Could Your Mobile Broadband Internet Provider Threaten Your Digital Privacy?

Even Becker*, Hubert Djuitcheu†
Division of Wireless Communications and Radio Positioning (WICON)
Technische Universität Kaiserslautern
Kaiserslautern, Germany
{*ebecker, †djuitcheu}@eit.uni-kl.de

***Abstract*—Users privacy is more and more relevant in today digital world. In this paper, we study how mobile network operators (MNOs) practices can lead to loss of privacy for mobile phone subscribers. This article focuses on the mobile phone service providers' implication in privacy violation. Network attacks from other agents, such as cyber-criminals, are not covered in this work. We review the impact of the location tracking improvement from 2G to 5G networks on police investigations and users' privacy rights. We also study the role of MNOs in users' sensitive data monetization and the legality behind this practice. There are few existing publications aiming to enhance mobile phone users' privacy protection against mobile broadband internet providers. We have tried to list all of them in this article.**

***Index Terms*—Privacy, location tracking, web tracking, surveillance, 5G networks**

I. Introduction

In 2013, Snowden revealed the National Security Agency (NSA) surveillance program. American secret legal authorities are spying people phone communications and online activities. The main goal of this surveillance is to fight terrorism but other political issues could be a motivation. These revelations were given wide coverage in the media. However privacy violation coming from other entities than the NSA are not widely publicized. Statistical studies [1], [2] show that most consumers are unaware and unconcerned how their private data are used without consent.

Mobile carriers are regularly leaking data of their users to third parties. Many mobile network operators (MNOs) ask private information, such as age, gender and nationality. The data are gathered in an anonymous way for statistics purpose and are legally shared with third-party partners. When customers sign a contract with their mobile phone service providers, they automatically agree with their privacy policies. However, MNOs documentation does not clearly inform the customers about how their personal data are stored and for what purpose it will be used afterwards. According to authors in [3], operators storing users' data in the cloud lose all control over this data when it is hosted abroad, for example, which would favour any manipulation by a third party. Furthermore, MNOs can store users' location data. Location tracking reveals a large amount of private information about a person and raises privacy concerns. In the U.S., mobile carriers can legally sell their customers' location data to companies as long as they report their activities in their privacy policies. Meanwhile, some American mobile phone service providers have misused users' sensitive data, such as location data, identity, phone call and messaging metadata without consent. They had a deal with some tech companies to sell data to clients, mainly marketers [4]. In February 2019, the Federal Trade Commission (FTC) has brought suit against several MNOs for violating their privacy policies [5]. However the media coverage of this case was negligible compared to Snowden revelations about the NSA.

Seeing these puzzling facts, one can wonder why MNOs are gathering their subscribers' sensitive data and which techniques they employ. This paper reviews the process of users' location data collection and analyzes if MNOs are compliant with data protection regulation when they share users' personal data with third parties, namely the authorities. Then techniques used by MNOs to track their customers' online activity are presented.

By highlighting MNOs guiltiness in privacy issues, from a technical point of view, this article aims to raise the interest in developing new solutions on both the network and the mobile phone side to tackle this problem.

II. Background and Motivation

The internet advertising market is worth hundreds of billions of dollars and is one of the fastest growing online businesses [6], [7]. The digital advertising spending worldwide amounted to 521 billion U.S. dollars in 2021 [8]. In comparison, the global organic food market was valued at approximately 227 billion U.S. dollars the same year [9], which is significantly inferior. More and more companies are selling digital advertising for websites. Access to users' personal data is important to be competitive on the digital advertising market. Indeed, the collected information builds user profiles, which companies can buy to target ads. These data are precious to fine-tune ads personalization. There are evidences that Big Tech companies like Google are breaching their users privacy for commercial gain [10]. Google owns widely used services like Google search, the most used search engine. This firm is therefore able to collect a huge amount of users' data and dominates the digital advertising market. In the early 2000s, this market was mainly focused on computer users who view ads on web browsers. However, since the adoption of the Internet Protocol Multimedia Subsystem (IMS) in UMTS networks, mobile

