Geolocation:

Addressing

The Rights Regarding

Our Location Information

Zofia Czarnik & Ariel Rosenberg

Mentored by Evan Oxman

Executive Summary

Geolocation, or an individual's real time location accessible through the internet, has gained traction as an issue of concern within the past decade. There is initially nothing harmful with geolocation as a concept. Geolocation is helpful to show certain trailers in areas it might be a hit, or tell a political figure which cities would be best to campaign in. It has become a tool in our everyday lives that provides a great advantage that in today's society would be ludicrous to ban. Unfortunately, the lack of regulation on the topic can potentially put individuals in danger or can be used without our knowledge. In the following paper we use Jorge Molina as an extreme example of what malstored geolocation could potentially cause. His phone, which only placed him at the scene of a crime before it happened, was used to give the officer reason that he was undoubtedly the criminal. The geolocation in the situation was obtained legally, however there should have been no reason a phone should be pinged by geolocation without an owner's knowledge. A solution to this issue might simply be an update to the way consumers are informed about the issue. After all, if Molina knew that his location would be deleted or that it would not be kept, he might not have been arrested. The following paragraphs will aim to explain why an awareness solution is best made as a company implemented regulation as opposed to a legislative or even judicial order. It will also explain why a more interactive agreement format will serve to both better protect and inform the individual as well as provide much needed transparency. As of now, ⅔ of Americans either are not informed or do not trust the information of geolocation data and it makes sense. A simple button that states “I Agree” does not make the user consider or read what they are agreeing to thus promoting a culture that is uninformed of what can be done about their location information. The solution proposed in this paper will aim to do the following: A format similar to that of what is currently being used for

online AP and other government testing provides a basis for a more engaged conformation of consent. A user would be asked to write out the top five usages and agreements that the company would want the user to know and the user would type out the statements. These statements would be updated every time the user has to make this agreement to keep information current and relevant should they change otherwise it would be reset every 6 months. There is no currently justifiable reason why a company would need a users location for anything longer than such. Once agreed to, the location tied to that user would be forced to be removed from servers unless the information is used for pending litigation. This solution is not without flaws, someone who is meditating a crime might just simply choose to not use the application. Our final paragraph will aim to explain the process if the situation were to arise along with any pushback or repercussions that might come as a result of both initial implementation and the proposed process as a whole.

