The University of Texas at Austin
Center for Media Engagement
Moody College of Communication

LOCATION-BASED TARGETING:
HISTORY, USAGE, AND RELATED CONCERNS

Pooja Iyer, Martin J. Riedl, Inga K. Trauthig, and Samuel Woolley

SUMMARY

Location-based targeting is increasingly being utilized in political campaigns and is often a subject of concern for privacy advocates. In today's hyper-connected world, people face challenges to their privacy due to the large amounts of personal data that are constantly being gathered. A great deal of this information is focused on people's personal habits, both online and offline: their location, movements, and behaviors. The use of location-based targeting in the political sphere poses a challenge to democracy because geolocation data can be exploited to deceive voters as well as to (unknowingly) influence voting behavior.

While political campaigns are increasingly utilizing location-based targeting, policymakers continue to struggle with adequate responses that would better regulate the comprehensive reach of location-based targeting. In order to provide practice-oriented research, the Propaganda Lab at the Center for Media Engagement created an overview on location-based targeting, including its history, the technologies behind it, and its usage over the years. The report also provides recommendations for the healthy development of these technological possibilities.

SUGGESTED CITATION:

Iyer, P., Riedl, M. J., Trauthig, I. K., and Woolley, S. (December, 2021). Location-based targeting: History, usage, and related concerns. Center for Media Engagement. https://mediaengagement.org/research/location-based-targeting

INTRODUCTION

In October 2020, Enza went to a Catholic church service in Wisconsin, as she usually does with her family on Sundays. Presidential elections were scheduled for November 8, 2020, and amidst the COVID-19 pandemic, political campaigners were utilizing innovative tactics to get more citizens to register to vote. Enza was convinced the elections did not really matter to her, and she had never been particularly interested in politics anyway. After attending the service that day, however, Enza was at home scrolling through social media when a Trump presidential campaign ad caught her attention. It showcased her information ostensibly aligned with Catholic values and encouraged her to register to vote. From an outsider's perspective, Enza seemed to have been targeted by CatholicVote, an organization that was working on one of the largest voter mobilization programs of the 2020 presidential elections.[1]

While Enza is a hypothetical character in this story, the location targeting tactic is not a hypothetical scenario. CatholicVote used these techniques in Wisconsin to identify and target Catholics and to persuade them to vote.[2] The Republican campaign mined church worshippers' data and later showed them campaign ads to get them to register to vote using geotargeting technology.[3] Political campaigns such as this one are increasingly utilizing big data, including location data, to target citizens with personalized political ads. This practice – also called micro-targeting – identifies voters who are assumed to be more easily convinced based on their identified interests and vulnerabilities.[4]

Individual users of a given app or technology provide consent to the ubiquitous terms and conditions provided upon download or purchase.[5] However, by virtue of giving their consent, users often inadvertently provide the companies or organizations behind the tools with access to a variety of data on their personal life, including browsing details, purchase behavior, voting habits, viewing habits, frequently texted people, most visited friends, frequently visited places, past and future travel itineraries, reading habits, number of people in the household, age, gender, and more. Consenting to use apps carries implications, often unintended ones, that surpass economic exploitation by commercial actors and can allow political actors to take advantage.

Location data provides information that, when combined with other forms of data, can indicate interests and allow political entities to micro-target individuals with personalized ads which may convince or sway voters.[6] This paper focuses on the history, trajectory, tools, and examples as they relate to location-based targeting.

LOCATION -BASED TARGETING: ORIGIN, USAGE, AND FUTURE POTENTIAL

Location-based targeting is utilizing a person's granular location data to target them with online or offline messaging based on their physical location.[7] When siloed, one piece of information alone may not prove to be a significant threat to one's privacy. However, combining that information with other granular data points, such as location data, gradually removes layers of privacy, leading to many possible opportunities to target and potentially deceive voters.[8]

Global Positioning System (GPS)

The origins of location-based targeting in America trace back to 1951, when Dr. Ivan Getting designed a three-dimensional system that utilized the time difference of radio signal arrivals to identify precise positions.[9] This technology was further enhanced with the launch of Sputnik, the first artificial satellite, in 1957. The launch showed that if the position of the satellite was known, the position on earth could be determined. These developments led to the invention of the Global Positioning System, primarily designed for the American Navy to track missiles underwater.[10] Global Positioning System, popularly known as GPS, is a U.S.-owned utility system that provides information on positioning, navigation, and timing services catering to space, military, and user-related endeavors.[11] For the purposes of tracing the history of location-based targeting, this paper focuses on the user segment of GPS utility, which is widely used by the public in mapping devices in their cars and phones.

