

## Case Study

+

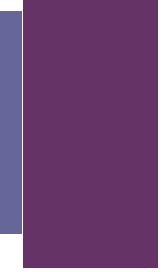
## Case Study 1- Wikileaks

Chapter 3: Ethics and Privacy:  
Page 73

*(from the recommended textbook)*



# + Questions



Think about the following questions before you read the case study.

- What are the underlying issue
- How can governments, organisations and even individuals prevent future disclosures? Is it possible to accomplish this task?
- Are the actions of wikileaks ethical?
- Should the general public have access to sensitive information? Why (not)?



## Case of WikiLeaks

WikiLeaks ([www.wikileaks.org](http://www.wikileaks.org)) was officially unveiled in December 2006. Julian Assange, one of the founders, was reportedly inspired by the leak of the Pentagon Papers. Assange intended WikiLeaks to serve as a dropbox for anyone, anywhere, who disagreed with any organization's activities or secrets. According to its Web site, WikiLeaks focuses on material of ethical, political, and historical significance. In its first year, the organization's database expanded to millions of documents. WikiLeaks continues to receive many new documents every day. Since its inception, WikiLeaks has had significant impacts on both businesses and governments. We discuss several examples below.

In January 2008, WikiLeaks posted documents alleging that the Swiss bank Julius Baer ([www.juliusbaer.com](http://www.juliusbaer.com)) hid its clients' profits from even the Swiss government by concealing them in what seemed to be shell companies in the Cayman Islands. The bank filed a lawsuit against WikiLeaks for publishing data that it claimed had been stolen from its clients. Baer later dropped the lawsuit—but only after generating embarrassing publicity for itself.

In October 2008, Iceland's Kaupthing Bank collapsed, saddling the country with \$128 billion in debts. Ten months later, Bogi Agustsson, the anchor for Icelandic national broadcaster RUV, appeared on the evening news and explained that a legal injunction had prevented the station from airing an exposé on the bank. Viewers who wanted to view the material, he suggested, should visit WikiLeaks. People who took Agustsson's advice found a summary of Kaupthing's

loans posted on the Web site, detailing more than \$6 billion funneled from the bank to its owners and companies they owned, often supported with little or no collateral. WikiLeaks promptly became a household name in Iceland.

The following year, WikiLeaks published documents generated by a pharmaceutical trade group implying that its lobbyists were receiving confidential documents from, and exerting influence over, a World Health Organization (WHO) project to fund drug research in the developing world. The resulting attention helped to terminate the project.

In September 2009, commodities company Trafigura ([www.trafigura.com](http://www.trafigura.com)) requested an injunction from the courts to prevent the British media from mentioning a damaging internal report. The report indicated that the company had dumped tons of toxic waste in the Ivory Coast that sickened 100,000 local inhabitants. Although Trafigura could prevent the official media from reporting this story, it could not stop WikiLeaks from publishing the information. The public became aware of the transgression, and Trafigura eventually had to pay out more than \$200 million in settlements to Ivory Coast victims of the toxic waste.

As consequential as these business leaks were, probably the most controversial WikiLeaks exposé involved the U.S. government. From November 2009 to April 2010, U.S. Army Private First Class Bradley Manning downloaded hundreds of thousands of diplomatic cables to a CD at an outpost in Iraq. He then passed the information to WikiLeaks. In doing so, Manning violated U.S. Code Section 1030(a)(1), which criminalizes unauthorized computer downloads.

Beginning on November 28, 2010, WikiLeaks published the contents of more than 250,000 diplomatic cables, the largest unauthorized release of contemporary classified information in history. Among these cables were 11,000 documents marked “secret.” The U.S. government’s definition of a secret document is one that, if released, would cause “serious damage to national security.”



Diplomatic flaps quickly ensued. For example, North Korean leader Kim Jong Il learned that China would consider supporting the unification of the peninsula under the leadership of the South Korean government. Similarly, Iranian President Mahmoud Ahmadinejad discovered that his Arab neighbors were pleading with the United States to launch an attack against Tehran's nuclear program.

