Exploring The Dangers of Data Collection

Jack Davidson

January 18, 2021

Data collection is rampant in our society and significant quantities of data are collected about the people in a multitude of varying mediums. The government infringes on the privacy of the people by harvesting vast amounts of data from the general population while school districts employ educational software that stores and collects every online movement that students take.

In a hearing held in 2017 to review the usage of data collection for use with facial recognition in law enforcement, over half of adults were found to be part of government facial recognition databases of which they may not even know they are a part [1].

The large amount of data collected on citizens "gives law enforcement a power they've never had before" [1]. Information is so easily and readily available to law enforcement. In the protests following the murder of Freddie Gray, Baltimore police "used [facial] recognition on social media photos to identify [protestors]. These targeted protesters were then arrested for unrelated causes [5]. Many peaceful protesters were monitored without reason [1].

Covert collection of data by the government is unjust because citizens should be able to trust that the government is acting in their best interest. The government should only monitor citizens when there is a just cause.

Monitoring the general population without just cause is a significant breach of privacy.

Go Guardian, a suite of web-based student monitoring and proctoring programs, collects data about our most precious segment of the population, children. This harmful student monitoring program is used at many districts across the United States including The Austin Independent School District, The School District of which Kealing Middle School is a part. School-issued Google Chromebooks have the proctoring software permanently installed. Teachers, administrators, and Go Guardian itself can remotely access and control the computers of students. Many of those AISD Google Chromebooks are the first personal computers that such students have ever had access to.

With web browsers being large, complex programs, often having various privilege escalation vulnerabilities, Go Guardian could have the ability to access the rest of your computer including running programs, accessing the network, and reading or writing your personal files. If a student was forced to install Go Guardian on their personal computer, sensitive information could be accessed by Go Guardian such as banking information, legal information, and other sensitive documents.

Go Guardian "[can] share information with our service providers that

[. . .] support our Offerings" [3]. The data Go Guardian collect and they can use it for any purpose such as selling or sharing it with other companies. Go Guardian receives money to collect data about students. School districts put forward vast amounts of resources for these malicious services. Go Guardian license rates cost around $12 per year for each device. In a school district such as Austin Independent School District with a population of around 80,890 students, to pay for Go Guardian licenses for only **one fourth of the students** in the District, it would cost $242,670 for **one year** of the service [2]. $242,670 is a large cost for such a harmful service.

The fact that Go Guardian is charging for a service *and* profiting from the data collection is abusive to the district and abusive to the student. Invasive educational software products like Go Guardian are a strain on school districts. The resources of school districts like AISD could be much better utilized by raising teacher salaries or providing more resources to students. Go Guardian is both a strain on privacy and a strain on resources.

Private companies such as Amazon, Netflix, and Facebook all collect personal data about you to strengthen their very accurate yet abusive recommendation system.

In exchange for services like Google, Facebook, and Reddit, the consumer returns their precious personal data. No private company is going to operate for free [4]. Technology companies can do any arbitrary thing they please with the consumer's data such as selling or giving as part of an agreement to third parties, using it for advertisement, or using it to tune their internal algorithms. Technology companies like Google, Facebook, and Reddit form a parasitic symbiosis between the producer and the consumer.

Both governmental and technological organizations collect personal data and control society with it. With data being collected through medium it can be hard to know what software we can use without worrying about being spied on, cornered, and abused. Luckily, there are ways we can circumvent such abuse. We can refuse to use these services even if it may be inconvenient and we can use only software developed by the *community* and *controlled* by the *users*.

Works Cited

[1] "Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties". House Committee on Oversight and Reform, 2019, https://oversight.house.gov/legislation/hearings/facial-recognition-technology-part-1-its-impact-on-our-civil-rights-and.

[2] "AISD District Demographics". Austin Independent School District, 2020, https://www.austinisd.org/planning-asset-management/district-demographics.

[3] "Product Privacy Policy". GoGuardian, Liminex Corporation, 2020, https://www.goguardian.com/product-privacy/.

[4] Hill, Steven. "Should Big Tech own our Personal Data". Wired, Condé Nast, 2019, https://www.wired.com/story/should-big-tech-own-our-personal-data/.

[5] Spivak, Jameson. “Maryland’s face recognition system is one of the most invasive in the nation — COMMENTARY”. The Baltimore Sun, Tribune Publishing, 2020, https://www.baltimoresun.com/opinion/op-ed/bs-ed-op-0310-face-recognition-20200309-hg6jkfav2fdz3ccs55bvqjtnmu-story.html.