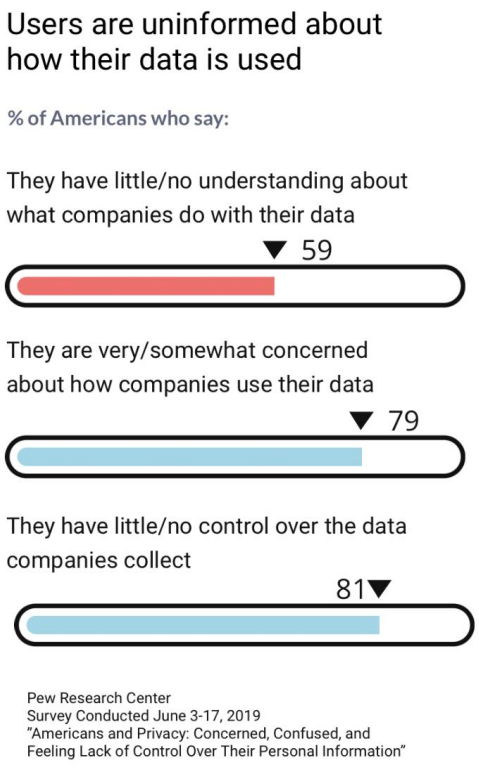
The Issue

Jorge Molina spent six days in prison for a crime he didn't commit. A murder in Arizona in March of 2018 remained unsolved for nearly nine months, leading law enforcement to turn to Google to help close the case. Law enforcement utilized their warrant issuance right to obtain data on who was near the crime scene around the time of the murder from Google's user location database, Sensorvault; the data indicated Jorge Molina as the perpetrator, and -- without any prior notice or knowledge of being investigated -- he was subsequently arrested by police "without a doubt" (according to the police report) that he was the murderer ("Geofence Warrants" 2508). Six days later, Molina was released from prison. Law enforcement had come to find that Molina's location data had incorrectly placed him at the scene of the crime and consequently, all charges against him were dropped. Instead, his mother's ex-boyfriend was arrested — this time correctly — after investigators paired their reliance on geolocation data with traditional investigative methods ("Geofence Warrants" 2508-2509, Valentino-Devries).

It is not law enforcement's usage of geolocation data that is the problem. Since Sensorvault's creation in 2009, law enforcement has been able to frequently request geolocation data to help solve crimes, whether as an isolated method or in tandem with other actions ("Geofence Warrants" 2512). That right is maintained by law and, to date, has not been successfully restricted or overturned. In numerous instances, geolocation data usage — namely with regards to improving public safety measures — have positive implications. Especially in urban areas where crime rates are high and population densities are more concentrated, law enforcement has been able to increasingly rely on valuable location data to identify, narrow down, and ultimately pinpoint perpetrators. Scores of individuals who were originally

encompassed in the geolocation data warrant (and are later dismissed as innocent) live entirely unaware that they were considered part of an investigation at all and remained uninformed that their geolocation data was being actively collected, stored indefinitely, and in many cases, shared. Both the affected and unaffected, however, "should not […] surrender all Fourth Amendment protection by venturing into the public sphere" ("Geofence Warrants" 2529).

Therein lies the problem. There are harsh implications behind cases like Molina's — ones that emphasize the reality that an individual's data is theirs in *subject* but not theirs in *control*. Molina's publicized case, along with similar ones, bring light to this very point. Technological corporations like Google have user data — from any time and any place — accessible at a moment's notice; Google itself is known to be the sole big-tech corporation that responds to warrants requesting that data (Valentino-Devries). Meanwhile, consumers are left in the dark about the rights they hold to restrict, regulate, and monitor the geolocation data held on them. This twofold problem breaches expected, but unestablished, transparency and privacy standards; current difficulties associated with personal data regulation, and unwillingness to entirely compromise on the benefits of geolocation data, lead to stagnancy on the issue.



While Molina's case can be considered an extreme example of geolocation misuse, a majority of Americans are not necessarily informed and thus they do not know what a company can be capable of doing with past location that is simply stored and never erased, currently, Google can save data for undisclosed amounts of time under the guise of wanting it to

be convenient for users to be able to access past routes when they visit the area again. There is no limit to how long someone's information can be stored and no real company justification why a user's data needs to be held onto for say 6 years after it was initially picked up. This misinformation and lack of transparency brings up the issue of convenience over inconvenience. "Conveniences" are typically responsible for overriding "inconveniences" associated with geolocation data collection. Corporations like Google, which regularly track, store, and profile this data, use some location information to help create personalized ads and retrievable history (amongst other features) for a better user experience. In turn, users hit "Allow" when a "Use Location?" request appears, or keep the option consistently turned on buried within Google's settings. As a result — regardless of whether or not geolocation data is even needed for the functionality of the platform's services — many users' locations are being tracked at nearly all times. Whether at frequently visited stores, unexplored attractions, or sensitive places like houses of worship, Google has detailed information on the places devices have been and the exact times associated with the movements. That "potentially powerful personal data" remains stored, unlimited in quantity (Worth).

