Gallo, P., & Kettani, H. (2020). On privacy issues with Google Street View. *South Dakota Law Review, 65*(3), 1-5.

On Privacy Issues with Google Street View

Patrick Gallo and Houssain Kettani
The Beacom College of Computer and Cyber Sciences
Dakota State University, Madison, South Dakota, USA

Abstract—**Mapping data gathered by governments, corporations, and private individuals can be published freely across the web for use in diverse application sets. Upon its collection, other data, private data, may become subject to the public eye. Evolving from multiple acquisitions in its almost twenty-year history, Google's Street View application offers the public historical and 360-degree views of the globe from across the world. With users serving as the target of marketing techniques, which often create a game of chess between developers, the privacy practices of other companies often come to light. In this paper, we consider these issues and suggest some mitigation that public, private, and partnership entities may take in this shared effort.**

Keywords-Cyber Security, Data Privacy, Google, Street View.

I. Introduction

"There's an app for that!", the known past response for any one person looking to digitize just one piece of their life with their mobile device. Now, we look to the second version of this single statement: "There's a service for that!" By the notion of the second statement, corporations like Microsoft, Google, Apple, and others look to the need of the people and see a service or desire of the world population to accomplish a goal, wherein, a mobile app most certainly is developed in conjunction. Google is only one of these such organizations, finding many needs for the world in the area of technology and providing many services and apps for a diverse range of platforms. From ad service to personal and corporate video chat solutions, Google has introduced a wide portfolio to help businesses and individuals accomplish their mission set [27].

Google has been in the news for various privacy breakdowns since its inception in 1998, however, various new products have pushed the envelope and activists often push for steps further to combat data privacy weaknesses or security of those in judicial requests [11]. Google came under the control of a parent-company, Alphabet, during a restructuring of assets and personnel in 2015; which coincidentally made Google a bit more "slimmed down" [28]. The founders of Google, then Stanford University students, Sergey Brin, and Larry Page sought to make sense of the information out on the Internet, meaning to organize and make available such data based on closest possible terms [11]. For a massive data company, Google has become in its short lifespan already, nearly twenty locations around the globe house data centers, with hundreds of thousands of servers located at each, with custom hardware optimized for the multitude of products and services such a company offers [14].

Privacy for Google has become a concern, both in its business practices and its cooperation with government entities for legal inquiries. A present, past, and future act for many corporations, including Google involve the acquisition of smaller services, apps, and projects to improve or assist in the rollout of completely new solutions. One such historical acquisition for Google involves a 2004 buy of a small entity which specialized in a mapping language, Keyhole Mapping Language (KML) [13]. Keyhole first combined three-dimensional imagery used in video game graphics with mapping data to create three-dimensional figures which today form the basis of some of the iconic "flyovers" [21]. One of the last big-name customers before its eventual acquisition by Google was In-Q-Tel (IQT), a United States intelligence community not-for-profit research "strategic investor" [26]. Google's eventual acquisition of Keyhole was a strategic move, as, at the time, about a fourth of searches on Google were originating toward Keyhole data sources and tools [19].

Google Earth and Google Maps, the platforms we know and love for providing views of our houses, being the base for a lot of map inlays on websites and the means by which we make it to our destinations. A specific evolution of these services first arrived in mid-2007 with the release of Street View, a product revolutionary at the time to provide virtual walkthroughs of sites and street driving from the standpoint of a 360-degree world [39]. Street View first began with simple filming from vehicles in larger cities, however, data gathering has since evolved to mount cameras in backpacks, on bicycles, on tripods, or other means of transportation to provide "access" to places traditional vehicles may not be able to go [39]. The process for imagery collection involves complex analysis of weather patterns and dozens of images fused together and presented in optimal conditions prior to its publishing on the web. The fused images then produce a 360-degree view which the end result allows for panning with a touch screen in the mobile app or with the click of a mouse from a personal computer [34]. Street View touts itself as a place where "…imagery enhances your experience…is useful…and reflects the world…" That being said, in nearly fifteen years of development, Google has worked to quickly identify misuse of the platform, such as the posting of terrorist content, explicit images, and intellectual property violations, among many [39].

