THE BIKE THIEF

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469577526

SUMMARY

A woman posts an ad on Craigslist for a bicycle in her yard. She posts her full numbered home address in the ad and specifies that the bike is "just collecting dust in the backyard." A thief soon arrives to the address, peeks over the back fence, and carries the bike away.

ACTIVITIES

Take a poll of if students have ever posted a home address online, whether to sell something, or as part of a social media profile. Did students consider any potential risks before posting the address?

Privately, have students search for their home addresses in Google. Do any personal results come up, related to family names, ages, ethnicity, net worth, or home price? Which websites are these results on? Are there any inaccuracies?

Research recent news reports of burglaries in your neighborhood or town. Are any linked to the use of location technology, such as GPS, posted home addresses online, or geotagged social media posts?

RELEVANT ARTICLES

Unlisted: Variations in Location Sharing by Craigslist Users. Seidl, D. and Allen, C. 2016. https://www.cartogis.org/docs/proceedings/2016/Seidl_and_Allen.pdf

Man is Accused of Using Instagram Photos to Burglarize College Sorority Members in Fullerton and Orange. Rocha, V. 2016. https://www.latimes.com/local/lanow/la-me-ln-instagram-burglarize-sorority-students-20160224-story.html

Please Enter Your Home Location: Geoprivacy Attitudes and Personal Location Masking Strategies of Internet Users. Seidl, Jankowski, Clarke, and Nara. 2020. Annals of the American Association of Geographers. https://doi.org/10.1080/24694452.2019.1654843

DISCUSSION POINTS

- Is there any reason you might want your full home address to go in an online ad?
- Can you think of any risks besides burglary that might result from posting a home location online?
- What are some safer methods of sharing location if your goal is to eventually meet with a stranger to sell or buy a product?
- Are there particular categories of items for sale that require better protection of location privacy than others (i.e. expensive goods or child products)?

LICENSE PLATES

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469610867

SUMMARY

This video features a mock interview with a "repo man," or a employee for a vehicle repossession company, talking about his use of automated license plate reader (ALPR) technology. The interviewee discusses how the ALPR camera system on his "spotter car" continuously collects license plate data, along with location, time, date, and photographs of all cars along his daily driving routes. He notes that he specifically targets certain parking lots and apartment complexes, and his company sells all the license plate location data to police, banks, and insurance companies.

ACTIVITIES

Have students identify and map the locations of nearby surveillance cameras. Are any of these cameras potentially equipped with ALPR (based on appearance)? Where do these cameras appear to be concentrated? Consider this an example of counter-mapping.

Help your students file a FOIA request to determine if your town is purchasing or using ALPR technology. See the MuckRock project at: https://www.muckrock.com/assignment/is-your-town-using-alpr-technology-108/form/

RELEVANT ARTICLES

Automated License Plate Readers (ALPRs). EFF. https://www.eff.org/pages/automated-license-plate-readers-alpr

This Company Built a Private Surveillance Network. We Tracked Someone With It. Cox, J. 2019. Vice News. https://www.vice.com/en/article/ne879z/i-tracked-someone-with-license-plate-readers-drn

Police License Plate Readers are Still Exposed on the Internet. Whittaker, Z. 2019. TechCrunch. https://techcrunch.com/2019/01/22/police-alpr-license-plate-readers-accessible-internet/

DISCUSSION POINTS

- Does ALPR lead to uneven surveillance between groups? If so, which groups of people are more likely to be surveilled?
- Is it fair to target certain neighborhoods or parking lots with ALPR, as the "repo man" in this video claims to do?
- Should companies be legally allowed to collect license plate locations and pictures?
- Is it fair to use systematic location surveillance to fight fraud?
- The "repo man" in this video claims that using mobile ALPR cameras is just like walking down the street recording plates with a pen and paper. Is this a valid claim? Are there any differences between these practices?

FOLLOWERS

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469618411

SUMMARY

A celebrity is enjoying a scenic walk alone in the forest, observing the foliage and taking photographs. A hacker locks on to the celebrity's location coordinates and notices there is an award of $2,500 for capturing photos of him. The hacker locates nearby flying UAVs, and initiates GPS spoofing to redirect the drones to the celebrity's location. The celebrity notices five drones in the air above him, and takes off running.

ACTIVITIES

Have students make a list of potential activities that camera-equipped drones could be repurposed for if their GPS systems were spoofed. Which of these are the most dangerous to human well-being?

Play a game of questions by having one student ask a question about GPS spoofing, the next student add on with a related question, and so on. Write all questions on the board. If someone offers a statement, all will shout "statement!" At the end, focus on one or two questions about GPS spoofing in greater depth.