Not surprisingly, the release of the cables also had wide-ranging repercussions within the United States. The government ordered a clampdown on intelligence sharing between agencies, and it established new measures to control electronically stored documents. U.S. Secretary of State Hilary Clinton charged that the massive cable leak "puts people's lives in danger, threatens national security, and undermines our efforts to work with other countries to solve shared problems." From the opposite perspective, many individuals and groups, including Daniel Ellsberg, supported WikiLeaks' actions.

Wikileaks' activities continue. In July 2010, WikiLeaks released the Afghan War Diary, a compilation of more than 76,000 documents about the War in Afghanistan not previously available to the public. During April 2011, WikiLeaks began publishing secret files relating to prisoners detained in the Guantanamo Bay detention facility. On July 5, 2012, WikiLeaks began publishing the Syria files, more than 2 million e-mails from Syrian political figures, ministries, and associated companies, dating from August 2006 to March 2012. On October 25, 2012, WikiLeaks began publishing The Detainee Policies, which contain classified or otherwise restricted files from the U.S. Department of Defense that discuss the rules and procedures for detainees in U.S. military custody.

+

Case Study 2 -  
Can anyone succeed with local  
online advertising?

Chapter 9: Social Computing

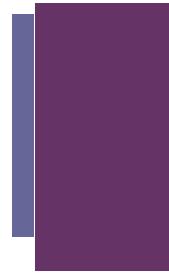
Page 310

(from the recommended textbook )



# + Questions

Think about the following questions before you read the case study.



What are the underlying issue

What can local businesses do?

How can social media tools help?

Do Google and Facebook offer anything that can be used by such local businesses?



## Case of Local Online advertising

Local businesses buy online ads. In fact, in 2012 local businesses spent \$19 billion on local advertising. Experts maintain that the local advertising business is potentially much larger, with estimates ranging from \$90 billion to \$130 billion. So, there is room for a great deal of growth in this area. Online businesses (e.g., Facebook, Google, Groupon, and LivingSocial), however, have traditionally not been profitable in local advertising. In addition, users of these Web sites typically access them via mobile devices, which are not “friendly”

# + Solution

Yelp was founded in 2004 primarily to help people connect with great local businesses. The Web site is like a large online bulletin board featuring user-generated content. The content consists of personal reviews based on experiences at local businesses. Yelp members are “in charge” as far as sharing, reviewing, and communicating is concerned. The main benefit of Yelp is the ease of communication that Yelpers experience. The site is like word-of-mouth for the digital world.

To write reviews or follow Yelp users, you must first sign up by creating a profile.

Yelp’s service is free for consumers, but local businesses pay to advertise on the site and to add premium features to their Yelp pages. The founders initially focused on establishing the service in a single city, namely, San Francisco. They then replicated their success in other cities including Chicago, Boston, and New York.

Yelp differentiated itself from other social networking companies by hiring a sales force, which eventually grew to 500 people. The company adopted this strategy because they learned that small businesses depended on salespeople with whom they had developed a relationship.

Yelp established a loyal consumer following, due in large part to the fact that the company is vigilant in protecting consumers from suspect content. The company developed an automated review filter to identify suspicious content and minimize exposure to the consumers. Yelp’s review algorithm assigns each establishment an average star ranking, and it filters out less-experienced contributors. The site also features a wide range of other features (lists, special offers, and events) that help people discover new businesses and communicate with one another.

Yelp then incorporated its reviews into Apple’s Maps app (the one that replaced Google Maps). Consequently, the hundreds of millions of iPhone and iPad owners who use Maps are now Yelp users. Yelp’s stand-alone apps, which attract 7 million users a month and are among the most popular free downloads in the Apple and Android stores, are now responsible for 40 percent of Yelp’s searches.

+

# Case Study 3 - Case of Google Glass

## Chapter 3: Ethics and Privacy

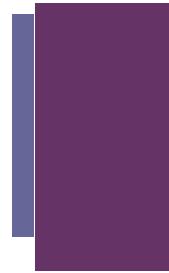
Page 84

(from the recommended textbook )



# + Questions

Think about the following questions before you read the case study.



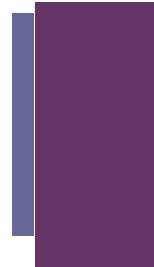
What are the underlying issues

Do you feel the functionality offered by Google glass outweighs the potential loss of privacy that the technology affords?