The rest of the paper is laid out as follows. In Section II, the technical backgrounds of Google Street View, Google infrastructure, and use cases for such data gathered are explained. Section III takes into account the potential privacy risks of Street View technology, the public's adoption of these possibly invasive technologies, and national security risks imposed as a result of public access to data. Section IV lays out potential liabilities of other products and practices done by Google, noting email advertising and web tracking in principal. Section V outlines practices of Google's competitors, behaviors of other platform data sources, and activity some entities have taken politically to back a "fundamental human right" of privacy. Finally, Section VI presents concluding remarks.

II. Technically a Feat

In the terms and conditions of becoming a partner toward Google Street View, a standard of quality for contributions exists, on the magnitude of seven and a half megapixels per image (or larger) and no filters [8]. In 2008, the company began testing a technology to blur the faces, license plates, or other identifying marks of a person or place, especially those which may have sensitive ramifications if revealed. Google faced similar concern by the public when the introduction of the now standard and expected views of our houses, offices, and other locations became available in Google Maps. Per a quote of John Hanke, then-Head of Maps and Earth products for Google, "…it took time…It needs debate…" [32]. Google faced concern in the area of images being live, which they are not, more populace areas, such as Washington, DC or New York City face more frequent updates to Street View products than forests of northern Russia, due to the interest of the imagery; Google Earth faces a similar imagery update timeline [39]. As more corporations begin competition in mapping platforms, two major players have emerged, Apple with Apple Maps, and Google with Google Maps. Both of these corporations have worked extensively to photograph the Earth from eye level, even both publishing updates to web pages to allow the public to be aware of the locations up for filming from vehicles which drive around the country filming and in the process also updating the accuracy of general mapping data [34]. This process is especially important as a new series of GPS satellites and receivers have been released and imagery first published.

While companies are generally quiet about their networks, Google has published documentation on peering, the act of interconnecting services and fiber physically in regions across the globe to better service their own infrastructure and other organizations via sharing fiber lines. The PeeringDB, a sort of online phonebook for Internet Service Providers (ISPs) lists Google as being connected to nearly seventy peering partners at a nearly equal number of locations globally. Google utilizes these partners at length to provide connection streams into its network ranging from capacities of ten gigabits to eight hundred gigabits [15]. The further network analysis, especially in documentation released by former National Security Agency contractor Edward Snowden revealed as a portion of programs Google and other technology giants were tapped into by way of internal fiber lines between facilities, which forced Google in 2013 to begin encrypting private network traffic [37].

In means of humanity, several products have come as a result of mapping data, mass gathering of data, and spiders, a technique used to crawl web pages and provide index information for search results. Google Earth Engine, a product released in 2010 provides countries with many natural disasters a way to analyze gathered data to plan for development, see and predict future land change, and prepare and respond to future or past events. These datasets are gathered using American Landsat and French SPOT program spacecraft. Google.org devoted ten million hours of compute time around 2011 for a two-year period processing data in its data centers [12].

III. Blurring the Lines for Security

While Earth, Maps, and Street View have provided unique perspectives of Earth from orbit or the street, particular concerns of governments and other entities have expressed displeasure of imagery published. Much in the way Europeans can "be forgotten" data once noted for public consumption on the Google platforms can be erased or blurred out for reasons of national security, privacy, or others. This has been seen as a way to suppress public information, much in the way a British politician sought unfavorable results removed from Google prior to him seeking re-election. Members of the public see the action of the "right to be forgotten" as possibly detrimental toward the access of information and to free speech in general. Knowing that a pedophile is exactly that and stories published of the act coming up in search results is indeed a risk to one person's legacy and reputation, while many feel that is simply the cost of doing business [34, 39].

In a national security perspective or simply a lack of imagery, blurred images may take the place of some real places on the globe. Antarctica is one of these locations where imagery is low-resolution or is not mapped in detail visually. Scientific analyses from satellites still take place of this global region, however, ice flow and thickness are more the concern, not penguins roaming the ice shelf in a feeding habitat. NASA maintains a mission, IceSat2, which devotes pole from its polar orbit approach to engage in continuing data analysis of melting flows of ice and thickness each season. Visually, users of Google Earth would see a lot of white pixels, the color of snow and ice, which is inefficient for the use of space-based assets to capture each orbit [18].

