man's hero is another man's villain. What role could social media play in society movement? We can see that social media led up to the uprising of "Arab Spring". And it's also debateable that the government like the US and NGOs has been supporting social media to do so [Ghannam \(2011\)](#). There are also nations that block their people to access the social media outside their nation. Users in those nations need to learn technology to bypass the blocking. To be honest, I have a hard time distinguishing thing we have to do, can do, should do, and should sometimes do in terms of social media from both provider's and user's perspective.

2 Conclusion

Social media is a new media. It has a lot of things in common with traditional media. Most of the traditional values and laws of media is also applicable to these new medias. Because of the technology, social media also brought many new challenges in the area of security than traditional media. Both the social media providers and users need to explore and learn how to protect their right.

References

- Ghannam, J. (2011), ‘Social media in the arab world: Leading up to the uprisings of 2011’, *Center for International Media Assistance* **3**.
- Lauterpacht, H. (1948), ‘Universal declaration of human rights, the’, *Brit. YB Int’l L.* **25**, 354.
- Wikipedia (2014a), ‘Social engineering (security) — wikipedia, the free encyclopedia’. [Online; accessed 21-November-2014].
URL: [http://en.wikipedia.org/w/index.php?title=Social_engineering_\(security\)&oldid=633431682](http://en.wikipedia.org/w/index.php?title=Social_engineering_(security)&oldid=633431682)
- Wikipedia (2014b), ‘Social media — wikipedia, the free encyclopedia’. [Online; accessed 21-November-2014].
URL: http://en.wikipedia.org/w/index.php?title=Social_media&oldid=634769950