SURVEILLANCE, JOURNALISM, AND THE CAPITOL RIOT

ETHICALLY REPORTING ON DATA EXPLOITATION AND GEOTRACKING

January 6, 2021 was a dark day in American history. As Congress convened in Washington, D.C., to count the electoral votes that would affirm Joe Biden's win in the 2020 presidential election, thousands of angry Trump supporters attacked the Capitol in an effort to block what they believed to be a false victory. Around 1 p.m., after attending Trump's "Save America" rally at the Ellipse Park that morning, protestors breached security barriers to storm the building by fighting with Capitol police, scaling the walls, and breaking windows (Barrett, Raju, & Nickeas, 2021). Once inside, smoke grenades were released and the mob "went door to door waving Confederate [and pro-Trump] flags, looting the offices of senators and congressmen, and repeating the false rhetoric that … Trump was the real winner of the election" (Jacobo, 2021). By 5 p.m., law enforcement orchestrated evacuations of both the Capitol itself as well as the nearby DNC and RNC buildings where pipe bombs had been found. Despite the chaos and deadly violence that transpired, the Capitol was secured around 8 p.m. and lawmakers returned to their session, concluding their duty to certify Biden as the 46th president of the United States (Barrett, Raju, & Nickeas, 2021).

In the weeks following, a number of opinion pieces were written about the events which occurred, from assertions of policing double-standards (Love, 2021) to arguments that Trump should face legal consequences for his role in encouraging the mob (The Washington Post Editorial Board, 2021). Honing in on a different focus however, one opinion article published in *The New York Times* used the attack as an opportunity to discuss geo-tracking, which happens when smartphone users allow apps access to their exact position using GPS technology. This location data is typically harnessed for advertising purposes, such as "measuring whether people visited a store after seeing an online ad or helping marketers build more detailed profiles for targeted advertising" (Thompson & Warzel, 2019). However, using this information for other purposes has recently received increased attention.

Some argue that geo-tracking data has the potential to be used in courts and by law enforcement to make society safer. For example, "Japan has asked owners of both public and private surveillance … to make user data available to authorities without warrants. This practice, which the Japanese government believes is helpful in solving crimes [and] tracking domestic abuse cases, is seen as one reason why Japan's crime rate is about a quarter that of the U.S." (Kirkpatrick, 2020). Similarly, geo-tracking has been used in the past year in an effort to slow the spread of the coronavirus as countries around the world have implemented measures such as "location monitoring systems to ensure that people who were carrying COVID-19 were staying at

home," "track[ing] the mobile-phone data of people suspected to be infected with the coronavirus … and warn[ing] those who may have come into contact with people infected with the virus" (Kirkpatrick, 2020).

Taking a more skeptical stance towards geo-tracking, Charlie Warzel and Stuart A. Thompson revealed that *The New York Times* received over 100,000 leaked data location pings for thousands of smart phones during the Capitol riot, which they then used to track the insurrectionists. "While there were no names or phone numbers in the data," they write, "we were [nonetheless] able to connect dozens of devices to their owners, tying [supposedly] anonymous locations back to names, home addresses, social networks and phone numbers of people in attendance" (Warzel & Thompson, 2021). Especially since they were able to find such personal information as individuals unrelated to any official office or law enforcement agency, Warzel and Thompson demonstrate just how troubling geo-tracking can be. What if it got into the wrong hands? Worse still is the fact that:

> Smartphone users will never know if they are included in the data or whether their precise movements were sold. There are no laws forcing companies to disclose what the data is used for or for how long. There are no legal requirements to ever delete the data. Even if anyone could figure out where records of their locations were sold, in most states, you can't request that the data be deleted.

Furthermore, using the case of one protester whose phone data showed he had entered the Capitol but photo evidence shows he merely stood on the outside steps, Warzel and Thompson illustrate how imprecise this information can be. Clearly, such errors are problematic because "a few feet can be the difference between a participant who committed a serious crime and an onlooker" (Warzel & Thompson, 2021). Overall, by demonstrating to the public just how much of their personal information can be collected and misused, Warzel and Thompson argue that geo-tracking surveillance is an invasion of privacy and such data should never be collected in the first place. Not only could it be used inappropriately by governments, law enforcement, and individuals, but there are also no laws protecting data from being bought and sold between other entities such as businesses or organizations. Indeed, we have already seen troubling implications of this in cases like Facebook's 2018 Cambridge Analytica scandal, where the voter-profiling company used leaked social media data to create "30 million 'psychographic' profiles about voters" (Meyer, 2018).