Convenience, however, should not lead to blind trust. Corporations cannot be expected to give up the popular practicalities that geolocation data usage provides, and authorities cannot be expected to give up technological developments in their crime-solving methods; likewise, however, no user should be expected to give up on their control of their privacy in the midst of this reality. The underlying cause of current user detachment from privacy control is ultimately a severe lack of transparency between corporations and consumers. Actions required of consumers to share geolocation data are simple; information presented when prompted to allow for the data usage is easily understandable and digestible. Reversing permissions and regulating data sharing

is not equally as simple, whether that be deliberate or unintentional. Privacy is more complex than an unexplained switch buried deep within account settings, and large corporations fail to present consumers with crucial and clear information on this pressing topic. Consumers not only have a right to data control and regulation, but also maintain a right to have a justifiable reason to trust corporations with digital data so closely tied to their real-world individuality. In conjunction, Google holds a responsibility to handle user geolocation data in a way that is conscientious of the information's sensitivity. This includes not only implementing limits on data collection and storage, but also involving users in their privacy control and the broader privacy conversation in an informative, collaborative, and purposeful manner.

The Options

In effort to re-establish this lost trust between consumer and corporation, a reformation has to be passed. Unfortunately, a reformation at a judicial level, while effective in theory, is not effective in practice. It is common knowledge that a court's ruling decision is non-binding and can be overturned readily. In addition, while the court hearings recently on TikTok and Snapchat bring the legal issue of privacy to light, they do not provide reform to the solution — not to mention, many cases involving location privacy hardly appeal beyond a municipal court. While one might pose there is no merit to arguing this, the reason many people choose not to pursue appeals is simply due to the knowledge that a tech company might simply get a "slap on the wrist" if they are found guilty as opposed to having an argument for true reform. While the Fourth Amendment legality is definitely applicable for location tracking, the inability for courts to quickly make and *predictably* uphold reform makes the option of pursuing any solution from a purely legal standpoint ineffective; even if enforcable, it would remain ambiguous and

needlessly complicated for the average person to understand. In addition, the neutrality of their decision still leaves room for outliers that might not follow the intended data protocol with regards to usage, storage, and deletion (Leckar). Most importantly however, it is difficult to expect courtroom judges to be fully suited to handle legislation on a new frontier that even Congress does not fully understand without the significant involvement and guidance of big-tech corporations.

A second option would be to ask for legislative reform. While it seems like the most sound solution, the reality is quite the opposite. It can be counter-intuitive and inefficient to legislate a reform for such a miniscule detail of a much larger problem. Given that our solution to geofencing issues involves transparency from company to company, it is extremely difficult to come up with a singular requirement that every company needs to abide by without variation. To this extent, freedom of information and disclosure should be at the forefront of the solution for both the consumer and the corporation. If the government creates a standard for the sake of creating a standard, neither companies nor consumers will truly be able to benefit individualistically to the fullest extent. Moreover, it is evident that recent court cases have only proven that work needs to be accelerated to prevent internet breeches at a much faster pace than what would be executed by Congress. In fact, further research as will be explained later would justify this as being a reform that could potentially solve itself should Google, Apple, Microsoft, et cetera do it of their own volition.

The Proposal

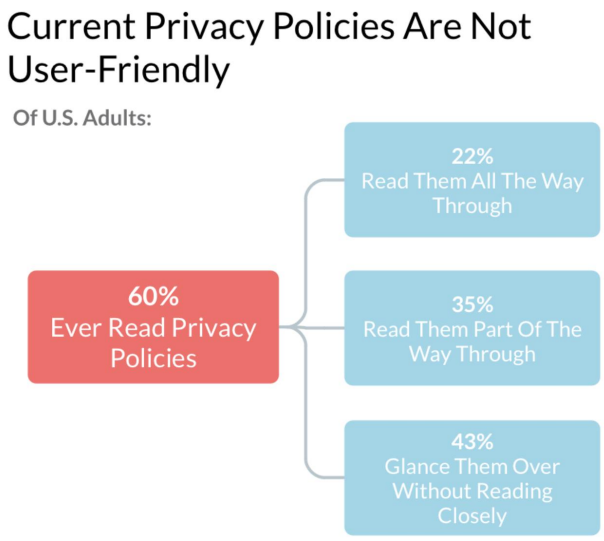
Having drawn these parallels between levels of effectiveness and viability, as well as having highlighted unignorable flaws in the aforementioned solutions, one truly applicable

