"I'll Be Watching You…."

Allison R. Deming

School of Information Studies/Syracuse University

IST 618: Information Policy

Professor Paul Gandel

November 22, 2022

"I'll Be Watching You…."

The last line is from a viral song released in 1983 by *The Police* called "*I'll Be Watching You*." Looking at the lyrics today compared to 1983, there is a sinister view of this ballad. In detail, it describes a man who has lost a relationship but seems to have some ownership over her. He explains how he will follow her every move, her new relationships when she lies, and even when she prays. Toward the end, he sings what we all feel, that he is obsessed with her and she belongs with him (according to him). While I wonder if this song would be received in the same way it was in 1983 was it was released contemporaneously, at the time, it spent a reasonable amount of time first on the Billboard Charts (even longer in Canada). The song won two Grammy awards (nominated for three), including *Song of the Year*. Back in the 1980s, it was much harder to do what this song describes: to keep tabs on someone at all times. Whereas today, with the right technological skills or access, many people can follow your every move without you knowing it is happening—this lack of knowledge through applications on cell phones and the cell phones themselves. While stalking became criminal in states in the late 1990s once it became known that many of these situations ended up in murder. This realization happened after a long string of police reports, restraining orders, and a sense of ownership of the relationship combined with the stalking. This sense and the actions involved make for murder in slow motion, whether or not it results in death.

Freed et al. (2019) found that 31 survivors of Intimate Partner Violence (IPV) had many vulnerabilities on their phones that exposed them to tracking and hacking with relative ease. This vulnerability led IPV survivors to a lack of comfort when interacting with technology, and it was not just cell phones. Trauma survivors were uncomfortable at work with their computers, email, and other machines they needed to use to keep their jobs. Additionally, malware, viruses,

straight-up geospatial tracking, and keystroke monitoring programs were found to be installed on computers in this and a second study by Leitão (2019) but expanded to devices such as Alexa, Siri, Home Security Systems, and other home-based technologies. I believe everyone has the right to feel safe in their homes.

Pritchard, T. (2021) wrote an article about the new Apple Air Tags and how people use them. Specifically, they are used at an alarming rate for stalking. Young women, and sometimes men, have found an Air Tag "following them" via their vehicles. The low cost of these items and easy trackability (All you need is an iPhone, which most people have). The idea is to keep track of objects, such as your pets or keys to your car, if you are prone to using them. I even know people who use them to track their children's backpacks, where they have a sense of security knowing where their child is at all times. A particularly frightening story from the Pritchard (2021) article details that Apple's new prevention program worked for a woman who had a tracker placed on her person at Disney World around 11:45 PM until 2:00 AM when the Find My Application by Apple alerted her to the item's presence. In my opinion, this is overly long. Notifications within five to ten minutes might be annoying for someone using a new device, but they could also save lives. Many women and men who are stalked experience IPV, and the most challenging time in the relationship are when the abused partner tries to leave. Once they get away, they are at risk, mainly if the abuser can track their every move.

According to Valentino-DeVries (2018), there are more than 200 applications that people can use to stalk someone. The article points out that 27% of women and 11% of men experience stalking at some point in their lives. These numbers are pretty high when there are applications someone may never know about readily available to put on their phone (Valentino-DeVries, 2018). Additionally, there is no Federal Law against doing so, which I hope has changed in the

past four years. There are applications made to track SMS messages on someone's phone. All you need is access to the person's phone for a short time to install and hide the application. Then, it will send all the text messages to the third party it is set up to send.

While not criminal in any way currently, many of us sign away our rights to access the applications we need to use our phones in everyday life. We sacrifice security for convenience, often failing to read or skim the user agreement. However, as quoted in the asynchronous material, I do not believe that the need for convenience in this hectic world disentitles us to privacy and comfort. Those who are more technologically savvy may be able to turn off the tracking services, but this disallows the use of many popular applications. These include but are not limited to Google Maps, Find My, FamilySafe, Life 360, Glympse Location Share, Android/Sprint Family Tracker, and object and car trackers (Unknown, 2021). I have two of these on my cats, one on my car, and a Smart Home. These programs and endless others can allow other family location programs that help you always know where your children are, and the same is said for anyone you are close enough to share. These voluntary applications install through user download or, in some cases, parents of the device user.

Even though this technology is scary in many circumstances, I believe that when used correctly and for good purposes. Like many people in the world, I have a family member in the early stages of Dementia (my Mother) and another family member (my Father) who had a mini-stroke a few years ago. He also still has some balance problems and sometimes falls. My brother and I worry about this as they like to maintain their independence and be relatively active. We cannot, so what is the solution? Two years ago, I ran across an ad that said the new Apple Series Five watch could detect falls and precise locations via GPS. Additionally, you can program the phone with people who are your emergency contacts, and if you fall and do not respond to say

you are safe within a quick time, it calls everyone, not only the emergency contacts but the local emergency services through the watch,

As individuals get older, especially if they have a form of Dementia, GPS-enabled watches, or other wearable devices could vastly assist caregivers. Alert systems, such as Silver Alerts and Amber Alerts, are used to get the word out about someone in vulnerable situations. Perhaps fewer of these would be seen, which to me is a fantastic thing, Rodrigues (2019) came to a similar conclusion in his dissertation research. The research also found that by using GPS tracking devices consistently, Alzheimer's patients followed reliable patterns throughout the day with machine learning algorithms. Past times that patients went off their usual routine or outside of the Geofencing provided information to help predict where they might be. This tracking is secondary to GPS tracking, which is the most accurate, but the research here is fascinating if the device is damaged or removed (Rodrigues, 2019). Additionally, with enough data points, we may be able to learn more about the disease itself.