Four years after its invention in 1959, the outline for the basis of modern GPS was planned, as the Department of Defense wanted to establish a reliable and robust satellite navigation system.[12] However, it was not until 1985 that GPS was made available to the public through wearables with GPS systems that were made by private companies.[13] Although private companies were able to utilize the system, the U.S. Department of Defense continued to maintain so-called 'Selective Availability' for national security reasons by intentionally introducing random error into the version used by the public.[14]

It was not until 2000, when the Clinton administration made GPS an open-source utility, that GPS became responsive to civil and commercial use by being able to provide accurate location information, thus ending 'Selective Availability'.[15] This development in the U.S. was a turning point worldwide for GPS utility in both being able to provide the public with accurate mapping information and in providing private companies with an important and accurate data layer to utilize in cars, computers, and mobile devices. This development was the first step towards easy and precise navigability for a larger public, paving the way for applications that use GPS data such as Google Earth, which renders 3D images of earth using satellite data. However, Google Earth has been criticized for its use by law enforcement as well as for its lack of security in regard to satellite images that are updated regularly and that provide

information on military bases, which could be potentially utilized by terrorists.[16] In America, GPS data-enabled geofencing technology soon paved the way towards geotargeting and geopropaganda.

Key Terms

Geolocation data	Data that describes the relationships between places, people, and time.[17]
Geotargeting	The practical use of geolocation data to target individuals and deliver personalized and location-specific content to their (internet-based) devices.[18]
Geofencing	The practice of drawing a virtual/digital boundary or a 'fence' around a physical location to identify and/or target individuals at a specific location.[19]
Geopropaganda	The use of location data by political entities to influence political discussions and decisions.[20]

Development of Geofencing Technology

While companies like Garmin and TomTom inserted live GPS in cars to allow for mapping and navigability, it was Qualcomm – a wireless technology company – that was first to implement live GPS in mobile phones. At the time, mobile phones came with 3G broadband[21] that had just enabled global radio access and sharing of multimedia messages (MMS).[22] Given that the only data available on mobile devices at this time was GPS, private companies began to identify methods to better utilize GPS to demarcate physical locations by drawing digital fences to identify a specific location, or 'geofenced' area.

Geofencing technology is defined as a virtual or digital parameter that is dynamically drawn around a physical location.[23] The fenced area can be as small as a polling booth or as wide as a football stadium.[24] Early use of geofencing technology was used to protect vulnerable populations – for example, to alert patients through a GPS tracker if their children traveled outside a predefined area or to keep Alzheimer's or dementia patients from wandering off – or to track and monitor people on parole.[25] Under the regulation of the Federal Communications Commission (FCC), geofencing technology was approved to be used for emergency location (or E911) purposes for precise location identification.[26] However, the legal standards and usage of this approval was questioned by the Center for Democracy and Technology, a non-profit organization that argued that cell phones were now a tracking device to be used for surveillance by law enforcement.[27]

In work environments, GPS tracking was used for efficiency purposes by tracking employees with a check-in and check-out time, by notifying employees who were closest to a certain customer, and even by notifying employers if an employee left a pre-defined area.[28] The transition from a public utility technology towards surveillance technology was seamless at this time and raised many ethical concerns around real-time tracking and monitoring in relation to people's rights to freedom and privacy.[29]

Technological Advancements in Location Identification: Wi-Fi, IP, and Cellular Data

While the applications and uses of geofencing continued, technology companies and cellular broadband continued to make strides in location technology. The years following 2007 were marked by a dramatic shift: The launch of the iPhone showcased the limitless utility of a mobile device through crucial features such as internet access and easy browsing navigability with a multi-touch interactive screen. Broadband technology made strides with the launch of 4G that enabled faster data processing and efficiency of radiofrequency. This was also the first time that 4G networks would follow an all-IP standard, meaning that while 3G utilized IP for data transfer only, 4G would use IP for all data, including voice data, thus enabling the transfer of high speed and low-cost information.[30]

IP, or Internet Protocol, is a set of rules or a protocol that defines how data is shared over a public network, the internet.[31] The availability of IP on devices connected each device to a physical location.[32] IP, along with one of the early location identifiers predating GPS and the usage of cellular tower data, provided multiple types of location data to enable accuracy and granularity.[33] Cellphone towers, or base stations, are physical network locations that provide cellular service to devices and, at the same time, provide that device's location data back to the service provider.[34]

Furthermore, wireless technology (or Wi-Fi, a collection of wireless network protocols typically used for local area networking and internet access in both business and home environments[35]) became publicly available in 1999. By 2010, it had become prevalent in mobile devices, thereby adding yet another location data point. In recent years, location data also started being tracked through mobile applications. When an application is downloaded onto a mobile device, the Software Development Kit (SDK) of that application has location preferences requested, which is often turned on as the default.[36] Thus, these third-party applications can track a user's location data with the same level of accuracy as the other technologies.