solution remains. This final and officially proposed solution reflects, through careful and thorough consideration, success in the delicate balance of all key factors involved in the issue at hand. It takes into account unalterable time constraints on both the consumer side and corporation side and serves as a "rules of the road" for those who want to use location data (Worth). It maintains the integrity of the complex information held by the corporation and the need for precision and clarity for the consumer; most importantly, it allows the consumer and corporation to actively participate in the privacy conversation by bridging the gap between mass-policies and individual needs, and allowing the disproportionate level of asymmetric information to equalize for the short-term and long-term benefit of both sides.

The third and decisively most successful way to combat the issue of geofencing, therefore, is to create not a legislative law, but rather regulation that would require tech companies like Google to follow a type of multistep verification on location consent for application users. This process would require an easy to understand summary for the users that would clearly state, in plain terms, why their location is required of the application or why it would "enhance their experience," what the tech company will do with the information (including the destruction of that information after a certain period of time), and how the company will handle the information. The page would include a field asking the user to read and type out the main bullet points of the sections as an "electronic consent and signature" that would replace the small "I agree" checkbox that is currently overused by tech companies. Reasoning for this solution proves that in order to be effective, companies would have to be transparent about their usage and intentions with storing location data to their consumers in a way that avoids current legal terms that many individuals cannot not understand. In addition, it would require

customers — who often mindlessly tap the "I agree" button out of convenience — to stop and process what they are consenting to in full by using the application.

This solution initially comes in the form of traditional communication methods familiar to the consumer: a notification. Simple at face value, this form of outreach presents consumers with this initiation of "conversation" directly, allowing the next steps to build incrementally in significance upon consumer engagement. This notification, therefore, would draw upon the style of present-day widespread system alerts (Amber Alerts, Severe Weather Alerts, etc); being quickly informative and non-discriminatory would be this method's strongest characteristics. The difference would lie in content, context, and instigation. Sent regularly (with a proposed six-month time span between send-outs), the notification would give all consumers a routine reminder of the current situation enveloping technological privacy — a perilous situation in its own right in an ever-developing digital world.



Pew Research Center
Survey Conducted June 3-17, 2019
"Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information"

The notification itself would be a short message from the corporation in question that conveys the purpose of the message's arrival, the responsibility the corporation holds to provide this to the consumer, and importance of its contents. This message may be as simple as the following: "Hi! It's your team at [corporation name]. We've compiled some key points of information for you to let you know where your privacy stands with us; just tap to open at any time. Thanks!"; naturally, it should be lengthened

or shortened to fit the "voice" consumers associate with the corporations they trust and the specific point of the message. Ultimately, however, the consumer should be assured that the notification does not come at any imposition of inconvenience, but rather is an opportunity for the consumer to reciprocally fulfill a responsibility to themselves to be kept "in the loop" about the current privacy reality in the most uncomplicated and unburden-some manner possible given the factors at play. Crucially, the message should not be merely dismissible with a force-of-habit swipe; it must be opened by the user. While the corporation is in no position to force its consumers to engage in the notification at a specific time, it can encourage acknowledgment of this crucial message at the user's convenience, just as is done with "Remind Me Later" features that accompany account change requirements, software updates, and other familiar routine messages.

Upon clicking the notification, a standard scroll page will open on the user's device; it will not be a site redirection or require any further prompting from the user, but will rather appear directly on the screen. Importantly, this page should not require any adaptation or new navigation, but rather present itself with the simplicity of a corporate policy notice with emphasized clarity both in appearance and content. The corporation should, however, add to page in ways that reflect the corporation's image; while this would ideally add further visual appeal to what the consumer finds before them, it also allows for the consumer to draw a concrete, subconscious connection between the effort for transparency and privacy control and the real entity actively working towards that effort.