Would you use Google Glasses?

If you were at a bar would you be comfortable speaking to someone wearing Google Glasses?

+



Google Glass is an augmented-reality, wearable computer with a head-mounted display. The glasses display information in a hands-free, smartphone-type format, and they can interact with the Internet via natural language voice commands. The device receives data through Wi-Fi, and it contains a GPS chip (global positioning system). (We discuss Wi-Fi and GPS in Chapter 8.) Users issue voice commands by first saying “OK glass” followed by the command. Alternatively, they can use their finger to scroll through the options located along the side of the device. Google Glass can record video, take pictures, start Google+ hangout, perform search, translate, perform facial recognition, provide directions, answer queries, use Google Now, and send a message. Essentially, these glasses can instantly capture and store every movement of every individual around the person wearing them.

Consider these questions relating to the privacy implications of Google Glass. What if someone around you who is wearing Google Glass records you on video or takes your picture and you don't even know he or she is doing it? Or, suppose you are being recorded during a business meeting at lunch? Can a child properly consent to being recorded? Is an adult who happens to be visible in the camera's peripheral vision in a bar consenting? Would you like a stranger to be able to automatically identify you with the glasses' facial recognition feature? These are only a few of the questions regarding the privacy concerns associated with Google Glass.



## Case of Google glass?

Perhaps the most fundamental questions are: Who owns the data generated by Google Glass? Who receives these data? What happens to them after they are captured? Presumably the data flow to Google, where they are analyzed to provide more personalized search results as well as more targeted advertising. After all, advertising is a significant source of revenue for Google. Imagine that you are wearing Google Glasses and, whenever you look at something—a shirt, for example—a special offer for that shirt pops up on your glasses. For many people, that would be simply too intrusive.

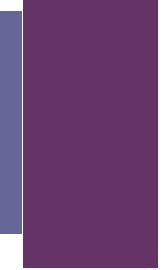
Some analysts contend that we are too worried over the privacy implications of Google Glass. They note that our courts have outlined a definition of “reasonable expectation of privacy.” If we reach a point where our surveillance technology is intrusive to a degree that everyone finds exploitative, then concerned parties

+

## Case Study 4 - Social giants slam bullying laws proposed by Australian government



# + Questions



Think about the following questions before you read the case study.

What are the underlying issues?

Can social networking websites implement such a law as described in the article?

Why(not)?

How can cyber bullying be prevented?

# Social giants slam bullying law

Digital giants Facebook, Twitter and Google have united to reject an Abbott government proposal that would force social media companies to remove content deemed harmful to young people.

The government has proposed appointing a children's e-safety commissioner with the power to force sites to take down posts containing bullying or harassment -an idea backed by child psychologists and family groups. The government is also considering creating a new Commonwealth cyber-bullying offence.

The Australian Interactive Media Industry Association - representing the major social media companies - says the proposal is too cumbersome and would not cover popular messaging services such as Snapchat and Kik.

NSW Police recently described Kik, a texting app that allows people to connect with strangers, as "the number one social media problem involving teenagers".

"A policy that clamps down heavily on the things that young people can say to each other on larger responsible sites has potential to drive young people to engage in risk-taking behaviour on services that have less well-developed protections in place and are not covered by the legislated scheme," the association said in its submission to the government.

# Social giants slam bullying law

"Given the government's commitment to de-regulation and reduction in red tape and lack of evidence that existing mechanisms are not operating as intended, we respectfully submit that the government should reconsider the proposal to introduce legislation to take down content and rather work to extend [existing protocols] to apply to more services."

Facebook argues the definition of harmful content is too broad and could be used to target, for example, photos of children "planking" with their friends.

"Rather than enhance the online safety of young people, the scheme has potential to legislate intergenerational conflict rather than encouraging conversations between parents and young people," Facebook said in a separate submission.

The free market Institute of Public Affairs think tank opposed the proposal on free speech grounds.

The Parliamentary Secretary for Communications, Paul Fletcher, has repeatedly said the current system of self-regulation was not sufficient to protect children against online bullying.

"[If] you're a child who is a victim of cyber-bullying, or a parent or a teacher wanting to assist that child, if the site doesn't respond when you notify a concern, you really have no redress at all," he said last month.