GPS, Cellular data, Internet Protocol, Wi-Fi, and SDK technologies work together in a mobile device to further enhance one data point – location of that device – to be more efficient in addressing user applications such as navigation and emergency calls.[37] But in order to perform these tasks, the device's location data has to be recorded and captured.

As smartphones became ubiquitous, location-data features such as maps and weather became widely available and provided a level of convenience to users.[38] As the era of big data expanded the scope of data collection, this also presented an opportunity to further commodify location-based data.

Geolocation Technologies

Global Positioning System (GPS)	Global Positioning System, or GPS, is a U.S.-owned utility system that provides information on positioning, navigation, and timing services and which caters to space, military, and user-related endeavors.[39]
Internet Protocol (IP)	Internet Protocol, or IP, is a set of rules that defines how data is shared over the internet and defines the address space of devices on the internet.[40]
Cellphone Tower	Cellphone Towers, or base stations, are physical network locations of cellular service providers that provide cellular service to devices and, at the same time, provide that device's location data back to the service provider.[41]
Wi-Fi	Wi-Fi is a collection of wireless network protocols typically used for local area networking and internet access in both business and home environments.[42]
Software Development Kit (SDK)	Software Development Kit, or SDK, is a collection of software development tools that is used to develop mobile applications and host trackers that enable tracking and sharing of data, including location data.[43]
Quick Response or QR Codes	QR, or Quick Response, codes are machine-readable matrix barcodes that contain information or data about an item that can be used to track and identify specific details such as websites or locations.[44]
Beacon	Beacons, or Bluetooth beacon technology that was invented by Apple, are small wireless transmitting devices that can track and send signals to devices nearby.[45]
Application Programming Interface (API)	Application Programming Interface (API) enables software applications to exchange data, including location data, and function seamlessly with other entities.[46]

Big Data and Its Commodification

The launch of Foursquare during South by Southwest in Austin in 2009 marks a turning point in the geotargeting ecology.[47] Foursquare (today called Swarm) is a location-based social media app that allows users to earn badges by frequenting places and logging their geographic activities.[48] While users compete with friends to become 'mayors' of places such as their favorite coffee shop, Foursquare/Swarm sells the data to advertisers. Foursquare/Swarm also opened its API (Application Programming Interface) the same year of its launch, enabling developers to access data and build applications on top of that data.[49] Openly accessible APIs marked a seismic shift in the technology world, as they allowed for developers to seamlessly build programs that can gather and match data points from multiple first-party sources.

First-party data is the information companies collect and store from their own sources.[50] Websites often collect data for web service sign-ups such as email, newsletter, music applications, subscriptions, and even purchases.[51] Google, Facebook, and Amazon are primary examples of first-party data companies as they collect and own data of their own users. Thus, these platforms own personal data such as name, age, gender identity, or email address alongside location data which are utilized by advertising campaigns.

Third-party data is the information used by companies who purchase data from multiple first-party data providers and combine them to build a user profile containing multiple data points of that individual.[52] Utilizing third-party data means that companies can not only identify users' locations in relation to a predefined location, but can also connect the location with a user's likes, dislikes, purchasing behavior, and browsing behavior among thousands of data about a single user.[53] This gave rise to geotargeting in the advertising industry, utilized to target advertisements to potential customers in order to influence future behavior. Advertisers work with a foundation of persuasion in changing behaviors by showing the right message, at the right time, in the right place, to the right target.

Precise Consumer Targeting Using Location-Based Technology: QR Codes and Beacons

Supermarkets and retailers are prime examples of innovation in using data to create a formula for attracting more consumers. Consumer data points include location data, socioeconomic status, and where a consumer is in their purchase cycle, which leads to personalization that can easily help evaluate not just a consumer's store location, but their location inside the store.[54] Retailers were also innovators in using the newer technologies that are often used in geotargeting, QR codes, and beacons.[55]

QR, or Quick Response, codes are machine-readable matrix barcodes invented in 1994 that contain information about the item attached.[56] Practically, QR codes contain data that can track and identify specific details such as websites or locations. Beacons, or Bluetooth

beacon technology that was invented by Apple, are small wireless transmitting devices that can track and send signals to devices nearby.[57] The market for beacon technology is predicted to exceed $25 billion by 2024, which can mainly be attributed to continuing increases in market penetration of mobile devices as well as the growing need for proximity targeting within location-based targeting solutions.[58] 5% of that growth is set to be held by retailers who utilize beacons to help transmit messages to a shopper's mobile device when they are at close proximity to increase revisits and impulse purchases.[59] Macy's was one of the first retailers to enable QR codes and took to a digital-first approach with GPS tracking for in-store analytics, along with placement of beacons – meaning that consumer's interactions with the retail ecosystem are all captured to analyze and help maintain a consistent and continuous relationship with the consumer, in order to enable brand loyalty.[60]