A couple out of Pennsylvania sued Google in the claim such imagery in Street View violated the "clearly marked" Private Road sign posted in their driveway. The lawsuit gained little traction in the courts, as imagery is gathered from the public domain, meaning sidewalks or streets without entering onto property marked private. There are clear practices for questioning the data posted by Google if there are disruptions or risks created in regard to the imagery made available [22]. Google once and for a very short time in the launch of the Street View platform did not remove faces or license plates with blurs, however, they have expanded the practice to automatic capabilities with analysis algorithms. At first glance, consumers could alert Google of their desire to be removed, if they were the individual in the image in question or owned the vehicle. Needless to say, policies were changed by Google shortly after to address the growing concern of privacy standards not in use at the time [23].

Sites of interest at a national level include sensitive government buildings, like the roof of the White House in Washington, DC, where when viewed from above, security assets meant to be hidden could in fact appear. Military activities of the United States both domestic and international have been off and on blurred and not for the last decade where aerial imagery is available. At a street level, Google first delayed Street View's release in certain regions of the United States, namely the Baltimore-DC region by request of the United States' Department of Homeland Security [10]. Some regulations exist from the United States' Department of Defense to the minimum of resolution which may be sold to other countries or private organizations. DigitalGlobe, a commercial imagery provider to various government customers, Google, and others petitioned the government to allow the sale of twenty-five-centimeter resolution per pixel imagery to non-government entities. Most data by default is not this sharp and often requires near perfect conditions to gather sharper imagery, which due to pass frequency by larger satellites, may only come less than once per the calendar year. DigitalGlobe's significant revenue stream originates from the US Department of Defense and at the time, such a request was considered as foreign competition is likely to offer comparable imagery resolution to customers, which lifting such a ban on higher resolution imagery could permit better competition [17].

IV. Google's Other Platforms

Imagery has been the main discussion item, however, Google's diverse portfolio of products in production or those in development currently may continue to test privacy bounds that the globe is comfortable with. Some of these have counted the practice of searching emails, tracking users on the web, and collecting data in applications on mobile devices even if a user has opted out of such behavior. In 2015, Google declared it would allow email addresses to be used to directly target ads toward consumers, a practice began by Facebook. In technical terms, this concept allowed a corporation to upload their contacts to Google to better target viewers of YouTube videos, sidebar ads when searching, and banner ads on pages, simply by comparing email lists a user may be enrolled in. While hashing is utilized to anonymize email addresses and prevent any sort of identification from either side, this entire concept is still one to watch from Google, which later canceled the project [35].

Targeted marketing, otherwise known as "Customer Match", by email was announced as coming to an end in 2017, meaning users would further only be subject to ads based on their search activity and other potentially non-personally-identifiable-information-leaking methods [36]. This action on Google's part concluded slightly over two years of controversial activity on the part of simply working toward furthering revenue and accuracy [5]. The scope of Google's reach in advertising market share was astronomical prior to mobile devices showing more prominence, however, in the shift, the market has required for Google to shift toward a more modern user scape so-to-speak, essentially where the audience went. Some of these ad-based revenue streams have become further difficult, Google not being alone [35]. In strategy, Apple does not make a large percentage of its quarterly revenue on anything but devices, only in 2019 have they really seen a larger shift to "services" or platforms that meet the criteria for a monthly billing cycle. Browsers like Firefox, Vivaldi, or others touting user privacy over ad-tracking have reduced capability further for Google, forcing a tension in effort to find a release of products that develop more revenue but also do not cross the societal line of expectation for privacy.

While Street View creates rather visible privacy concerns, a hidden dilemma came slowly in the form of waves, nearly six hundred gigabytes of wireless network data gathered from Street View vehicles [20]. German regulators, long before the implementation of the European Unions' General Data Privacy Regulation (GDPR) questioned Google about the practice. The technical controls of this practice were limited following public outcry, however, the general principle involved taking on data of broadcasted network Service Set Identifiers (SSIDs). Google vehicles also passing near public wireless access points also picked up some data from users' search activity. At that point back in 2010, Google began encrypting every search on its home page by default to further Internet security and verified use [25].