phone users have started to play a more important role in the digital advertising market. Indeed, the IMS allows MNOs to deliver internet protocol multimedia to mobile users. As a result, more and more people are using their mobile phone instead of their computer to use various online services. In addition, mobile apps have an important role in the digital advertising market because they can contain ads. When a mobile app has permission to view the user' location, apps owners, like Starbucks, collect and supply these location data for the location data market [11]. This allows advertisers to track users' location and usage of apps. In a near future, the mobile market is expected to represent 70% of the global internet advertising market [12]. In addition, the amount of personal data shared on mobile networks has grown significantly. Since the availability of low cost smartphones for the mass in 2010, people can browse the internet, use various messaging services and upload photos or videos without computers. Consequently more users' sensitive data are circulating under the eyes of MNOs and privacy has become a major problem. Furthermore Nurse et al. [13] show in their article that the users' privacy is even more threatened with the compulsory adaptation imposed by Covid 19, where users are forced to enter confidential information about their health and their personality.

Another aspect of privacy violation is government surveillance. In authoritarian or semi-authoritarian countries, people can be victim of harassment and vengeance if they express dissenting opinions. Journalists of Zimbabwe have proved [14] that Internet Service Providers (ISPs) and MNOs are sharing, often illegally, individual data with the government to hamper political opposition or human rights defence.

This article investigates the process of tracking mobile phone users and the legality behind MNOs data collection and sharing with third parties such as government authorities. Current solutions to the studied privacy issues are also presented.

III. Literature Review

The computer networking community is aware of the techniques used by advertising companies to breach their customers privacy. M. Koop thesis [12] contains a survey of web tracking techniques and dedicated protection mechanisms. Notable solutions are Virtual Private Networks (VPNs) and the Tor Project. Techniques especially used by large ISPs, namely Domain Name System (DNS) logging, are not discussed in this work. Schmid et al. [15] have addressed DNS security and privacy issues. DNS abuses by both cyber-criminals and ISPs are mentioned. However, the mobile phone service providers' participation to privacy violation is not being taken seriously by the telecom community. Telecom researchers address security and privacy issues regarding networks attacks coming from external entities, namely cyber-criminals and fake base stations. Privacy issues in location-based service (LBS) applications have also been addressed and possible tracking from LBS providers has been mentioned in [16]. More recently, a few publications involving massive tracking from *honest-but-curious* entities [17], [18] have appeared but this term refers to third parties like multimedia service providers, rather than network operators. Many anonymization techniques to prevent localization have been proposed [19] but these solutions are inappropriate for hiding the geolocation information from MNOs. Only a few telecom publications [16], [20]–[22] mention that MNOs play an active role in private data leakage. Most of the existing telecom literature limits MNOs culpability in data leakage to insecure data handling. Indeed, ISPs and MNOs sometimes handle their customers sensitive data insecurely. Private data can be stored with no encryption or encrypted with a weak algorithm. For example, Motorola has stored users' login information for online services like Facebook on its own servers [12]. Then external attackers can seek these data. A possible solution could be to prevent MNOs collecting users' sensitive data but location data are problematic. Indeed, MNOs need to know where users are located in order to provide connectivity. Consequently, it is not possible to prevent location data collection and new solutions to anonymize the data need to be found.

P. Schmitt et al. [21] have proposed a new network architecture called Pretty Good Phone Privacy (PGPP) to protect users' identity and location data against MNOs. Their software-based solution can be deployed on existing networks and do not need any hardware modification. In their solution, all subscribers have SIM cards with the same Subscription Permanent Identifier (SUPI). Contrary to current 5G networks where users are authenticated using SUPIs at the Authentication Server Function (AUSF), PGPP has a special authentication scheme. This way, the SUPI value is nullified. The PGPP network can provide connectivity to the users with an IP address and the globally unique temporary identifier (GUTI) ensures unique identity. Another attempt to stop MNOs intrusive data collection is proposed in [22]. A virtual private mobility network (VPMN) is combined with anonymization techniques to prevent the leakage of location data. As in PGPP, an independent authentication and billing authority is used. These solutions are designed for standalone 5G and are not compatible with LTE and non-standalone 5G, which have an older core network architecture.