Beacons are unique in that they are currently the most precise location technology and are also inexpensive.[61] Beacons are said to collect data from a device nearby without sending any signals to that device as long as it has its Bluetooth turned on.[62] Furthermore, they do not need to be physically altered for their collection purposes to change, which can be done in the cloud.[63] A beacon once employed for one purpose can be changed and employed for another.[64] Due to these significant realms of application, beacons were used by the Trump 2016 campaign by placing them on lawn signs and tracking and signaling nearby mobile devices with campaign messages.[65] While this in itself does not pose a threat to privacy, Trump's campaign page updated its Terms & Conditions by 2020 to include language that allowed them to "collect information from smartphones using beacons," propelling the campaign's ability to micro-target users with personalized political messages to sway their votes.[66]

FROM PERSUASION TO PROPAGANDA: GEOLOCATION-BASED TARGETING MAKING ITS WAY INTO POLITICS

In Guyana's 2015 elections, the left-wing party, the People's Progressive Party, was trumped by its opposition, the People's National Congress, after 23 years with the help of IP targeting by El Toro, an advertising technology company based in Louisville, Kentucky.[67] In this instance, a country in the northern mainland of South America recorded a big win for the right-wing party; this win was even more significant considering that the government-controlled TV and radio, making those media inaccessible to the opposition candidate as a means for reaching voters.[68] David Granger, the 2015 Guyana presidential candidate who ultimately won the election, used El Toro's services to apply location-based ad targeting to deliver political messages.[69]

One of the early instances where geo-technology was utilized in American politics was when Senator Lisa Murkowski's campaign utilized geo-fencing technology to target the U.S. Department of the Interior with advertisements. The advertisements advocated for allowing Alaska to build a road through a wildlife refuge with the purpose of making two remote towns more accessible, a project which the Department of the Interior had been declining, citing environmental concerns.[70] The Senator's campaign decided to target to Interior Department officials during lunchtime browsing with a geo-targeted YouTube video ad on Facebook urging them to take action.[71] The petition to build the road was later approved by the Trump administration, subsequently to be fulfilled by the Biden administration.[72]

With realms of applicability stretching from voting rights groups who encourage voting by mail-in ballots in majority-black neighborhoods in Georgia[73] to groups promoting pro-life messages such as free ultrasounds targeted near abortion clinics in the country,[74] location-based targeting has clawed its way into politics, raising questions about ethics and about the technology's impact on the future of the political landscape. As geotargeting technologies are extending into the political space, they thus constitute geopropaganda.

Geopropaganda, a subset of computational propaganda, is the gathering of digital location data and its use in political messaging and advertising across a variety of platforms to manipulate public opinion.[75] Voting data – through voter files – is generally available at the state, county, and congressional district level, with basic demographic information at a household and individual level.[76] This data, along with behavioral data, can provide insights on consumers in that area that allow them to be targeted with relevant and persuasive political messaging.[77] Combined with the granularity of location data, narrow political ad targeting, including geotargeting, is being increasingly utilized in political communication.[78]

In prior work, the Propaganda Lab at the Center for Media Engagement established the importance of using campaign applications as a means for presidential candidates to talk directly to their voters and as a way to collect data without relying on third-party applications.[79] In 2020, both the Biden and Trump campaigns utilized geotargeting strategies to target and mobilize their voters.[80] From mining data by geofencing political rallies to geotargeting at an individual level based on socioeconomic status and cultural values, the political campaigns actively utilized location-based technologies to gain momentum and votes. The sophistication of these technologies allows for a platform-agnostic approach, wherein an ad is not limited to mobile devices and can be shown to a potential voter on their television by mapping the IP address to that household.