Conscious of the limited availability of the consumer, the corporation must demonstrate clarity and organization throughout its material. This team proposes a very specific model to follow, supported by instances of similar practices being implemented at a basic level and studies

revealing the relationship between consumers and time devoted to words on a screen. Directly upon opening, the page would contain around five, bolded, seven-to-twelve-word phrases separately highlighting the most key points of the overall message. A study researching the amount of words on a page and amount of these words read by the user reveals a very rapidly declining inverse relationship between the two. For a user to read about 85% or more of the words presented to them, on average there cannot be more than about 50 words on the page in front of them; with just an additional 50 words, the amount of words read plummets to about 50% (Harald et al, Nielsen). The goal with the five main phrases, therefore, is to both maximize readability and comprehension while highlighting the most consequential pieces of information owed to the consumer. The content of these phrases rely heavily on the exact location privacy policy pertaining to the intended audiences, but should be presented clearly and written from the perspective of a consumer. Such phrases may state messages similar to "I have a right to request deletion of my data" or "My geolocation data is accessible by law to select authorities" — ultimately providing a very personal and user-relevant overview of location privacy.

Pew Research Center
Survey Conducted June 3-17, 2019
"Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information"

Each phrase will then be interactive in serving as a drop-down point. A user can click each sentence to then reveal two subfields. The second subfield is no more than an open and honest presentation of details and relevant information pertaining to the header it falls under. This simply exists to provide users with a more in-depth coverage of their privacy's standing, the rights corporations hold, and — crucially — the rights that consumers hold. The goal of the

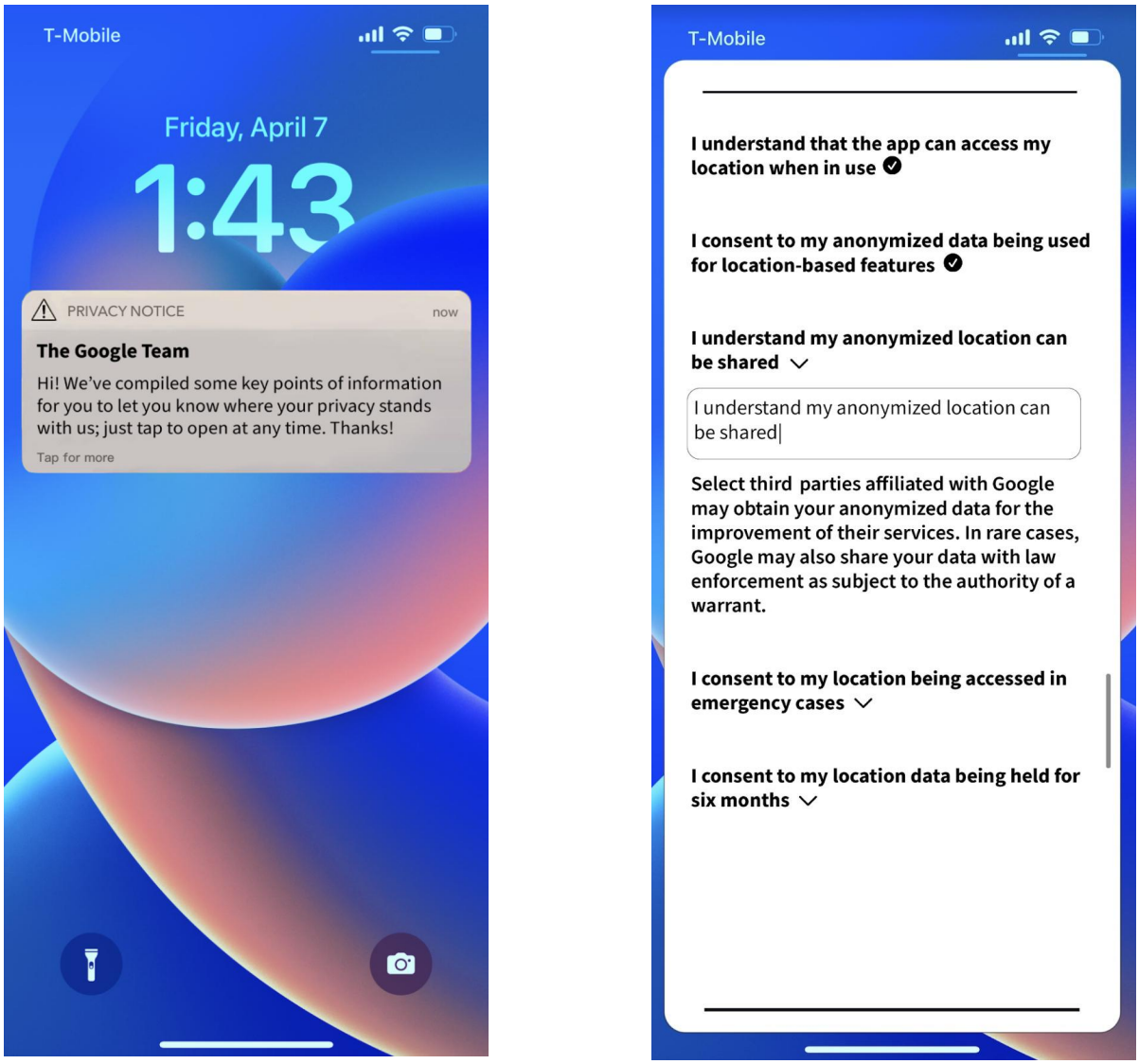
header, therefore, is to open the minds and curiosities of those reading the page to then internally prompt them to read more when that is made possible through this subfield. Again, however, the page should not fall into the trap that traditional privacy policies fall into by overwhelming users with content; the elaboration under each header should exceed no more than one hundred eleven words in striving for 50% or more user engagement; the moment anther header is clicked, the previous one collapses, so that focus remains directed throughout the process. No user can be required, nor forced, to read the information provided to them under each header, but it is in the user's interest to do so and the corporation's interest to make that possible and encourage this outcome.