RELEVANT ARTICLES

How Vulnerable is GPS? Milner, G. 2020. The New Yorker. https://www.newyorker.com/tech/annals-of-technology/how-vulnerable-is-gps

Rethinking Spatial Data Quality: Pokémon Go as a Case Study of Location Spoofing. Zhao, B. and Zhang, S. 2018. The Professional Geographer. https://doi.org/10.1080/00330124.2018.1479973

New GPS 'Circle Spoofing' Moves Ship Locations Thousands of Miles. Goward, D. 2020. GPS World. https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/

DISCUSSION POINTS

- What risks does GPS spoofing pose outside of UAVs? What kinds of applications that rely on GPS might be affected by spoofing? How might spoofed GPS applications damage physical infrastructure?
- Are there any examples of GPS spoofing that would be beneficial for public safety or national security?
- What factors make GPS vulnerable to spoofing? What could change that would make GPS more secure? Would this be worth the tradeoffs? See the first article listed above for context.

TEXT MESSAGES

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469619017

SUMMARY

This video features mock interviews with two adults who separately endured a barrage of overly personal marketing text messages. Both discovered that when they swiped their credit cards at different cafes, they were signed up for a rewards program linking their credit card swipes to their cell phone data and social media accounts, including their locations. These data links enabled the marketing company to calculate how long one of them lingered by a shop window, where they currently were, and whether they were alone, offering discounts for preferred characteristics. The interviewees discuss their reactions to finding out the extent of the data being collected about them.

ACTIVITIES

In small groups, make a list of pros and cons for location-tailored marketing. Are there cases in which you want to receive ads based on where you've been?

Have students call out potential inferences that could be made about individuals using real-time phone data, Could location be used to infer whether someone is on a date, their physical activity levels, or other sensitive information?

RELEVANT ARTICLES

Even Brick-and-Mortar Stores Are Tracking You While You Shop. Neal, M. 2013. Vice. https://www.vice.com/en/article/9aapga/even-brick-and-mortar-stores-are-tracking-you-while-you-shop

Private Intel Firm Buys Location Data to Track People to their 'Doorstep.' Cox, J. 2020. Vice. https://www.vice.com/en/article/qj454d/private-intelligence-location-data-xmode-hyas

How Target Figured Out a Teen Girl was Pregnant Before her Father Did. Hill, K. 2012. Forbes. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

DISCUSSION POINTS

- How likely do you think it is that companies have teamed up to link credit card information with cell phone location data?
- Is is plausible that companies are collecting data on how long you stand in front of a display or whether you're alone?
- Which is more intrusive, the frequency of the messages these interviewees received, or their personal nature?
- Have you ever inadvertently signed up for marketing communications you didn't want to receive? What did you do?

APPLICANTS

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469619731

SUMMARY

A mock company called LocCheck advertises its services to employers seeking advanced background checks on their applicants. LocCheck offers the "location edge," tracking applicants' phone locations from the minute they leave an interview. The company advertises that tracking where applicants go outside the interview can alert employers of risky behaviors to better inform hiring decisions. In the final scene, an applicant is flagged in LocCheck for repeatedly visiting a medical center. Based on this information, an HR representative recommends selection of a different candidate.

ACTIVITIES

Hold a debate, splitting the class into *for* and *against* location tracking of job applicants. How would LocCheck assist in risk management for a company? How would it lead to discrimination against job candidates?

Have students make a list of potential "false ids" of risky behavior that might take place just by relying on location data. What impact does GPS data accuracy have? What happens if messy data is taken as accurate?

RELEVANT ARTICLES

Twelve Million Phones, One Dataset, Zero Privacy. Thompson, S.A. and Warzel, C. 2019. The New York Times. https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

The Employer-Surveillance State. Shell, E.R. 2018. The Atlantic. https://www.theatlantic.com/business/archive/2018/10/employee-surveillance/568159/

Workplace Surveillance in Times of Corona. Rodriguez, K. and Windwher, S. 2020. EFF. https://www.eff.org/deeplinks/2020/09/workplace-surveillance-times-corona

DISCUSSION POINTS

- If you read that LocCheck was a requirement to interview for a position you were interested in, would you still apply for the job? Why or why not?
- Imagine you had a job as a bartender, and LocCheck flagged you as a risk for spending time in a bar every night. What would you do?
- What do you make of the final scene, where an applicant is passed over for visiting a medical center most days. Is this ethical or legal?
- Would you participate if you were notified of the start and end times of the location tracking, or if you were paid?

SMART ENERGY

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469620031

SUMMARY

A woman gets up in the morning and chats with her partner over coffee, adjusting the smart thermostat in her home and observing the settings on her phone. She leaves for work and turns down the thermostat. Employees at a utility company obeserve on a map the locations of homes with the heat turned down during the day. A burglar targets the empty house where it is known the heat is off, suggesting that no one is home. Additional video is shown of others adjusting their smart thermostats for the day.

ACTIVITIES

Take a poll about the connected devices in students' homes. Do students have smart thermometers? Doorbell cameras? Connected refrigerators? Speakers? Cars? Locks? Have they ever experienced suspicious activity with these devices?

Have students make a list of vulnerabilities with smart devices. How else (besides burglary) might a hacker or other observer of connected data impact residents of the home without proper security?