IV. Location Tracking

A. Triangulation Accuracy Improvement from 2G to 5G Networks

The Cell Site Location Information (CSLI) is stored by mobile phone service providers. The gathered data allow to detect a cell phone's location. MNOs use the CSLI for troubleshooting, adjusting network performance and to determine when roaming charges apply. The CSLI can also provide the historical movements of a cellphone. Expert RF engineers need some times to process the data, so the location tracking is not real time. The triangulation is not precise in GSM networks because only one cell is connected to the device. The accuracy of location information from a single tower varies from "a few blocks to several square miles" [23]. Additional metrics, such as neighbor cell levels can be used to improve the precision. A GSM parameter called timing advance (TA) can give information about the distance between the phone and the

connected cell. More TA values for triangulation can be found if the signal hands over to another cell. Besides, triangulation is easier in 3G and 4G networks because of Multiple Serving Cells in a connection session or call. Active Sets are used in 3G systems while 4G systems rely on Physical Cell IDs.

In 2007, the first mobile phones with built-in Global Positioning System (GPS) receiver appeared on the market. On authorities requests, cell phone companies can store prospective GPS data in addition to CSLI to improve tracking accuracy. The police can also place a GPS tracking device on a suspect vehicle but this is considered out of scope for the purpose of this article. The Radio resource location services (LCS) protocol (RRLP) is available in GSM and UMTS. It can combine CSLI and GPS data to provide geolocation information for emergency calls. This protocol can activate the GPS without any authentication. MNOs can therefore seamlessly provide these location data for law enforcement requests. In 2014, a better emergency location-based service called Advanced Mobile Location (AML) was designed for smartphones. It can combine CSLI, GPS and Wi-Fi data. When the user calls an emergency number, this location data is automatically sent. Many MNOs have enabled this service all around the world, allowing callers' location tracking. Since 2022, AML is a mandatory feature for smartphones sold in the E.U.

In addition to track their subscribers' location, MNOs can identify them via the international mobile subscriber identifier (IMSI), which is unique and permanent. In 5G networks, the IMSI has been replaced by the SUPI. Standalone 5G systems are said to have better security and privacy because many problems of Long Term Evolution (LTE) networks, like IMSI catchers, are solved. However 5G networks allow even more accurate location information than previous generations. Indeed, cells are smaller and artificial intelligence tools are integrated in 5G networks to infer location. Furthermore, when millimeter-wave transmissions are used, localization accuracy in the order of 10 meter or less can be achieved outdoors [22]. Consequently, location tracking is even more problematic in 5G networks. MNOs should anonymize the users' location information before using them for data analysis tasks like machine learning (ML). When using privacy preserving machine learning techniques, there is a trade-off between the level of anonymization and the ML model's predictive accuracy. Furthermore, the use of stronger privacy models can result in loss of the ML model's output usability [24]. Low privacy levels will probably be used to avoid this problem. The users' privacy is therefore not completely preserved.

B. The Regulation of Targeted Surveillance

In most countries, during a police investigation, search warrants are needed to seek information from third parties, such as email service providers, ISPs and phone companies. After getting a search warrant, the police can rely on CSLI to track someone location. This location information is used especially in homicide, robbery and drug cases [25].

However, in the U.S., the "third party doctrine" (TPD) allows law enforcement to seek information from third parties without the use of a search warrant for criminal cases. The TPD emphasizes that information voluntarily turned over to third parties are not private and thus are accessible by the police. Consequently, law enforcement requests to cell phone providers to provide CSLI for specific phones don't require a search warrant under the TPD [25]. However in 2018, the Supreme Court decided for the first time a case that requires a search warrant. This case is known as Carpenter v. United States [25]. Carpenter was represented by the American Civil Liberties Union (ACLU). Usage of CSLI to perform targeted surveillance was recognized as a privacy violation and the TPD was reconsidered. The ACLU succeeded in improving mobile phone users' privacy rights.