While nearly a decade ago, in 2011, Google, unlike competitors with browsers such as Firefox, Safari, and Internet Explorer, refused a sign on to the global "Do Not Track" project [6]. While the objective was to increase privacy online for consumers, Google's refusal to work Chrome into the mix of its computing applications. In 2012, Google reversed course and then added this feature to Chrome [6]. While it is recommended to never conduct certain business with a public computer, such as a library or with a personal computer in a coffee shop on public wireless access, Google Chrome and other browsers may inherently provide a risk for users, even on their own computer and private session. As a result of session data created, Chrome forensics data and browser data syncing records, such as passwords, credit cards, and email addresses may pose a risk to an unpatched or unencrypted system [9].

V. The Competition

When panning out competition toward Google, very few entities have the might to forgo financially the profit Google makes from their services and advertising each quarter. Apple for a good part of their history has been the device manufacturer, with higher prices attributing to solid revenue and profit recorded for most quarters in the last decade. Services aligning to media consumption have been the major game in 2019, with Apple announcing the Apple TV+ platform, Disney launching its own content platform, and of course the long-established current competition from the likes of Hulu, Netflix, and Amazon's Prime Video service. Apple in its own services category with iTunes, iCloud, App Store Sales, and other products has already risen to the level of a Fortune 500 corporation should it ever sever ties with the device manufacturing portion of Apple [4]. In the capability to raise revenue elsewhere, Apple pushes privacy as the pinnacle of its products [16].

In a race to compete largely with Google in the mapping products arena, Apple has since 2012, and with some beginning hiccups, has launched and added to Apple Maps. Directions notably involving the Los Angeles Airport runway and often misplaced towns, streets, and parks [3]. In the summer of 2018, Apple announced its commitment to rebuild its mapping program from the ground up, gathering the most accurate data and assumedly learning from all of the blunders they and nearly a decade earlier, Google had suffered from Street View involving blurs [29]. Apple Maps also worked to publish a list of locations within the United States where vehicles, beginning in 2015, began filming with sensors to gather updated and independent data, instead of using third parties' sources and licensing, a source of Google and Apple first splitting ways in 2011, leading to Apple Maps [29]. Following suit with Google's expansion to bikes and backpacks, Apple in larger cities began in late 2018 executing its own plan to improve walking directions and bike path routes around larger California cities [24].

While Apple Maps offer a glimpse of privacy practices honored and encouraged by Apple, a larger page published by the company goes further to expand on privacy simply being "…a fundamental human right…" [30]. Apple moves to make the claim their devices are built with privacy right in, keeping anything you want to share, yours to share. In recent light of GDPR, outrage of the public with other corporations, and other entities, Apple one of many entities involving users in the decision to share data and analytics with developers pushes to randomize data and then share it, claiming only distant patterns are recognized, such as a battery use percentage of Siri [30].

Google's struggle for privacy originates in key areas of their business model; analytics of products, tracking of customers, and education privacy. Apple, per a privacy practices page and security documentation published annually, spells out specific technical and short summaries of product behaviors. A majority of analytics are utilized by developers of products and software to improve results, if used for Siri or searches, or optimization of resources, if the battery is the component in question. In its browser as of 2018, Safari limits cookie tracking and Intelligent Tracking Prevention, which caught many ad-supported websites in Apple's crosshairs, meaning some had to seek revenue by other means. Apple in response to some of the outcry declared, "…Ad tracking technology has become so pervasive that it is possible for ad tracking companies to recreate the majority of a person's web browsing history…" [7].

Across the web, many companies, not just Google or Facebook, younger users represent a significant portion of the user base. Some users circumvent age policies with a declaration they are over or meet the age requirements outlined by Google or Facebook for obtaining an account. Many schools have switched to cloud-based productivity suites, with Google, Microsoft, and Apple with iCloud being large contenders. In using these platforms, Google may obtain large amounts of student data entered by staff and teachers, or search habits of students, developing a "digital file" on very young, unsuspecting minors. In many cases, our classrooms have evolved outside the four walls and doors of the traditional story-book stereotype "red schoolhouse of America". The "Children's Online Privacy Protection Act" and the "Children's Internet Protection Act" cover privacy and content filtering regulations for public institutions, such as libraries or schools to require controls in place to limit access to obscene material. The hand of many organizations is forced as they receive federal funding to offer services, an example being small, rural library systems. Cisco with its Meraki product line has become an industry leader in networking and device management for many institutions, including healthcare or primary and higher learning environments [1].