The success of this solution, however, hinges significantly on the first of the two subfields. Having now addressed the issue of overly-dense information that typically overwhelms consumers, the prevailing problem of non-comprehension remains. Simplifying the information may encourage consumers to become aware of their geolocation data privacy situation in the moment, but consumers *need* to process the information being presented to them if they are to utilize that knowledge as they continue to grapple with their data's privacy and sharing in the future. To enforce the information, therefore, companies need only to implement one additional step: a subfield of restatement.

Though a seemingly simple solution, the implications of this addition are vast. By creating an area under each section in which the user can retype the short and simple header (word for word), the consumer immediately becomes actively aware of the words they just read. This technique is already implemented on a similar scale with organizations like The College Board. In order to ensure that students become aware of the regulations surrounding Advanced Placement (AP) exams, every test-taker must retype a short paragraph in which they

acknowledge what they can and cannot do during the exam. The goal is to foster awareness of contents the policy contains not just when on the policy page, but when proceeding to every page on which these regulations still apply. The logic follows similarly in this solution's application of the technique. By requiring users to retype the key points — or with possible accessibility options, utilize a voice-to-text option — the user fosters awareness of the current reality surrounding geolocation data privacy not just when on the policy page, but also when visiting any sites in the future that openly require location data collection.

An open-forum box would mark the beginning of the end of the page. True to form, this box would serve as an opportunity for individuals to share their thoughts, ideas, and concerns concerning their privacy situation, prompted by a simple "Tell us what you think" sentence preceding it; this too could be made accessible through a voice-to-text option so that each and every person has the opportunity to have their voice heard. This is crucial to making the



Proposed Model: Notification Structure (left) and Policy Structure (right)

"conversation" between the two parties truly two-sided. The goal thus far has been for corporations to be transparent about the rights and regulations they put in place, but consumers reciprocally deserve a chance to be transparent about their opinions and feelings on these regulations and how it positively or negatively impacts them in ways not necessarily addressed by the corporation.