While nonprofit organizations such as the American Civil Liberties Union (ACLU) are highlighting the consumer privacy and surveillance perils of location-based targeting, the public's dependency on technologies that utilize this data, along with the lack of legal and regulatory restrictions, make the future of privacy appear bleak.[81] With more

political campaigns around the globe utilizing location-based targeting, geopropaganda is increasingly at the forefront of political campaigns.[82]

Examples of Political Campaign Usage of Geopropaganda

Example	Description
CatholicVote's targeting of Catholic churchgoers in 2020[83]	This lobbying organization used geofencing of churches to identify Catholics who frequently attended services. After cross-referencing this with other data, they were able to identify Catholics that were not registered to vote and target them with personalized content.
Sen. Lisa Murkowski's campaign's targeting of the U.S. Department of the Interior in 2016[84]	Sen. Lisa Murkowski's campaign geofenced the U.S. Department of the Interior building to rally support for their cause of permitting a road through a wildlife refuge.
El Toro's support in the Guyanese Presidential elections in 2015[85]	David Granger, a 2015 Guyana presidential candidate who ultimately won the election, used El Toro's services to apply location-based ad targeting in delivering political messages.
Republican candidate and former president Donald J. Trump's campaign's targeting of voters in 2016 and 2020[86]	Republican candidate and former President Trump's campaign placed beacons on lawn signs to track and signal nearby mobile devices with campaign messages. In 2020, Trump's campaign page updated Terms & Conditions to include language that allowed them to "collect information from smartphones using beacons" to geotarget voters with personalized content.

CONCLUSION

Tracing the origins of geolocation targeting from defense purposes to commercial usages and finally to political purposes makes clear how important this practice has become in a larger digital ecology. As with all data, concerns arise as data get used for questionable measures. For example, commercial actors such as personal injury law firms have been accused of preying on vulnerable people for profit by targeting patients in emergency rooms with geofencing technology.[87] At the same time, law enforcement agencies use geofence search warrants, also known as reverse location search warrants, with relatively expansive geofence areas to retrieve location data and identifiers about people.[88] These warrants risk over-inclusion of unwitting individuals (and their data) in the perimeters of the warrants.

Companies continue to push the boundaries and pursue what's practically possible, often with little regard for the ethical implications and potential repercussions of the technology. This is not to say that geolocation targeting has not been or could not be put to good use. But the basis of geolocation targeting, the combination of location data with other data points to directly target content on the basis of location, especially when individuals are unaware of how and why a particular message has reached them, is concerning. The following actions and deliberations could be considered:

- **Addressing consent**: Lengthy terms and conditions that allow the described usage of user data are too complex and hence often ignored. To address this issue, policymakers could introduce a mandatory summary prefacing terms of service, which might have more potential to be read by users. For this summary, a survey drafted and rolled out by independent researchers asking for users' biggest concerns with regard to their data could inform which points make it into the mandatory summary. An example of addressing potentially unfair terms of service is the 2021 Irish Consumer Rights Bill, which is national legislation working to implement the EU's Digital Content Directive (Directive 2019/770) and which introduced a "black list" of contractual terms and conditions that are always considered unfair and hence need to be omitted by companies.
- **Addressing competition**: Accepting the terms of service before downloading an app or signing up for a service are often also seen in a fatalistic manner; in other words, users don't think they have a choice as they are unaware of competing apps or services. In this case, competition that pushes profit-seeking actors to consider user demands more prominently could be encouraged. To do this, public campaigns showcasing what different apps and services do with user data and how they differ could reach many people and have the potential to attract people to platforms that value their privacy. The impact that public debate can have was demonstrated

when many WhatsApp users shifted to other messaging apps, such as Signal, after WhatsApp announced a privacy update that would enable data sharing with its parent company Facebook.[89]

- **Addressing legislation**: The increase in geofence warrants over the past three years has further ignited a conversation on a right to privacy since – in the case of geofence warrants – data is collected from everyone within a specific geofenced area irrespective of background or suspicion.[90] While these warrants themselves are relatively new, their origins date back to 2004 when federal agents investigated an individual on drug trafficking by placing a GPS tracker in the car to track their movement and locations.[91] And while traditional search warrants require physical entry and need to fulfill several preconditions before being permitted by a judge, digital warrants seem easier to obtain. This points to the need for federal privacy regulation, including with regard to location data.[92]
- **Addressing transparency**: If all stakeholders ranging from political campaigners relying on geolocation data to technology companies providing the data take transparency seriously, citizens would be in a much stronger position to know how their data is used, as well as identify and protect themselves from potential deception based on geolocation targeting. First steps in this direction have been taken, such as when Google published a transparency report in 2021 showing that 25% of data requests from law enforcement to Google were geofence data requests. While Google is the most common recipient of geofence warrants, other companies including Apple, Snapchat, Lyft, and Uber have also received such warrants.[93] Non-profit organizations such as the Electronic Frontier Foundation (EFF) argue that some geofence warrants violate deep-rooted Fourth Amendment law; part of their successes in court are based on judges' convictions that warrants were overbroad.[94] In other words, while the courts agreed that the government had established probable cause that a single cell phone user within the geofence might have committed a crime, the courts also held there was no probable cause to believe all the other devices in the area were connected to the crime as well. Therefore, in these cases, courts rejected the government' argument that search warrants were narrowly tailored. This points toward an understanding that technical possibilities – enabled by geolocation data – are harnessed by law enforcement as well as commercial companies. While these issues won't be solved fast, increased transparency could at least enhance accountability.
- **Addressing accountability**: Lastly, it is imperative that critical news coverage accompanies a diversifying roster of geolocation data techniques. Journalistic coverage and investigative reporting can increase public pressure on various actors lured by the potentials of geolocation targeting.

