Barun ICT Global News

JUNE 2022

YONSEI UNIVERSITY Barun ICT Research Center

01

The True Price of Using the Internet

Jiri HAVEL

Department of Economics (MA Candidate), Yonsei University

A number of Internet companies have recently been under pressure regarding the handling of their data. Facebook's Mark Zuckerberg has been dragged through hearings about various concerns of the company's data protection policies and recent reports show that even its engineers do not know much about what's done with our data [1]. Similarly, Google has recently been pressured to give its customers the option to remove personal data from search by request [2]. Much of this is initiated via regulators who failed to foresee the growth of this sector and its impact on our privacy. General Data Protection Regulation (GDPR) in the EU was among the first drastic measures implemented, and it paved the way for other countries to implement similar policies. This, however, may affect the Internet firm's bottom line.

It is common for consumers to think that Internet platforms such as Facebook or Google offer their services free of charge. We pay for their services with our data and hence we need to keep track of how much we pay in terms of data. So, what's the exact price we pay? Does the price change over time or is it flat? These questions aren't easy to answer. When we sign up for any online platform, we pay upfront by providing basic information about ourselves but often, along the way of using those platforms, we pay extra by providing more information.

One way to assess the price of our data is to look at how online platforms inform us about updating terms and conditions occasionally. Those conditions almost always involve a clause about changes in our personal data use and since our data is the currency in the digital world, we should pay extra attention to these clauses. Every new right we agree to give them essentially represents a price increase for using online services. Similarly, we may view every additional piece of information they ask for as a price increase as well. With every new right we allow them and data points we reveal, we become a more expensive piece of information for a targeted advertisement, the main source of revenue of those firms. This has been well documented by Thomas Hazlett in his testimony on Facebook at the Senate Judiciary Committee [3] who argues that the amount of data companies like Facebook use has increased and has been more often used for targeted advertisement.

Although the regulators calls can be alarming and draw catastrophic scenarios, all the big online platforms, as well as the entire Internet market, keep growing and getting more popular. The fact that none of the "free" online platforms have converted to paid service is a manifestation that people are willing to pay the increasing price in terms of personal data and the rights to them. It is hard to believe, at this point, that someone would be willing to pay in dollars for using a search engine or social network platform. By introducing stricter regulations, the costs of Internet firms may increase and although one may only speculate about the real effect of this, there is a chance that it forces online platforms to cut back on the quality of their service or even implement a paid system.

Sources

[1] Franceschi-Bicchierai, L. (2022). Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document. Vice. https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

[2] Irwin, V. (2022). Google will now remove personal information from search by request. Protocol. https://www.protocol.com/bulletins/google-search-personal-information

[3] Senate Judiciary Committee. (2020, March 10). Hearing on Vertical Foreclosure and Antitrust Remedies in the Information Economy. Testimony of Thomas W. Hazlett on Facebook and the FTC

02

The Privacy-Convenience Trade-Off

Kostiulin MAKSIM

Department of Economics (Ph.D Candidate), Yonsei University

Voice assistants like Siri and Alexa bring convenience and efficiency to our daily lives. Powered by AI and IoT, these assistants are capable of voice interactions, controlling other smart devices, making to-do lists and much more. However, this technology is also powered by personal data collection, which puts it at the center of privacy concerns [1].

When you activate a voice assistant, it allows your device to collect and store every word you say and analyze your preferences and lifestyle. And it is not just AI that processes your records. Major voice assistant companies like Google, Apple and Amazon, employ thousands of people to manually sort and categorize users' voice data as a part of supervised learning [2]. According to Amazon, "employees are not given access to the identity of the person engaging in the Alexa voice request", a claim that was criticized after a series of errors when Alexa sent a private conversation of a coworker to the user's husband [3].

Alica, a voice assistant developed by Yandex, a Russian Internet giant, is another example of the possibilities of privacy breaches. Although Alica does not record voice data unless it is deliberately activated by a special word, Yandex acknowledged that sometimes it can be activated by similar words and then inadvertantly record private conversations [4]. The main reason behind errors like that is the fact that these

products are produced quickly, and the main algorithms are primarily designed for speech recognition, and only then at security. It doesn't matter if the voice assistant is activated by a phrase, is constantly active or is in the off state - a leak is possible. The received data can be used by a third party both for marketing purposes and for industrial or personal espionage. Since, in the activated state, the voice assistant saves all the information heard and can send it to the manufacturer for analysis, personal data becomes available to an unlimited circle of people. Therefore, when using voice assistants or smart speakers, it is recommended to limit the list of actions that they can perform, as well as to exclude the possibility of accidentally activating the voice assistant by setting a unique word to enable it.

Interestingly, a recent survey showed that the majority of users are aware of privacy-related dangers when using voice assistants, but choose to trade their privacy for convenience [5]. The main reason cited was that it became impossible to avoid public access to private data and resist the convenience promised by new services.

Sources

[1] Chalhoub, G., & Flechais, I. (2020). Alexa, Are You Spying on Me?: Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. HCI, https://doi.org/10.1007/978-3-030-50309-3_21

[2] Cellan-Jones, R. (2019, April 11). Smart speaker recordings reviewed by humans. https://www.bbc.com/news/technology-47893082

[3] Statt, N. (2019, April 10). Amazon's Alexa isn't just AI — thousands of humans are listening. The Verge. https://www.theverge.com/2019/4/10/18305378/amazon-alexa-ai-voice-assistant-annotation-listen-private-recordings

[4] Denisov, O. (2019, August 5). «Яндекс» отреагировал на сообщение о прослушке «Алисы. [Yandex responded to comments about eavesdropping]. https://ura.news/news/1052394143

[5] Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. Proceedings of the ACM on Human-Computer Interaction, 2(CSCW), 1-31.