Finally, at the ultimate end of the page, the corporation would place a notice stating that upon submitting the completed policy, some action will be taken to protect data privacy. Ideally, the corporation would have this be an acknowledgement-and-consent method for data deletion; in other words, upon reevaluating the current geolocation privacy situation every six months (or the time frame chosen by the corporation), the corporation would delete the user's data up to that time frame. This would serve firstly as an incentive for users to participate in this privacy process: namely, to authorize the deletion of their data. It would, however, also hold corporations accountable by the general public for failure to protect data privacy. The spaced-out, routine deletion of user data would decrease the immeasurable amount of data (and subsequently-filled storage) handled by corporations. It would additionally make data as temporal as possible so as to avoid unreasonable search of personal data long after its intended digital relevance. Admittedly, this would require further change in the field of data privacy, whether that be on a corporate or legislative level. Some corporations would foreseeably hesitate to implement a data-deletion protocol as it would require them to delve into a highly hands-off approach to user data past a given time frame; while it could create "clickback [...] that would enhance privacy," it would also drastically affect corporations' ability to utilize that location data far past a several-month time frame, whether for their own purposes or for sharing (Leckar). It could, however, be meaningfully integrable into this full solution if ultimately pursued.

Understanding the Solution

In conjunction with one another, the parts of the proposed plan create an optimal solution to a multi-factor issue. First and foremost, it is highly viable from an implementation standpoint. A simple notification and basic policy page are well within the capabilities of a tech giant like Google and require minimal investment of resources and efforts into their creation. Moreover, it

considerately acknowledges and addresses the barriers currently stunting transparency between corporations and consumers. Consumers will be presented the most critical and high-priority information with clarity, speed, and efficiency. Furthermore, consumers have the opportunity to fulfill a responsibility they have to themselves for the sake of their digital safety within minutes, at their convenience, and without hassle so as to avoid imposing any true disturbance on users' day-to-day digital lives.

Importantly, the corporation would not have to overcome any significant barriers to implement such a measure. The method presents an altered form of privacy disclosure, which already stands within the reaches of corporate handling; to this extent, neither legal nor constitutional challenges should overshadow the solution. The simplified, implemented policy itself may, however, arouse discontent around the current privacy situation created by the corporation. The direct awareness brought about by the newly-framed policy may reveal stark realities previously unrealized by consumers, which could lead to complaints or even legal action in response to the current regulation (or lack thereof) of corporate use of consumer data. While brought to light by the simplified policy, this is not directly a complication with the solution itself. The corporation merely restates what is already ingrained in the official, numerous-page policy that it holds for the legality of their system's operation; a negative reaction to the content of the simplified policy would merely elicit the need for a broader change in the corporation's privacy standards. In this regard, the proposed notification and policy system would further serve as an indicator of user satisfaction with their privacy situation.

The success of this method would need to be tracked over time to gauge its effectiveness amongst users. The notification itself and its ability to capture the attention of audiences can be measured through response-time data. As the notification would be sent out to all

simultaneously, the differences in response times could be easily calculable. The amount of completed policies that are sent after one day, two days, a week, et cetera would demonstrate the level of immediate engagement brought about by this solution. This would, of course, be the responsibility of the corporation to track and address accordingly; the simplicity of carrying out such a measurement, however, provides an easily-implementable performance indicator at the initial level.