American MNOs can legally sell their customers' location data to companies. Therefore, U.S. authorities sometimes ask phone users' data to third parties rather than MNOs. This way, U.S. authorities can track an individual location without a search warrant. For instance, the police has snooped on phone location data without a warrant by using data from Securus, a prison technology company who is buying location data to MNOs [26]. Another example of Post-Carpenter surveillance tool for criminal investigations is Fog Reveal, sold by Virginia-based Fog Data Science LLC. This software product combines location data bought on the location data market. The police can use it without search warrant.

Data protections regarding sharing with third parties are stricter in the E.U. thanks to the General Data Protection Regulation (GDPR). Consequently, European telecommunication companies cannot share sensitive customers information to marketers and agencies. However the E.U. is not safer than the U.S. regarding data sharing to governments. Even if European MNOs have to anonymize the data to comply with the GDPR, researchers at MIT showed in 2018 that people can be easily identified from their location history [5]. In addition, many European countries laws, such as the Germany's Telecommunications Act, allow the authorities to ask communication service providers information about their subscribers without a search warrant. For instance, the police can monitor someone online activity by seeking dynamic IP addresses assigned by the ISP during a period of time. Worst in France, a military programming law introduced in 2013 allows French authorities to monitor all the internet traffic in real time without a search warrant [27]. Even if many communication services, such as Skype and WhatsApp, have an end-to-end encryption option, the French police might be able to list all the people contacted by a specific person. The adoption of this law has lead to a flood of protests in France.

C. Enhanced Surveillance by Using the Phone Operating System

CSLI provides a general estimate of a phone's location with a precision of 50 meters [28]. In Graham's case [29], the culprit mobile phone service provider warned that CSLI is not enough precise to be used for the judgment. The police has relied on the location data available in Android, also known as Google's Location History. These data can be accessed via

warrant requests from law enforcement. The Android system gives more precise location information by combining CSLI with other sources such as GPS and Wi-Fi networks. The mobile phone user can be tracked with a precision of 10 meters. The police can also ask Google to identify all Android phones in a place where a crime occurred on a specific time frame like for example 6 hours. The ACLU complained about privacy violation because innocent people location data are gathered and analysed.

The GDPR states that mobile data, namely location data, must be anonymized before it is shared with any organization, such as the government [5]. However in 2020, at the beginning of the Covid pandemic, millions of people were ordered to stay at home and the authorities used location information from mobile service providers to increase surveillance. These information were probably not anonymized. Many countries authorities have released apps for Android and iOS to detect and track infected people. Indeed, mobile applications can access users' sensitive data, such as location history and contact list, when the app permissions are set accordingly. Both Google and Apple received requests from different governments to allow Covid related apps to bypass data protection built in the Operating Systems. France's digital minister was disappointed with Apple refusing the French government request [5]. Indeed, iPhones' location data are collected anonymously. The user identity is protected unless the user provides explicit consent to allow Apple to de-anonymized the data. This case shows that Big Tech companies are not always the main culprit in privacy violation.

V. MNOs Implication in Personal Data Leakage

A. Tracking Methods for Advertising Programs

MNOs and ISPs use super-cookies to track online activity of users [30]. This practice is motivated by network performance enhancement but Vallina-Rodriguez et al. [20] think that digital advertising is also the reason. Super-cookies are used on websites to enhance targeted advertisements. Simple cookies are only stored in the browser, while super-cookies work at a deeper level, i.e. the network layer, and are permanently saved on the user device when a website is visited. They allow websites visitors tracking by identifying a visitor connection, whereas simple cookies identify users at the application layer. ISP Super-cookies infiltrate better users privacy because advertisers can know which websites the user frequently visits and the time spend on them. They are created by injecting unique tracking identifiers into HTTP requests. However, the header cannot be injected into an HTTPS request. MNOs and ISPs can bypass this protection: they deploy HTTP proxies and force their usage to downgrade users' secure HTTPS requests to HTTP ones. It was not possible to delete these cookies until Firefox 85, which was released on January 2021 [31]. Using a VPN can also be a solution to avoid ISP super-cookies. However, some VPN providers may keep logs or reveal subscribers IP to adversaries, which is another privacy issue.