In competition now with Google's prior activity of searching emails for advertising purposes and also to allow for ultimate circumvention of illegal wiretaps by government entities, a small not-for-profit company, ProtonMail, grew out of the European Organization for Nuclear Research (French: CERN) research facility in 2014 with engineers committing off time to explore new security solutions. ProtonMail's mission is to "…build an Internet that respects privacy and is secure against cyberattacks…" [2]. With all data end-to-end encrypted, ProtonMail can lead success of Internet security further with its location in Switzerland, a privacy-conscious country which requires high courts, similar to the United States' District Circuit Courts, District Appellate Courts, or the Supreme Court, to grant a warrant for information to be released in limited form to requesting entities [31]. In a recent posting, ProtonMail publicly came out in support of the California "Privacy for All Act of 2019", a blanket privacy regulation putting much more control of data in the hands of consumers. This act is extremely powerful as many tech giants call Silicon Valley home for their headquarters, foreign entities may do business in California, or other domestic corporations maintain business presences [40].

VI. Concluding Remarks

Whether end-to-end encryption, blurring license plates of cars on the road, data privacy as a whole has seen hoops and bounds. Corporations, individual states, and entire countries have come together to support the defined "human right" that is privacy. In various forms, whether it to ward off government surveillance, mass collection of data for advertising, or to maintain better security for consumers whose data gathered is exposed in data breaches, the push is clear at all levels. In Congress, state legislatures, and corporate board rooms, the people stand ready to take action into their own hands if inappropriate steps are taken. These may be by way of legal action, protests, or movement of data out of particular jurisdictions; however, each move presents a step to work toward counteracting, an ever-present step in cybersecurity and privacy as a whole, reactive. Privacy practices of Google in mapping data, classroom activities of students, and email data for advertising have seen possibly adverse side effects to which we have adopted as the new norm for our society and worked to conquer the next hurdle we are thrown. From the street, or from space, the view is masked or not, and many things may be a blur of confusion in the lines of legislation and policy of tech giants.

References

[1] Brejcha, J. (2016, February 23). 10 things you need to know about Cisco Meraki. *Cisco UK & Ireland Blog.* Retrieved from https://gblogs.cisco.com/uki/

[2] Tschabitscher, H. (2019, March 25). ProtonMail Review: Free secure email service. *Lifewire.* Retrieved from https://www.lifwire.com/

[3] Arthur, C. (2012, September 28). Apple Maps: Tim Cook says he is 'extremely sorry'. *The Guardian.* Retrieved from http://www.theguardian.com/

[4] Gadgets Now Bureau. (2018, May 3). Why Apple's services business is as big as a Fortune 500 company. *The Gadgets Now.* Retrieved from https://www.gadgetsnow.com/

[5] Cakebread, C. (2017, June 23). Google is going to stop reading the mail in your Gmail inbox to target ads to you. *Business Insider.* Retrieved from: https://www.businessinsider.com/

[6] Claburn, T. (2012, September 15). Google Chrome to get 'do not track'. *Informationweek*. Retrieved from https://informationweek.com

[7] Clover, J. (2018, January 9). Ad firms hit hard by Apple's intelligent tracking prevention feature in Safari. *MacRumors.* Retrieved from https://www.macrumors.com/

[8] Armstrong, C. (2017, May 9). Create your own Street View Imagery with new 360 cameras. *Google Maps Blog.* Retrieved from https://blog.google/products/maps/

[9] Magnet Forensics. (2017, March 10). Digital Forensics: Artifact Profile – Google Chrome. *Magnet Forensics Blog.* Retrieved from https://www.magnetforensics.com/

[10] Elsworth, P. C. T. (2008, March 1). Pull up a chair for a walking tour. *The Providence Journal*. Retrieved from https://www.projo.com/

[11] Frick, W. (2014, August 20). How Google has changed management, 10 years after its IPO. *Harvard Business Review Digital Articles*. Retrieved from https://hbr.org/

[12] Gardner, T. (2010, December 2). Google unveils satellite platform to aid forest efforts. *Reuters.* Retrieved from https://www.reuters.com/

[13] Google. (2004, October 27). Google acquires Keyhole Corp. *News from Google.* Retrieved from http://googlepress.blogspot.com/

[14] Kinsta. (2019, April 19). Where are your Google Cloud Data Center locations?. *Kinsta.* Retrieved from https://kinsta.com/