ACKNOWLEDGEMENTS

This report was funded by Open Society Foundations, Omidyar Network, and the John S. and James L. Knight Foundation.

ENDNOTES

[1] Eaton, J. (2019, July 19). Catholics in Iowa went to church. Steve Bannon tracked their phones. *ThinkProgress.* Retrieved from https://archive.thinkprogress.org/exclusive-steve-bannon-geofencing-data-collection-catholic-church-4aaeacd5c182/.

[2] Schlumpf, H. (2020). Pro-Trump group targets Catholic voters using cellphone technology. *National Catholic Reporter.* Retrieved from https://www.ncronline.org/news/parish/pro-trump-group-targets-catholic-voters-using-cell-phone-technology.

[3] Schechner, S, Glazer, E, Haggin, P. (2019, October 10). Political Campaigns Know Where You've Been. They're Tracking Your Phone. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889.

[4] Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., ... & de Vreese, C. H. (2018). Online political microtargeting: promises and threats for democracy. Utrecht Law Review, 14(1), 82-96.

[5] Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128-147.

[6] Eddy; Zuiderveen Borgesius, F. et al.

[7] Valentino-DeVries, J., Singer, N., Keller, M. H.. & Krolik, A. (2018, December 10). Your apps know where you were last night, and they are not keeping it secret. *The New York Times.* Retrieved from https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[8] Valentino-DeVries et al.; Zuiderveen Borgesius, F., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., ... & de Vreese, C. H. (2018). Online political microtargeting: promises and threats for democracy. Utrecht Law Review, 14(1), 82-96.

[9] Alexandrow, C. (2008). The story of GPS. In R. Carpenter (Ed.), DARPA: 50 years of bridging the gap (pp. 54-55). Defense Advanced Research Projects Agency. Retrieved from https://www.darpa.mil/attachments/(2O10)%20Global%20Nav%20-%20About%20Us%20-%20History%20-%20Resources%20-%2050th%20-%20GPS%20(Approved).pdf.

[10] Mai, T. (2017, August 7). Global Positioning System History. NASA. Retrieved from https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html.

[11] National Coordination Office for Space-Based Positioning, Navigation, and Timing (2017). The Global Positioning System. Retrieved from https://www.gps.gov/systems/gps.

[12] Alexandrow.

[13] Zumberge, J. F., & Gendt, G. (2001). The demise of selective availability and implications for the international GPS service. Physics and Chemistry of the Earth, Part A: Solid Earth and Geodesy, 26(6-8), 637-644; Edwards, B. (2015). Who needs GPS? The forgotten story of Etak's amazing 1985 car navigation system. Fast Company.

[14] Zumberge, & Gendt.

[15] National Coordination Office for Space-Based Positioning, Navigation, and Timing. The Global Positioning System. Retrieved from https://www.gps.gov/systems/gps/modernization/sa/.

[16] Velho Diogo, G. (2016, October 7). Google Earth, Surveillance, and the Power of Digital Cartography. Institute of Network Cultures. Retrieved from https://networkcultures.org/longform/2016/10/07/google-earth-surveillance-and-the-power-of-digital-cartography/.

[17] Arminen, I. (2006). Social functions of location in mobile telephony. *Personal and Ubiquitous Computing*, *10*(5), 319-323.

[18] Bandy, J., & Hecht, B. (2021). Errors in geotargeted display advertising: Good news for local journalism?. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1-19.; Bashyakarla, V. (2018, September 11). Geotargeting: The political value of your location. *Tactical Tech.* https://ourdataourselves.tacticaltech.org/posts/geotargeting/; Chen, Y., Li, X., & Sun, M. (2017). Competitive mobile geo targeting. *Marketing Science, 36*(5), 666-682.; Poese, I., Uhlig, S., Kaafar, M. A., Donnet, B., & Gueye, B. (2011). IP geolocation databases: Unreliable?. *ACM SIGCOMM Computer Communication Review*, *41*(2), 53-56.

[19] Küpper, A., Bareth, U., & Freese, B. (2011, October). Geofencing and background tracking–the next features in LBSs. In *Proceedings of the 41th Annual Conference of the Gesellschaft für Informatik eV.*

[20] Joseff, K., Woolley, S. (2020, May 22). COVID-19 isn't the only threat to privacy. *Foreign Affairs.* https://www.foreignaffairs.com/articles/2020-05-22/covid-19-isnt-only-threat-privacy.