Another technique used by large ISPs is DNS Redirect. Cyber-criminals use this DNS attack, as well as DNS Cache Poisoning to make the user visit malicious servers. The internet protocol is used in the 5G core network. 5G systems can therefore also be affected by this attack. DNS Redirect is not always of criminal origin. Indeed, ISPs can redirect their customers to ad servers that contain advertisement rather than malware scripts. Some countries also use this technique to impose internet censorship. DNS Redirect can be avoided with a VPN that provides its own secure DNS servers.

Large ISPs are creating fingerprinting techniques to efficiently analyze their customers DNS queries [32]. One widely used technique is DNS redirection via NXDOMAIN. When customers visit a misspelled webpage like 'googl.com', the DNS lookups fail and they are redirected to Web servers containing advertisement. N. Weaver et al. call this practice *"DNS error traffic monetization"* [33]. The legal issue of this practice is not fully addressed by privacy regulations. There are a few specific companies that joined the DNS redirecting market. On September 2019, major communication service providers sent a letter to the congress to complain about the availability of DNS over HTTPS (DoH) in Google products [34]. This technique of DNS encryption can prevent ISPs from logging users' DNS queries. However, when a user connect to a server with DoH, the ISP can still know the server IP address, but the visited web page and its content are invisible. One year before, another form of DNS encryption called DNS over TLS (DoT) was already available in Android 9 (pie) [35]. This out-of-the-box feature is built in the Operating System and can be easily enabled without any scripting or third-party tools, making DNS encryption available for the mass in 2018.

ISPs claimed critical Internet dysfunctions could happen if the users do not rely on their ISP's DNS. However a conflict of interest regarding consumers' data collection could be the complain reason. Indeed, both ISPs and DoH providers may want to log their users' DNS queries for advertising targeting. Quad9 DNS seems to be a privacy respecting DNS service but this option was removed from Google Chrome DoH settings. Indeed, Google wants people to use DoH with Google Public DNS or Cloudflare DNS. This way, Google and Cloudflare will collect most of the DNS traffic when DoH is enabled. Having a stronghold on the market of DoH will allow these companies to better control the digital advertising market [32]. They are helped by Mozilla, which enables DoH by default when Firefox is installed in the U.S.

B. Insecure Integration of Third-Party Services in the Core Network

Mobile carriers can provide third-party application content. Mobile applications offering multimedia services can be quickly developed and deployed using the IP Multimedia Subsystem (IMS). The IMS allows third party developers to easily deploy their applications over mobile networks. Since 2G networks deployment, the IMS is located in the core network. IMS common signalling is based on Session Initiation Protocol (SIP). Third party applications such as IMS

based LBS applications, are running in the IMS core. These software products are deployed using SIP application servers.

MNOs trust the third-party applications integrated in their systems and let them interact with potentially sensitive information found in the SIP signalling, the application data and the charging and billing systems. It is possible that third party software products abuse this trust to perform intrusive data collection and sell these data to marketers. Third party applications should not be able to access users' sensitive data. A need of *"independent network security zones"* for the IMS architecture was already expressed when UMTS was standardized [16], [36].

In order to use IMS based multimedia services, LTE and 5G users have to authenticate two times: one authentication at the network layer and one at the IMS service layer. IMS authentication algorithms are more vulnerable. Thus, IMS services cause vulnerabilities in LTE and 5G networks [37]. Besides, IMS is used in LTE and non-standalone 5G systems for Voice over LTE, Video over LTE and SMS/MMS over LTE. Consequently, third parties might use IMS vulnerabilities to read SMS and listen to phone conversations. This problem is still relevant in standalone 5G networks where third party services are even more integrated in the core network. IMS is still used for Voice over 5G and other services. For their network architecture, P. Schmitt et al. [21] recommend to use outside messaging services rather than the usual IMS system located in the core network.