[15] PeeringDB. (2019, February 13). Google *LLC. Peering DB.* https://www.peeringdb.com/asn/15169

[16] Grothaus, M. (2016, February 17). Tim Cook opposes court order that Apple must help FBI unlock iPhone. *The Fast Company.* Retrieved from https://www.fastcompany.com/

[17] Gruss, M. (2014, April 15). U.S. intel community endorses easing resolution limits on commercial imagery. *SpaceNews.* Retrieved from https://spacenews.com/

[18] Heiney, A. (2018, September 15). ICESat-2 Successfully Launched on Final Flight of Delta II Rocket. *National Aeronautics and Space Administration (NASA) Blogs.* Retrieved from https:///blogs.nasa.gov/

[19] Kilday, B. (2018). *Never lost again: The Google Mapping revolution that sparked new industries and augmented our reality*. New York, NY: HarperCollins Publishers.

[20] Lopresti, M. (2011, March 28). Google "Wi-Spy" controversy rages on, raises more questions. *EContent*. Retrieved from https://www.econtentmag.com/

[21] Mark, E. (2004). Inter-related Scaled Models of the Built and Natural Environment: Merging CAD with Satellite Image Viewing. *Proceedings of the 22nd Education and Research in Computer Aided Archetectural Design in Europe (eCAADe) Conference,* Copenhagen, Denmark, 480-488. Copenhagen: Architecture in the Network Society.

[22] Mills, E. (2008, April 4). Couple sue Google for invading privacy with Street View. *CNET.* Retrieved from https://www.cnet.com/

[23] Mills, E. (2008, June 1). Google now zaps faces, license plates on Map Street View. *CNET.* Retrieved from https://www.cnet.com/

[24] Mogg, T. (2018, November 19). Apple confirms its collecting data on foot to improve its Maps app. *Digital Trends.* Retrieved from https://www.digitaltrends.com/mobile/

[25] Nicks, D. (2014, March 13). Google will start encrypting your searches. *Time.* Retrieved from http://time.com/

[26] Yannuzzi, R.E. (2007, May 4). In-Q-Tel: A new partnership between the CIA and the private sector. Retrieved from https://www.cia.gov/

[27] Biswal, R. (2019, February 6). Top 20 most popular Google products and services. eCloudBuzz. Retrieved from https://www.ecloudbuzz.com/

[28] Rosoff, M. (2015, August 10). What is Alphabet, Google's new company?. *Business Insider.* Retrieved from https://www.businessinsider.com/

[29] Panzarino, M. (2018, June 29). Apple is rebuilding Maps from the ground up. *Tech Crunch.* Retrieved from http://social.techcrunch.com/

[30] Apple. (2019, March 25). Apple ID & Privacy. *Apple.* Retrieved from https://support.apple.com/

[31] Proton Technologies AG. (2016, July 8). ProtonMail Security Features and Infrastructure. *Proton Technologies AG.* https://protonmail.com/docs/business-whitepaper.pdf

[32] Shankland, S. (2008, May 13). Google begins blurring faces in Street View. *CNET.* Retrieved from https://www.cnet.com/

[33] Toobin, J. (2014, September 22). The solace of oblivion. *The New Yorker.* Retrieved from https://www.newyorker.com/

[34] Grtenberg, C. (2017, December 11). Google just launched three new photography apps. The Verge*.* Retrieved from https://www.theverge.com/

[35] Statt, N. (2015, September 28). Google will let companies target ads using your email address. Retrieved from The Verge. Retrieved from https://www.theverge.com/

[36] Statt, N. (2018, July 18). Apple's iCloud partner in China will store user data on servers of state-run telecom. *The Verge.* Retrieved from https://www.theverge.com/

[37] Timberg, C. (2013, September 6). Google encrypts data amid backlash against NSA spying. *The Washington Post.* Retrieved from https://www.washingtonpost.com/

[38] Wakefield, J. (2014, May 15). Politician and paedophile ask Google to 'be forgotten'. *BBC.* Retrieved from https://www.bbc.com/

[39] O'Kane, S. (2017, October 2). You can now capture Google Street View scenery with your car for $3,500. *The Verge.* Retrieved from https://www.theverge.com/

[40] Wollard, B. (2019, April 17). We support stronger privacy regulations in California. *Proton Technologies AG.* Retrieved from https://protonmail.com/