RELEVANT ARTICLES

How Nest, Designed to Keep Intruders Out of People's Homes, Effectively Allowed Hackers to Get In. Albergotti, R. 2019. The Washington Post. https://www.washingtonpost.com/technology/2019/04/23/how-nest-designed-keep-intruders-out-peoples-homes-effectively-allowed-hackers-get/

Change This One Setting to Stop Hackers from Taking Over Your Smart Home Devices. Gelinas, J. Kim Komando. https://www.komando.com/security-privacy/change-this-one-setting-to-stop-hackers-from-taking-over-your-smart-home-devices/600227/

Closing the Blinds: Four Strategies for Protecting Smart Home Privacy from Network Observers. Apthorpe, N., Reisman, D., and Feamster, N. 2017. ARXIV. https://arxiv.org/pdf/1705.06809.pdf

DISCUSSION POINTS

- Have you heard of two-factor authentication? Do you use it for any of your logins?
- A smart thermostat can save energy by automatically turning down the heat when you might otherwise forget. Does the energy efficiency and ease of a smart thermostat override any privacy concerns?
- How might advertisers benefit from access to your smart thermostat data?

GPS TAGS

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469620519

SUMMARY

A wildlife ecologist describes advances in animal tracking with GPS collars and the benefits of the improved technology for ecological research. A parallel is drawn between GPS tracking of animals and GPS tracking of humans via cell phones. The ecologist discusses how GPS enables scientists to track migration routes, animals' unique paths, and impacts in high-traffic areas. As the ability to track both humans and other animals with GPS becomes more ubiquitous, this video is intended to spark discussion of any relevant differences between the two. The ecologist also mentions the vulnerability of the GPS location data to cybersecurity threats due to its valuable and sensitive nature.

ACTIVITIES

Hold a class debate on the merits of GPS animal tracking for research purposes. Is there any potential for harm to the animals? Do animals have a right to privacy?

Hold a follow-up debate on the merits of (involuntary) GPS tracking of humans for research purposes. What are the pros and cons? How is this similar to or different from animal GPS tracking?

RELEVANT ARTICLES

Digital Jail: How Electronic Monitoring Drives Defendants Into Debt. Koman, A. 2019. ProPublica. https://www.propublica.org/article/digital-jail-how-electronic-monitoring-drives-defendants-into-debt

The Internet of Animals That Could Help to Save Vanishing Wildlife. Curry, A. 2018. Nature. https://www.nature.com/articles/d41586-018-07036-2

The 21st Century Threat to Wildlife is "Cyberpoaching". Norton, K. 2020. NOVA. https://www.pbs.org/wgbh/nova/article/21st-century-threat-wildlife-cyberpoaching/

DISCUSSION POINTS

- Is it fair to compare GPS animal tracking to tracking of humans using smartphone GPS?
- Which do you think is more pervasive, company tracking of humans using GPS or research tracking of animals using GPS tags and collars?
- What risks are involved in amassing location data of rare and endangered species online?
- Should organizations obtain consent from consumers to track phone GPS data in cases of public safety or in a public health crisis?

DRAGNET

GEOPRIVACY VIDEO SERIES

HTTPS://VIMEO.COM/469621161

SUMMARY

A man is walking his dog on a sunny afternoon. Unbeknownst to him, a burglary is taking place in his neighborhood. The police obtain a warrant for cell phone location data in the area at the time of the crime. Since the dog-walker circled the vicinity several times, and has the most location points nearby, he is erroneously implicated in the crime and arrested.

ACTIVITIES

Have students research federal, state, and local laws related to location privacy, including reading the text of the laws. Is there anything preventing law enforcement from obtaining your GPS data if found to be nearby a crime scene? How about in a neighboring state?

Consider scenarios where one person might borrow another's phone, or when a crime occurs in a many-storied building, or when someone doesn't carry a phone. What impacts would these have on the resulting GPS data being used to look for suspects? Have students report on potential outcomes.

RELEVANT ARTICLES

Tracking Phones, Google Is a Dragnet for the Police. Valentino-DeVries, J. 2019. The New York Times. https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html

Google Tracked His Bike Ride Past a Burglarized Home. That Made Him a Suspect. Schuppe, J. 2020. NBC News. https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761

An Empirical Test of Household Identification Risk in Geomasked Maps. Seidl, D., Jankowski, P., and Nara, A. 2018. Cartography and Geographic Information Science. https://doi.org/10.1080/15230406.2018.1544932

DISCUSSION POINTS

- Should law enforcement be able to cast a dragnet to capture phone GPS data, with or without a warrant?
- Do you think there should be a system of recompense for individuals falsely accused of a crime due to location data?
- What data accuracy factors contribute to the risk of falsely identifying a crime suspect based on location data?
- Imagine that a crime occurs in a 10-story residential building, with many phones inside. These might all appear at the same X-Y coordinates. How would an analyst discern which were at the scene of the crime?