There are sure to be policy and procedure questions that arise out of this type of technology. I am sure by now that the reader may have made the comparison to that of prisoners who are on house arrest and must wear an ankle monitor. While this may not be an issue when speaking of children and tracking their phones by the parents before the children are of age, what about a situation where an adult with Dementia who wanders off quite often does not want to wear a device? We could go further with the hypothetical saying that neighbors come out to help, as do the police. This search is costly and time-consuming, but it is in no way illegal. One can go missing from family and community forever if one likes. So, how should this be treated?

Yang and Kels (2016) make some good policy and procedure suggestions for those with Alzheimer's. These would provide GPS monitoring. Their product is not a watch: it is shoes. My

first thought was that this is completed surreptitiously, and while I am sure that many caring, frustrated family members have resorted to things like this – but the article has a better idea, Alzheimer's is detected far earlier than it was in the past. The window between diagnosis and one losing all of their mental faculties to make decisions provides an opportunity that people of the past did not have time to plan and make their wishes known on what they are comfortable with (Yang & Kels, 2016).

I see this added to a Living Will, which lets you pick how and when you want to die (especially if you are incapacitated). A Living Will allows you to choose whether you want to be put on life support and have all possible procedures done to save your life anywhere in between the opposite. This choice would include no life-saving measures, or a do not resuscitate order. If your body starts the death and dying process, nothing will intercede to stop that process (Lazaroff & Orr, 1986). While this method of choice for passing, I think that, like Yang & Kels's (2016) proposition, ethically is a great way to solve a problem before it happens. The only reservation that comes to me is the moments of clarity many Alzheimer's or Dementia patients experience. Sometimes they are entirely aware and easily capable of making decisions for themselves. It may last days and minutes – but they have their wits about them. What would be the ethical consequence if they change their mind after the paperwork during one of these times?

Overall, there are negative and positive things about geolocational tracking, just like any other device or technology when it comes out. Wayne (2012) pointed out something I hope we all know, once something is on the internet, it is forever. While I did not touch on this in the main body of the paper, I would like to bring up data brokers. Data brokers buy or obtain your information from third-party applications or companies. Commonly, one's data is available to data brokers when companies are looking for another revenue stream, or it is their main revenue

stream in addition to advertisements. Generally, you (or your data) are the product when something is free to use.

In many cases where juveniles commit crimes and get the chance for expungement, data brokers do not follow the right to forgetting laws that apply to them. Those with expunged records work hard to change their behavior and stay out of trouble. They work for and deserve the fresh start the courts give them; unfortunately, in data packages sold by data brokers, this information exists many years after the events. The same is true of those wrongly convicted or fully exonerated of their crimes. This retention is something that needs more legislation. This legislation applies to how data is collected, stored, and, more importantly: sold. This potential change will give those who earned the chance to start over and allow people who are being stalked or using their data against them.

References

Freed, D., Havron, S., Tseng, E., Gallardo, A., Chatterjee, R., Ristenpart, T., & Dell, N. (2019). "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-24.

Leitão, R. (2019). Anticipating smart home security and privacy threats with survivors of intimate partner abuse. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (pp. 527-539).

Lazaroff, A. E., & Orr, W. F. (1986). Living wills and other advance directives. *Clinics in Geriatric Medicine*, *2*(3), 521-534.

Pritchard, T. (2021). *Apple AirTag stalking is still a real danger — here's how to protect yourself*. Tom's Guide.

Rodrigues, D. J. L. F. D. V. (2019). *Risk Assessment for Alzheimer Patients, using GPS and accelerometers with a Machine Learning Approach* (Doctoral dissertation).

Unknown, E. (2021). *Top 9 best family tracking apps for iPhone & Andriod (2021).* www.airdroid.com 9 Best Family Tracking Apps in 2022 Comments. Retrieved November 20, 2022, from https://www.airdroid.com/parent-control/best-family-tracking-app/

Valentino-DeVries, J. (2018). *Hundreds of Apps Can Empower Stalkers to Track Their Victims*. New York Times. https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html

Wayne, L. D. (2012). The data-broker threat: Proposing federal legislation to protect post Expungement privacy. *The Journal of Criminal Law and Criminology (1973-)*, *102*(1), 253-282.

Yang, Y. T., & Kels, C. G. (2016). Does the shoe fit? Ethical, legal, and policy considerations of global positioning system shoes for individuals with Alzheimer's disease. *Journal of the American Geriatrics Society*, *64*(8), 1708-1715.