VI. Conclusion and Outlook

MNOs can leak users' sensitive information to third parties. This leakage can be of unintentional origin, like insecure data handling and blind trust in third-party apps running in the IMS core. Nevertheless, MNOs can track and monetize their subscribers' online activity. Smartphone and computer users can obfuscate their online activity from ISPs with tools like DNS encryption and VPNs. However, the user has to trust the DNS service provider or VPN provider.

MNOs can provide mobile phone users' location information to the police. In some judgments, like Graham's case, these data are not considered reliable. However, the triangulation is more and more accurate with new generations of mobile networks and could be precise enough to influence police investigations and court decisions. In addition, some MNOs are collecting users' location information for data analysis tasks or to supply them to the location data market. Thus, new anonymization techniques need to be found to prevent MNOs from tracking users' location.

References

[1] M. Farooq and Q. A. Qureshi, "Privacy of internet users in the era of transformative marketing," *Journal of Management Practices, Humanities and Social Sciences*, vol. 4, no. 2, pp. 25–28, 2020.

[2] M. Rzeszewski and P. Luczys, "Care, indifference and anxiety—attitudes toward location data in everyday life," *ISPRS International Journal of Geo-Information*, vol. 7, no. 10, p. 383, 2018.

[3] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[4] S. J. Andrews, *Hegemony, Mass Media and Cultural Studies: Properties of Meaning, Power, and Value in Cultural Production*, p. 195. Rowman & Littlefield, 2016.

[5] C. Pandit, H. Kothari, and C. Neuman, "Privacy in time of a pandemic," in *Proceedings of the 2020 13th CMI Conference on Cybersecurity and Privacy (CMI)-Digital Transformation-Potentials and Challenges (51275)*, pp. 1–6, IEEE, 2020.

[6] H. Aksu, L. Babun, M. Conti, G. Tolomei, and A. S. Uluagac, "Advertising in the IoT era: Vision and challenges," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 138–144, 2018.

[7] H. Djuitcheu, M. Debes, M. Aumüller, and J. Seitz, "Recent review of Distributed Denial of Service Attacks in the Internet of Things," in *Proceedings of the 2022 5th Conference on Cloud and Internet of Things (CIoT)*, pp. 32–39, IEEE, 2022.

[8] Statista Research Department. https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/, Jun 2, 2022.

[9] M. Shahbandeh, research expert covering agriculture & FMCG. https://www.statista.com/statistics/869052/global-organic-food-and-beverage-market-value/, Jun 20, 2022.

[10] K. A. Houser and W. G. Voss, "GDPR: The end of Google and Facebook or a new paradigm in data privacy," *Rich. JL & Tech.*, vol. 25, p. 1, 2018.

[11] M. Yuen, "How big data warehouses and AI in data analysis are transforming business intelligence in 2022." https://www.insiderintelligence.com/insights/ai-data-analysis/, 2022.

[12] M. Koop, *Preventing the Leakage of Privacy Sensitive User Data on the Web*. PhD thesis, Universität Passau, 2021.

[13] J. R. Nurse, N. Williams, E. Collins, N. Panteli, J. Blythe, and B. Koppelman, "Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy," in *Proceedings of the International Conference on Human-Computer Interaction*, pp. 583–590, Springer, 2021.

[14] A. Munoriyarwa, "When watchdogs fight back: resisting state surveillance in everyday investigative reporting practices among Zimbabwean journalists," *Journal of Eastern African Studies*, vol. 15, no. 3, pp. 421–441, 2021.

[15] G. Schmid, "Thirty years of DNS insecurity: Current issues and perspectives," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2429–2459, 2021.

[16] L. Zheng, "An IMS concept and security design for mobile content service," 2007. Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=24e599c5b2920de80c4657acef803437fcffe0fe.

[17] N. Chalkiadakis, D. Deyannis, D. Karnikis, G. Vasiliadis, and S. Ioannidis, "The million dollar handshake: secure and attested communications in the cloud," in *Proceedings of the 2020 IEEE 13th International Conference on Cloud Computing (CLOUD)*, pp. 63–70, IEEE, 2020.