[21] Chidi, A.G., (2002, January 18). Qualcomm turns cell phones into GPS systems. CNN. Retrieved from https://www.cnn.com/2002/TECH/ptech/01/18/qualcomm.gps.idg/.

[22] Agrawal, J., Patel, R., Mor, P., Dubey, P., & Keller, J.M. (2015). Evolution of Mobile Communication Network: from 1G to 4G. International journal of multidisciplinary and current research, 3.

[23] Küpper et al.

[24] Küpper et al.

[25] Mcnamee, A. (2005). Ethical issues arising from the real time tracking and monitoring of people using GPS-based location services. Honors thesis. University of Wollongong. https://ro.uow.edu.au/thesesinfo/4.

[26] Oaks,C. (1998). 'E911' Turns Cell Phones into Tracking Devices. *Wired.* Retrieved from https://www.wired.com/1998/01/e911-turns-cell-phones-into-tracking-devices/.

[27] Oaks.

[28] Mcnamee.

[29] Mcnamee.

[30] A. H. Khan, M. A. Qadeer, J. A. Ansari and S. Waheed (2009). 4G as a Next Generation Wireless Network. 2009 International Conference on Future Computer and Communication, 334-338. doi: 10.1109/ICFCC.2009.108.

[31] OECD (2014). The Economics of Transition to Internet Protocol version 6. OECD Digital Economy Papers. Np. 244. Retrieved from https://read.oecd-ilibrary.org/science-and-technology/the-economics-of-transition-to-internet-protocol-version-6-ipv6_5jxt46d07bhc-en#page1.

[32] OECD.

[33] Funakoshi, M., Culliford, E., & Foo, W. (2020, October 12). How political campaigns use your data. Reuters. Retrieved from https://graphics.reuters.com/USA-ELECTION/DATA-VISUAL/yxmvjjgojvr/.

[34] Mcnamee.

[35] Henry, P. S., & Luo, H. (2002). WiFi: what's next?. *IEEE Communications Magazine*, *40*(12), 66-72.

[36] Eddy.

[37] McGuire, R. (2007). The power of mobility: How your business can compete and win in the next technology revolution. John Wiley & Sons.

[38] Valentino-DeVries et al.

[39] National Coordination Office for Space-Based Positioning, Navigation, and Timing.

[40] OECD.

[41] Mcnamee.

[42] Henry & Luo.

[43] Morrison, S (2020, July 8). The Hidden Trackers In Your Phone Explained. *Vox.* Retrieved from https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location.

[44] Denso Wave Incorporated (2021). *History of QR code.* Retrieved from https://www.qrcode.com/en/history.

[45] Binder, M. (2019). Republican campaign put beacons on lawn signs to track phones, company says. *Mashable.* Retrieved from https://mashable.com/article/beacons-location-tracking-republican-campaign.

[46] IBM Cloud Education. (2020, August, 19). Application Programming Interface (API). *IBM.* Retrieved from https://www.ibm.com/cloud/learn/api.

[47] McCracken, H. (2019). Foursquare's first decade, from viral hit to real business and beyond. Fast Company. Retrieved from https://www.fastcompany.com/90318329/foursquares-first-decade-from-viral-hit-to-real-business-and-beyond.

[48] McCracken.

[49] Siegler, MG. (2009). Foursquare Lets Others Play With Its API. *TechCrunch.* Retrieved from https://techcrunch.com/2009/11/16/foursquare-api/.

[50] Mayer, J. R., & Mitchell, J. C. (2012, May). Third-party web tracking: Policy and technology. In 2012 IEEE symposium on security and privacy (pp. 413-427). IEEE.

[51] Mayer, & Mitchell.

[52] Mayer, & Mitchell.

[53] Mayer, & Mitchell.

[54] Turow, J. (2017). The aisles have eyes. Yale University Press.

[55] Turow.

[56] Denso Wave Incorporated.

[57] Statler, S., Audenaert, A., Coombs, J., Gordon, T., Hendrix, P., Kolodziej, K., … & Rotolo, R. (2016). Beacon technologies (p. 21). Berkeley: Apress.

[58] Wadhwani, P. (2018). Beacon Technology Market Set to Surpass $25 Billion by 2024. RFID Journal. Retrieved from https://www.rfidjournal.com/beacon-technology-market-set-to-surpass-25-billion-by-2024.

[59] Wadhwani.

[60] Turow.

[61] Statler et al.

[62] Statler et al.

[63] Statler et al.

[64] Binder.

[65] Binder.

[66] Binder.

