What Happened to Privacy?

Joseph Sarko

Kent State University

06 November 2014

In our current day and time, technology is ubiquitous and almost inescapable. Even for individuals who are laggards of technology, they are still exposed to it and reap and carry the benefits, and also the disadvantages associated with them. Privacy has always been important for people, and in a day and age when staying low key and keeping your actions covert is at a high, the difficulty in actually doing so remains high as well, and in some areas parallels with an individual's use of technological devices.

Over the next few pages I will compare and contrast the recent advancements of technology in society and their shared advantages and disadvantages and then look at the group Anonymous, who has over the last few years been at the center of several high profile hacks and what it is they are trying to accomplish. Finally, I will examine the process of data mining and what it means for my internet privacy.

Anonymity is defined by nightline as, "the ability to not leave footprints." (Koppel, T. 2002) However, when you leave invisible breadcrumbs everywhere you go, physically and virtually, is that really possible? Technology is providing society with outstanding benefits to public safety and law and order. For instance, a bank's ATM camera lead investigators to a key suspect in the 9/11 attacks, and a camera on an apartment building spotted the truck Timothy McVeigh used to detonate a bomb in front of a federal building in Oklahoma City. When San Diego implemented traffic cameras to monitor people running red lights, they saw a forty percent decrease in violations, and brought in around three million dollars of revenue to the city (Koppel, T. 2002). With technology at a price point too where security systems and deterrents are so affordable establishments really have no excuse to not be using them, they are quickly becoming a detective's best friend in bringing criminals to justice. More likely than not, if a business is robbed and it doesn't have surveillance systems in place, one or more buildings in the immediate

vicinity most likely will. Tampa Bay, Florida is actively working on a network of cameras throughout the city that takes a snapshot of your face and cross references it with a criminal database to determine if you have been arrested before, or if there are outstanding warrants for your arrest (Koppel, T. 2002). This gives law enforcement a powerful new arsenal of tools at their disposal to help ward off would be wrong doers, but also to catch criminals in or after the act, but what is the personal cost of privacy associated with these technological advancements?

Technologies that help keep the peace and lower crime rates look and perform well on paper but not always have the public support implementers would like to see. The reason for this is the fine line that is being crossed between police surveillance, and personal privacy. When media outlets learned of Tampa bay's surveillance network, it was immediately compared to the system put in place in Prague by its communist government years earlier (Koppel, T. 2002). Having a network of cameras could potentially catch criminals and prevent crime, but constantly being watched and your every move monitored is making people uneasy. Plenty of other systems too that have been put in place to come at a privacy cost. The traffic cams installed in San Diego carried the risk of ticketing the owner of a vehicle who may not have even been driving the car. Even worse, as Dick Armey pointed out, if an individual lends a friend his vehicle while he is on vacation and gets ticketed through the system, there's a chance he could miss his court date and be placed in contempt of court all with him being completely unaware (Koppel, T. 2002). Oversights such as this are a potential risk to innocent Americans and could severely impact their life if a victim. There has even been a lot of privacy concerns regarding Google, and how their search engine handles requests. As was demonstrated in the video, "Google is watching you", every keystroke entered into Google's instant search results in a request being sent to Google's servers, even if nothing is actually searched. The issue here is the as explained in the video, if a

high profile figure were to type something illicit into Google's search box, even if in incognito, the request is still stored on their servers, attached to that individuals device, and can be used against them (Knowledge In It's Purest Form, 2011).

In recent years, a hacking and activist entity known as Anonymous has emerged comprised of loosely connected individuals from all over the world with different goals and philosophies that stand up for what they want, some are in it for entertainment, and some are in it to bring about a change in the world (Anonymous, 2012). For a group with no central leadership or direction, it can be difficult to gauge the motives and intents of a group that operate as individuals for different causes united under one name, "Anonymous". However, through a series of publicity stunts and video releases, a large part of the group can be attributed to trying to reveal corruption and lies in the society around us (MrDoxAnonymous, 2012). In some ways they have brought about a lot of good in the world, and despite a lot of negative attention putting them even on the same pedestal as terrorists I feel the organization as a whole has a just nature guiding their every move. For instance, one of the biggest events to put Anonymous on the map in Ohio was the group bringing the football players who raped a girl in Steubenville, Ohio to justice. They were able to hack into and release incriminating evidence that linked players to the incident (Love, D. 2013). Earlier in 2011 they lead attacks against elusive child pornography websites, resulting in many of them being put out of business (Love, D. 2013). The group also points out in some attacks just how easy it can be to release personal information, highlighting company's security holes.

This brings me to an increasing issue of online privacy and companies that exist solely to seek out our personal info, compile it, and then sell it. In the video, "Invasion of the data snatchers", shows just how easy it is becoming for information brokers to gather personal data

online, organize it, and attach it to your name. This information comes from locations we may not even think to delete, such as profile data on apps, or information we thought was private on social media accounts (Reputationcom, 2011). Speaking of social media accounts, I was unaware that even though my privacy at home on my personal computer and on Facebook may be airtight, I could still be at risk if my friends security settings are less than desirable or if one of my friends simple wants to distribute content on my profile without my knowledge, as there really is nothing stopping them, and this was excellently showcased in the video, “Do you really have a private life online?”(Friendly Screens, 2011). After all these privacy holes in many of the apps and websites I use have been brought to my attention, I’m starting to rethink a lot of my social accounts and just what I have posted previously and especially what I will post in the future. This is my final semester of college and it would be a shame if I were to miss out on a job opportunity because I was careless with my online reputation and identity.

References

Anonymous. (2012, January 18). Who is Anonymous? [Video File]. Retrieved from https://www.youtube.com/watch?v=BUuCjPN93vo

Friendly Screens. (2011, February 24). Do you really have a private life online? (social network privacy loss due to friends) [Video File]. Retrieved from https://www.youtube.com/watch?v=-e98hxHZiTg

Koppel, T., Donvan, J., ABC News., & Films for the Humanities & Sciences (Firm). (2002). Whatever happened to privacy?. (Digital video collection.) Princeton, N.J: Films for the Humanities & Sciences.

Knowledge In It's Purest Form. (2010, August 29). Google is Watching You [Video File]. Retrieved from https://www.youtube.com/watch?v=wbBDQgFNoqw

Love, D. (2013, April 27). 8 Things That Anonymous, The Hacker 'Terrorist' Group, Has Done For Good. Retrieved from http://www.businessinsider.com/good-hacks-by-anonymous-2013-4?op=1

MrDoxAnonymous. (2012, December 27). Anonymous 2013[Video File]. Retrieved from https://www.youtube.com/watch?v=a4JRKPljG3Y

Reputationcom. (2011, March 17). Invasion of the Data Snatchers: How to Protect Your Online Privacy [Video File]. Retrieved from https://www.youtube.com/watch?v=ceGdmZ_LLfg