CS Ethics: Consumer Surveillance Tools

Emily - against surveillance | Catherine - for surveillance

Summary:

Consumer surveillance is the collecting, analyzing, and profiting of consumer data. Companies monitor things like purchase history, location, gender, age, etc.. Common methods of surveillance are cookies, app tracking, and smart devices, like home assistants and wearables. Everyday objects like GPS, Amazon Alexa, Amazon Ring (doorbell camera), and health devices (e.g. Fitbit, Apple Watch) are all recording information on our human attributes and daily life behaviors. Surveillance can be used for good, as it can help solve crime, prove innocence, and improve security. If the data is monitored properly, it can be a great asset to society. Recordings in the public are also not an invasion of privacy, as being in a public space means one will be perceived. However, others argue that surveillance is an invasion to privacy, and involves dubious consumer consent. When the data is not monitored properly, it can fall into the wrong hands and subject consumers to identity, exploitation, and security issues. It also affects everyday life by influencing consumers to make certain decisions, and allowing companies to discriminate against and falsely stereotype consumers, posing ethical issues.

Question: Is consumer surveillance more beneficial or more concerning?

Emily - Against Surveillance

Consumer surveillance - collecting, analyzing, and profiting from data on consumers. Some of the data could be things like purchase history, location data, gender, age, etc.

- Common methods include tracking cookies (small file of info.), app tracking, and smart devices
    - Smart devices like home assistants and wearable devices
- Popular consumer surveillance tools include but are not limited to GPS, Amazon Alexa, Amazon Ring (doorbell), and health devices (e.g. Fitbit, Apple Watch)

Issues:

- Privacy
    - Corporations know TOO much about you
    - Alexa's software gathers info with no notice to consumers
        - Email and physical address, phone numbers you call, purchases you make (e.g. airline travel), considered purchases, other information
        - Smart assistants are always listening in case you call key words
    - Microsoft Word + Intel embedded tracking identifiers
    - Facebook likes -> can determine personal attributes like race, religion, political views, sexual orientation, drug use, etc.
    - Social media -> Personality traits (e.g. emotional stability, impulsivity, depression)
    - Browsing history -> Job + educational level
    - Typing patterns -> emotional states (e.g. confidence, sadness, tiredness)
    - Can figure out if you are speeding or your exact location
- Consumer consent
    - This info is often used w/ out consumers' explicit consent or knowledge
    - When companies do ask for consumers to opt in/consent
        - Consumers aren't aware of the significance of the data collected
        - The terms are unclear for consumers
    - Companies intentionally make it hard to opt out and intentionally make terms unclear + misleading
        - Users can't turn off all tracking in 1 click, they often need to manually deselect things
        - Consumers are sometimes denied access to a service if they don't allow tracking
    - Terms of service can change without the consumer knowing
- Security
    - Despite corporations compiling all of this data, they sometimes don't have proper security measures in place -> can lead to data security issues -> identity theft, fraud, deceit, manipulation, and exploitation
    - When tools like GPS and doorbell cameras have access to important information, they need to have effective security
        - In March 2023, 9/10 home surveillance cameras on the HK market failed to meet European cybersecurity standards
        - These tools are vulnerable, easy targets to hack

        - Burglars could use GPS or doorbell cameras to determine when you aren’t home
- Surveillance Pricing
    - Companies can use the info they collect to give “personalized pricing” based on customer’s aspects, like racial groups, gender, interests, or behaviors
        - Opens the door for inequality and discrimination
        - Circumstantial pricing (e.g. a car insurance will charge more if they know you park in a shady neighborhood prone to carjacking)
- Influence decisions
    - Early intention of collecting data -> consumer purchases
        - Receiving ads when talking about a product (audio data) or walking by a store (location tracking)
        - Can influence purchases during different time intervals (e.g. companies know your habits and emotions, like if you are an impulsive shopper when sad)
    - The use of data has branched out to insurances, credit scoring, risk management, and policing
        - Companies are already using this data to calculate creditworthiness, predict health risks, predict hospital costs
        - Manipulation - targeting people with messaging adapted to their personalities and views (e.g. targeting voters for political manipulation)

https://www.proquest.com/docview/418937896/36FFCFB33ADF400CPQ/5?accountid=36166&sourcetype=Newspapers
https://crackedlabs.org/en/corporate-surveillance
https://www.ftc.gov/system/files/ftc_gov/pdf/Commercial%20Surveillance%20and%20Data%20Security%20Rulemaking%20Fact%20Sheet_1.pdf
https://www.proquest.com/docview/2681995858/36FFCFB33ADF400CPQ/8?accountid=36166&sourcetype=Newspapers
https://www.wbur.org/onpoint/2024/08/14/surveillance-pricing-harm-consumers-ftc-data
https://www.proquest.com/docview/3083646544/36FFCFB33ADF400CPQ/3?accountid=36166&sourcetype=Newspapers
https://www.proquest.com/docview/2786904198/36FFCFB33ADF400CPQ/1?accountid=36166&sourcetype=Blogs,%20Podcasts,%20&%20Websites
https://www.proquest.com/docview/240580408/4549DACEFC1B43CCPQ/3?accountid=36166&sourcetype=Newspapers

Catherine - For Surveillance

Surveillance can be used to discover crimes, and solve cases. The government has a right to make sure that none of its citizens are engaging in criminal activity online. In emergencies, police deserve to have access to data that could potentially save peoples lives.
Surveillance can also be used to collect helpful information to improve future pursuits.
Also there are some cases where the data is not collected, and yet the people still behave better. This is called self-surveillance. The MTA utilizes this often, as they put these circular mirrors in the corners of stairs occasionally. This type of surveillance is harmless, and still helps the security of the community.
Ways surveillance can help:

- Cameras help deter crime
- Recordings can help solve criminal cases
- Eye-witnesses will sometimes get things wrong
- They can help get an accurate story on a specific issue

Surveillance itself is neutral, it's what is done with the information that could be harmful. But as long as there are responsible, trustworthy people taking care of our data, then surveillance isn't a problem.
Surveillance in a public area isn't an invasion of privacy, as everyone is out and about, and it is expected that people will see each other.
This is also true on the internet, if it can be seen by other people, it can be recorded as data.
In the case of the Amazon Ring camera, although the police should have to state a valid reason to access the footage, the cameras are in a public setting so ultimately there isn't a breach in privacy. Amazon's new policy of requiring a warrant to access the footage is a good solution, as police can use this footage to help them on their cases.
Camera's also have no bias. They record everything as it transpired, and can be much more accurate than eyewitnesses or policemen. They can help bring an objective summary of what happened, and prevent innocent people from being falsely accused.

https://www.bossecurity.com/2022/12/21/benefits-of-surveillance-cameras-in-public-places/#:~:text=December%2021%2C%202022,if%20you%20are%20in%20trouble.
https://www2.law.ucla.edu/Volokh/camerascomm.htm