Using Amazon Ring for Policing Efforts

Dhruval Bhatt
May 3rd, 2020

Police work and solving crimes has always been an intelligent process. Until recently, police predominantly relied on tips, stakeouts, physical surveillance, tracking and their intuition to determine when, where and whom to suspect and prosecute. However, now, with access to big data and advanced algorithms, police have increased the ability to capture, aggregate, and process an ever-greater volume, velocity, and variety of data" (Ferguson 8). In his book, "Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement", Andrew Ferguson, highlights the benefits and flaws of many new policing tools, such as, PredPol, Persistent Surveillance System, Geofeedia, etc. Such tools have enabled the police to make informed decisions on whom to suspect or the location of crime, to quickly act to catch criminals or even prevent a crime. Despite the increased efficiency and improved data driven decision, these big data enabled tools and its use could be biased, inaccurate and in some cases unconstitutional

One such source of big data is Amazon Ring, a gadget that is sold as a fancy doorbell and peephole to regular consumers but can be enabled to share footages to law enforcement to investigate and prosecute possible crimes. What differentiates this tool from some of the above-mentioned technologies, is that law enforcement is not explicitly setting this tool up for intel, but they rely on ordinary citizens to share data collected on their private property, if required. Nonetheless, it raises questions of violation of constitutional rights, privacy, and potential issues with its usage. Understanding this is not only critical for evaluating the use of this product but a bigger question of ethics of using consumer goods for policing.

The use of Amazon Ring's data does not seem unconstitutional in an obvious way. The fourth amendment of the US constitution protects people against unwarranted search and seizure, without probable cause. An incriminating footage recorded on Amazon Ring could be the justification for arrest and prosecution. Considering that an ordinary citizen is providing information gained from their own private property, it could be equated to a person tipping off the police or giving an eyewitness account, which is an acceptable practice. The argument against this is in the outcome of United States v. Jones court case, where GPS tracking was found unconstitutional due to the privacy concern of "long- term aggregated nature of the data collection

and use" (Ferguson 100). While the court holds law enforcement agency liable to crossing a line in "the dilemma of the "collect it all" mind- set", this caution should extend to ordinary citizens as well when their ability to monitor increases infinitely and jeopardizes other's rights to privacy.

Due to the concern of invasion of privacy, it is not ethical to capture everything in the device's view constantly. The conflict lies between ones right to record from their own property and other's right not to be filmed without consent in their own space. However, it may be acceptable to capture footage of one's own property and public space. While one's home is a sanctuary with guaranteed privacy, "U.S. Constitution through the Fourth Amendment has not provided much protection for activities that occur in public spaces" (Ferguson 98). The field of vision of Amazon Ring should be limited to own property and activities on public pathways and street. Any suspicious activity monitored here can and should be freely shared with the police. It would still be courteous to one's neighbors and possibly deter crime in their own home to have some notification of this video monitoring.

While the physical monitoring occurs in citizen's property, the data is stored, managed and used to its potential through a private business, Amazon. The issue with relying on private companies for critical data is that the cost may not always be affordable or they "could decide not to continue working in the policing space [or] abandoning the technology" (Ferguson 130). The business must be held accountable to ensure that the data is secure, is used for limited purposes and presented without tampering, even if there is a conflict of interest if the business is indicted for criminal activity. Additionally, consumers should be aware of the company's collection and usage of data. This is not just limited to Amazon. As more commercial devices collect data and as more data is sold and used for various purposes, a concept of "digital public space" should be transparently discussed. When one willingly puts out information on open digital platforms, like a Facebook post or data explicitly agreed for public use, "anything you say can and will be used against you in a court of law" (Miranda warning). However, digital tools should not be used to unwittingly collect data from consumers and used or sold for other purposes without their consent.

The use of Amazon Ring for police work is not outright illegal or unethical but there should be constraints on how long the data is aggregated, what is monitored and how it is used. As all tools, ethics of usage falls on the humans using it. Misrepresenting data, unfairly targeting minorities and using "technology [to monitor] political protesters, religious dissenters and

everyone", should be strictly opposed (Ferguson 106). In discussing protection, it is important to distinguish that all the privacy protection and fourth amendment discussions is to ensure that police power is not abused. It is not to give criminals a fair chance to commit crimes without being caught. Having considered ethical and constitutional constraints, advanced surveillance can and should be used without qualms to thwart crimes.

References

Ferguson, Andrew G. Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York University Press, 2017.