The success of the policy itself, and its intended effect of increasing user awareness, corporate transparency, and topic comprehension would require more nuanced and in-depth analysis. The Pew Research Center's 2019 Survey, "Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information", provides a solid framework for yet another performance indicator. The survey asked pressing questions to technology users about their understanding of how their data is used, the effectiveness of current privacy policies, and their trust in corporations to handle their data safely; the results were concerning, revealing that a majority of users are currently worried and unsatisfied with the current data privacy situation and the lack of initiative to better inform consumers (Atske). It would therefore be valuable to carry out another survey post-implementation to measure the new percentages and proportions of people that feel lack of control over their data and, conversely, who feel more informed and confident in their data's usage. The 2019 survey provides a good comparison point for new key performance indicators, but it need not be relied upon solely for understanding these changes. Corporations could, if desired, precede the post-implementation survey with a pre-implementation survey better tailored to the points of change pursued by the corporation itself. Any significant changes before and after in the number of people who

understand what the company does with their information, the rights consumers hold with regards to their data, et cetera would indicate either success or ineffectiveness of the method.

This solution as a whole very intentionally avoids proposing a radical or unprecedented change to the current system in place. The recent failure of wide, sweeping changes proposed across the nation thus far stand testament to the fact that both consumers and corporations are unwilling to risk the comfortable familiarity of upholding the current privacy situation for a change that could drastically alter this reality. Rather, substantial but incremental changes are markedly needed — ones that start at the most fundamental level between users and platforms. The components of this entire proposition are not "radical" individually, but they do present a powerful force when tied together as so presented in this solution. The proposal strengthens communication, trust, and awareness; it avoids imposition, jadedness, and overbearingness. Its possibility for success is justified by its reliance upon existent features scattered throughout the digital world (notifications, text bars, open-forum boxes, etc) that have already proven auspicious, as evidenced by their individual prominence on the internet. The key is the formulated and organized combination of such features that maximizes impact given every constraint in question. The solution thus lies in gently introducing a familiar unfamiliarity to individuals on both the user and corporate side, confidently in the form of the outlined and carefully-designed proposal.

The flexibility of this solution is what truly underscores it as valuable in the face of the current digital world. Privacy concerns span far beyond geolocation data storage, usage, and sharing; there are numerous areas of data, including keyword, purchase, and browser data, that all pose risks to individual privacy. While this solution is curated to address location data privacy due to its increasingly severe risks and significant implications, the model is highly applicable in

addressing other issues. By merely adjusting the focus of the notification and policy, and attaching differing guarantees of corporate action, big tech can increase transparency with regards to how and why sensitive data is used across the board; the key performance indicators, societal impacts, and requirements for implementation would remain similar, and therefore render the solution more risk-averse to take on after initial implementation. The solution has been designed to be truly far-reaching in both relevance and influence; addressing the pressing geolocation data privacy situation -- and refocusing on the consumer as an individual with regards to their location information -- is promisingly only the beginning.

Works Cited

Atske, Sara. “Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information.” *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 17 Aug. 2020,

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

"Geofence Warrants and the Fourth Amendment." Harvard Law Review, vol. 134, no. 7, May 2021, pp. 2508–2529.

Harald Weinreich, Hartmut Obendorf, Eelco Herder, and Matthias Mayer: "Not Quite the Average: An Empirical Study of Web Use," *ACM Transactions on the Web*, vol. 2, no. 1 (February 2008), article #5.

Leckar, Stephen. Personal Communication. 7-10 April 2023.

Lynch, Jennifer. "First Court in California Suppresses Evidence from Overbroad Geofence Warrant." *Electronic Frontier Foundation*, 11 Oct. 2022, https://www.eff.org/deeplinks/2022/10/california-court-suppresses-evidence-overbroad-geofence-warrant.

Nielsen, Jakob. "How Little Do Users Read?" *Nielsen Norman Group: World Leaders in Research-Based User Experience*, 5 May 2008, https://www.nngroup.com/articles/how-little-do-users-read/.

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

Varner, Maddy, and Alfred Ng. “Thousands of Geofence Warrants Appear to Be Missing from a California DOJ Transparency Database,” *The Markup*, 3 Nov. 2021, https://themarkup.org/privacy/2021/11/03/thousands-of-geofence-warrants-appear-to-be-missing-from-a-california-doj-transparency-database.

Worth, Steven. Personal Communication. 28 March 2023.