[67] Aretakis, R. (2015, June 19). Louisville startup helps client win Guyana presidency. *Louisville Business First.* https://www.bizjournals.com/louisville/blog/2015/06/louisville-startup-helps-client-win-guyana.html.

[68] Aretakis.

[69] Aretakis.

[70] Hill, K. (2016, April 21). How a Senator used Facebook ads to influence employees in a single D.C. building. *Splinter.* https://splinternews.com/how-a-senator-used-facebook-ads-to-influence-employees-1793856310.

[71] Hill.

[72] Bies, L. (2021, March 17). Biden administration supports refuge-splitting road in Alaska. *The Wildlife Society.* Retrieved from https://wildlife.org/biden-administration-supports-refuge-splitting-road-in-alaska/.

[73] Corasaniti, N. (2020, June 2). Geofencing at the ballot box. The New York Times. Retrieved from https://www.nytimes.com/2020/06/02/us/politics/geofencing-absentee-ballots.html.

[74] Choose Life. (2021, September 14). Reaching women early in pregnancy. *Choose Life Marketing.* Retrieved from https://www.chooselifemarketing.com/reaching-women-early-in-pregnancy/.

[75] Woolley, S. C., & Howard, P. N. (Eds.). (2018). Computational propaganda: Political parties, politicians, and political manipulation on social media. Oxford University Press.

[76] Funakoshi, M., Culliford, E., & Foo, W. (2020, October 12). How political campaigns use your data. *Reuters*. Retrieved from https://graphics.reuters.com/USA-ELECTION/DATA-VISUAL/yxmvjjgojvr/.

[77] Funakoshi.

[78] Joseff, K., Carter, J., & Woolley, S. (2021, February 11). The disturbing implications of increasingly narrow political ad targeting. *Brookings TechStream.* Retrieved from https://www.brookings.edu/techstream/the-disturbing-implications-of-increasingly-narrow-political-ad-targeting/.

[79] Glover, K., Gursky, J., Joseff, K., & Woolley, S. C. (2020, October 28). Peer-to-Peer texting and the 2020 U.S. election: Hidden messages and intimate politics. Center for Media Engagement. https://mediaengagement.org/research/peer-to-peer-texting-and-the-2020-election.

[80] Schechner et al.

[81] Stanley, J. (2018, December 11). There's nothing inevitable about apps that track your every move. *American Civil Liberties Union.* Retrieved from https://www.aclu.org/blog/privacy-technology/location-tracking/theres-nothing-inevitable-about-apps-track-your-every-move.

[82] Crampton, J.W., Waterson, J., & Dugan, E. (2017, June 7). The Tories are exploiting a new spending loophole to launch a last-minute Facebook Ad Blitz. *BuzzFeed.* Retrieved from https://www.buzzfeed.com/jimwaterson/the-tories-are-exploiting-a-new-loophole-to-launch-a-last; Gursky, J., Glover, K., Joseff, K., Riedl, M.J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico. Center for Media Engagement. https://mediaengagement.org/research/encrypted-propaganda.

[83] Schlumpf.

[84] Hill.

[85] Aretakis.

[86] Binder.

[87] Allyn,B. (2018). Digital Ambulance Chasers? Law Firms Send Ads To Patients' Phones Inside ERs. NPR. Retrieved from https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers.

[88] Fussell, S. (2021). An explosion in geofence warrants threatens privacy across the U.S.. *Wired.* Retrieved from https://www.wired.com/story/geofence-warrants-google.

[89] Curry, D. (2021). Signal Revenue & Usage Statistics. Business of Apps. Retrieved from https://www.businessofapps.com/data/signal-statistics/.

[90] Fussell.; O'Brien, T. (2021 November 12). New writs of assistance: Geofence warrants and the Fourth Amendment. *SSRN.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834623.

[91] O'Brien.

[92] Laperruque, J. (2021, August 25). Geofence warrants: The last piece of the location privacy puzzle. *Project On Government Oversight (POGO).* Retrieved from https://www.pogo.org/analysis/2021/08/geofence-warrants-the-last-piece-of-the-location-privacy-puzzle/.

[93] Rathi, M. (2021). Geofence warrants and the Fourth Amendment. *Harvard Law Review*. (2021, May 10). Retrieved from https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment/;

Rathi, M. (2021). Rethinking Reverse Location search warrants. *The Journal of Criminal Law and Criminology*, 111(3), 805–837.

[94] Lynch, J., & Sobel, N., (2020, August 31). New federal court rulings find geofence warrants unconstitutional. Electronic Frontier Foundation (EFF). Retrieved from https://www.eff.org/deeplinks/2020/08/new-federal-court-rulings-find-geofence-warrants-unconstitutional-0.