[18] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Computing*, vol. 22, no. 2, pp. 42–51, 2018.

[19] Y. Qiu, Y. Liu, X. Li, and J. Chen, "A novel location privacy-preserving approach based on blockchain," *Sensors*, vol. 20, no. 12, p. 3519, 2020.

[20] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, and V. Paxson, "Header enrichment or ISP enrichment? Emerging privacy threats in mobile networks," in *Proceedings of the 2015 ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization*, pp. 25–30, 2015.

[21] P. Schmitt and B. Raghavan, "Pretty Good Phone Privacy," in *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*, pp. 1737–1754, 2021.

[22] S. Tomasin, M. Centenaro, G. Seco-Granados, S. Roth, and A. Sezgin, "Location-privacy leakage and integrated solutions for 5G cellular networks and beyond," *Sensors*, vol. 21, no. 15, p. 5176, 2021.

[23] L. M. McMahon, "Limited Privacy in'Pings:'Why Law Enforcement's Use of Cell-Site Simulators Does Not Categorically Violate the Fourth Amendment," *Wash. & Lee L. Rev.*, vol. 77, p. 981, 2020.

[24] N. Senavirathne and V. Torra, "On the role of data anonymization in machine learning privacy," in *Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 664–675, 2020.

[25] A. Harm, "Privacy Concerns In The Digital Era: An Analysis Of The Third-Party Doctrine's Usage In The Criminal Court System," 2021. Available online:

https://ir.library.illinoisstate.edu/cgi/viewcontent.cgi?article=1003&context=urs2021cjs.

[26] Z. Whittaker, "US cell carriers are selling access to your real-time phone location data." https://www.zdnet.com/article/us-cell-carriers-selling-access-to-real-time-location-data/, 2018.

[27] EDRi, "France: Real-time interception of e-communications by security forces." https://edri.org/our-work/france-real-time-interception-e-communications-security-forces/, 2013.

[28] S. Murphy, "Watt Now: Smart Meter Data Post-Carpenter," *BCL Rev.*, vol. 61, p. 785, 2020.

[29] R. Brandom, "Police are filing warrants for Android's vast store of location data." https://www.theverge.com/2016/6/1/11824118/google-android-location-data-police-warrants, 2016.

[30] J. Hoffman-Andrews, "Verizon injecting perma-cookies to track mobile customers, bypassing privacy controls." https://www.eff.org/deeplinks/2014/11/verizon-x-uidh, 2014.

[31] S. Englehardt and A. Edelstein, "Firefox 85 Cracks Down on Supercookies." https://blog.mozilla.org/security/2021/01/26/supercookie-protections/, 2021.

[32] J. S. Choi, "Fingerprinting DNS over HTTPS (DoH)," 2021. Available online: https://smartech.gatech.edu/bitstream/handle/1853/64895/CHOI-UNDERGRADUATERESEARCHOPTIONTHESIS-2021.pdf?sequence=1.

[33] N. Weaver, C. Kreibich, and V. Paxson, "Redirecting {DNS} for Ads and Profit," in *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI 11)*, 2011.

[34] T. B. Lee, "Why big ISPs aren't happy about Google's plans for encrypted DNS." https://arstechnica.com/tech-policy/2019/09/isps-worry-a-new-chrome-feature-will-stop-them-from-spying-on-you/, 2019.

[35] A. M. Koshy, G. Yellur, H. J. Kammachi, V. Isha, R. Kumar, M. Moharir, and N. Deepamala, "An Insight into Encrypted DNS protocol: DNS over TLS," in *Proceedings of the 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, pp. 379–383, IEEE, 2021.

[36] M. T. Hunter, R. J. Clark, and F. S. Park, "Security issues with the IP multimedia subsystem (IMS)," in *Proceedings of the 2007 Workshop on Middleware for next-generation converged networks and applications*, pp. 1–6, 2007.

[37] S. M. Ali, M. Çakmak, and Z. Albayrak, "Security Classification of Smart Devices Connected to LTE Network," in *Proceedings of the International Conference on Smart City Applications*, pp. 1125–1131, Springer, 2021.