Though Warzel and Thompson "intended the story as a warning against surveillance" and "only publish[ed] the names of people who gave their permission to be quoted in [the] article," some questioned whether publishing this information was ethical, regardless of any greater purpose they had hoped to serve (Gilliard & Cahn, 2021, and Warzel & Thompson, 2021). In an opinion piece from *Medium*'s *OneZero* publication, Chris Gilliard and Albert Fox Cahn agreed with the stance of the *Times* but criticized their distribution of the geo-tracking data saying: "The *Times* cannot have its cake and eat it too. If this type of data exploitation and tracking is unethical, then it is unethical—the paper should not itself participate in these practices in pointing out how bad they are" (Gilliard & Cahn, 2021). Here, the authors assert that "regardless of the disclaimers and caveats" Warzel and Thompson's use of this data undermines the overall point and could even influence public opinion antithetically (Gilliard & Cahn, 2021). While the use of the geo-tracking data received justification in this case because law enforcement used it to track rioters at the Capitol, Gilliard and Cahn point out that if "surveillance technologies expand, they won't be primarily aimed at white extremists … [but] will be systematically targeted at BIPOC communities," such as when the Minneapolis police department gave Google a geofence search warrant during the George Floyd protests (Gilliard & Cahn, 2021). Ultimately

then, they argue, showcasing data exploitation in the way that Warzel and Thompson did is more likely to garner *support* for geo-tracking, possibly influencing "the public [to] pull back from vital [data exploitation] reforms at the very moment they're likely to go through" (Gilliard & Cahn, 2021).

Of course, "many people were shaken to their cores by the events of January 6," but Gilliard and Cahn hold that "it's precisely during the most dire [sic] times that our commitment to ethics should guide us the most" (Gilliard & Cahn, 2021). While this may be true, deciding *what* the ethical response should be is not necessarily cut and dry. In the end, questions surrounding if and how to use location data, as well as how to report on it, are unlikely to be answered with certainty any time soon since "there will always be some tension between the desire to protect personal privacy and the clear value of information that can be used to solve crimes or keep the public safe" (Kirkpatrick, 2020). Whether we ultimately choose to prioritize one over the other or find creative solutions to overcome the seemingly irreconcilable conflict, these considerations will only become more pressing as technology continues to develop and become ubiquitous in our lives.

Discussion Questions:

1. Do you agree with Warzel and Thompson, Gilliard and Cahn, or neither? Why?
2. What should Warzel and Thompson have done differently, if anything? Would their argument have been less impactful had they not used the insurrectionist's geo-tracked data?
3. How much do intentions matter in evaluating the ethics of another's actions?
4. Are tools like geo-tracking technology *inherently* unethical or does it depend on *how* they are used?
5. If proper restrictions were put into place, could geo-tracking be used to assist law enforcement in an ethical and safe manner? Why or why not? What would such restrictions look like?
6. What arguments could be promoted for and against a surveillance society?

Further Information:

Barrett, T., Raju, M., & Nickeas, P. (2021, January 7). "US Capitol Secured, 4 Dead After Rioters Stormed the Halls of Congress to Block Biden's Win." *CNN*. Available at: https://www.cnn.com/2021/01/06/politics/us-capitol-lockdown/index.html

Gilliard, C., and Cahn, A. F. (2021, February 8). "Note to Reporters: If Surveillance Data Shouldn't Exist, Then Don't Use It." *OneZero*. Available at: https://onezero.medium.com/note-to-reporters-if-the-data-shouldnt-exist-then-don-t-use-it-3e745fe32367

Jacobo, J. (2021, January 10). "A Visual Timeline on How the Attack on Capitol Hill Unfolded." *ABC News*. Available at: https://abcnews.go.com/US/visual-timeline-attack-capitol-hill-unfolded/story?id=75112066

Kirkpatrick, K. (2020, October). "Who Has Access to Your Smartphone Data?" *Communications of the ACM Magazine*, Vol. 63 No. 10, Pages 15-17. Available at: https://cacm.acm.org/magazines/2020/10/247585-who-has-access-to-your-smartphone-data/fulltext

Love, D. A. (2021, January 14). "The Capitol Riot Exposed Police Double Standards." *Aljazeera*. Available at: https://www.aljazeera.com/opinions/2021/1/14/the-capitol-riot-exposed-police-double-standards

Meyer, R. (2018, March 20). "The Cambridge Analytica Scandal, in Three Paragraphs." *The Atlantic*. Available at: https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/

The Washington Post Editorial Board. (2021, January 8). "Trump Must be Punished for What He Did This Week — and Checked from Doing Worse." *The Washington Post*. Available at: https://www.washingtonpost.com/opinions/pence-must-protect-the-country-from-trump-between-now-and-jan-20/2021/01/08/18c76318-51de-11eb-83e3-322644d82356_story.html

Thompson, S. A., and Warzel, C. (2019 December 20). "Smartphones Are Spies. Here's Whom They Report To." *The New York Times*. Available at: https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html

Warzel, C., and Thompson S. A. (2021, February 5). "They Stormed the Capitol. Their Apps Tracked Them." *The New York Times*. Available at: https://www.nytimes.com/2021/02/05/opinion/capitol-attack-cellphone-data.html

Authors:

Hailey Wammack, Kat Williams, & Scott R. Stroud, Ph.D.
Media Ethics Initiative
Center for Media Engagement
University of Texas at Austin
April 26, 2022

Image: lev radin /Shutterstock.com

This case was supported by funding from the John S. and James L. Knight Foundation. These cases can be used in unmodified PDF form in classroom or educational settings. For use in publications such as textbooks, readers, and other works, please contact the Center for Media Engagement.