03

Digital Medical Data: A Treasure Trove for Hackers

Dongha CHOI

Department of Life Science and Biotechnology, UIC, Yonsei University

When large amounts of medical data are stored digitally, they can then be accessed at high speeds [1]. Despite the benefits of digital storage, medical data is not fully protected; hackers can bypass security systems to illegally access the medical data of individuals. It must be protected because it can affect a person's dignity and cause harm when they are improperly disclosed [1]. Globally, hackers steal medical data for purposes such as blackmailing for money, which is why individuals need to know how to proceed if such a situation were to arise.

Vastaamo, a Finnish mental health provider, had its records of thousands of patients hacked and leaked online by the extortionist RANSOM_MAN [2]. Psychotherapy records often have sensitive information, including the patients' intimate notes and mental health conditions [3]. Vastaamo stored its patients' mental health records on a MySQL server, which had significant vulnerabilities. The company didn't anonymize the records nor encrypt them - a couple of firewalls and a login screen were the only things that protected the patients' confessions. This faulty security system easily allowed the hackers to steal the medical data of many patients, including a Finnish citizen named Jere. During his therapy sessions, Jere talked about his abusive

parents, drug usage, and thoughts about committing suicide. After each session, Jere's therapist would upload the therapy notes into Vastaamo's server, which the hackers stole. The hacker then demanded Jere to pay a ransom from €200 up to €500 so that his information could be deleted forever. "Those notes contain things I am not ready to share with the world," said Jere, "being honest turned out to be a bad idea [2]." Just like Jere, the hackers made the victims regret their decision in seeking help for their mental health, when it should have been highly encouraged to do so.

Another unfortunate data breach happened to The Hospital Group, which is the UK's leading specialist weight loss and cosmetic surgery organization. The hacker group known as REvil demanded a ransom after gathering more than 900 gigabytes of patients' photos, especially of their appearance before they did the surgery. Patients would be uncomfortable in disclosing such information because they find it embarrassing if someone else knew that they tried to change their appearance through surgery. Simon Hails, who did a chest reduction surgery from The Hospital Group, said, "I've tried to keep my surgery private and not even some of my friends and colleagues know about it, so the data breach is concerning for me [4]."

There are some actions that individuals can do after hackers steal their medical data to mitigate its effect. Because medical data contains personal information, individuals can be vulnerable to identify theft. To prevent this from happening, individuals should immediately ask for a copy of their medical record to see if their identity has been accessed fraudulently and contact medical facilities that asked for payments they didn't make and alert them of identity theft [5]. Moreover, victims who receive ransom demands can file an independent cybercrime complaint [6]. Although these actions may not change the fact that the hackers still have their medical data, taking action is better than not doing anything at all.

Sources

[1] Price, W. N., & Cohen, I. G. (2019). Privacy in the age of Medical Big Data. Nature Medicine, 25(1), 37–43. https://doi.org/10.1038/s41591-018-0272-7

[2] Ralston, W. (2021, May 4). They Told Their Therapists Everything. Hackers Leaked It All. Wired. https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/

[3] Shen, N., Sequeira, L., Silver, M. P., Carter-Langford, A., Strauss, J., & Wiljer, D. (2019). Patient Privacy Perspectives on Health Information Exchange in a mental health context: Qualitative study. JMIR Mental Health, 6(11). https://doi.org/10.2196/13306

[4] Tidy, J. (2020). Hackers threaten to leak plastic surgery pictures. BBC. https://www.bbc.com/news/technology-55439190

[5] Johansen, A. G. (2021). What to do after 5 types of data breaches. Norton. https://us.norton.com/internetsecurity-emerging-threats-what-to-do-after-a-data-breach.html

[6] Internet Crime Complaint Center (IC3). (n.d.). Frequently Asked Questions. https://www.ic3.gov/

04

Data Breaches and Remote Work: Do You Have a Cybersecurity Plan?

Christina LIU

Department of International Business, University of California, San Diego

With the pandemic increasing the number of those working from home, the rise of remote working policies and the work-from-anywhere mindset has kicked in for many workers. This increase in accessible workplaces has also created another COVID-19 side effect - cyber-crimes are increasing [1]. Since the start of the pandemic, online criminals have been using various social engineering attacks centered around the pandemic to distribute malware packages [1]. According to IBM's 2021 Cost of a Data Breach report, the average cost of one has increased 10% from 2020 to 2021, the highest single year increase in the last 7 [2]. In addition, breaches involving remote work as a factor saw the average cost being $1.07 million higher [2]. The expansion of the modern day "office" now puts companies in a vulnerable position as with an extension of locations from your living room to a local café, the expansion of their cybersecurity strategy must go beyond their traditional perimeters [3].

To help prevent these cyberattacks, systems like cybersecurity mesh architecture (CSMA), are used to decentralize cybersecurity and create "multiple access points that carry zero-trust enforcement the entire way [3]." The benefit of this system allows for a zero-trust enforcement to a variety of nodes which means that for

companies with hybrid or work-from-anywhere policies, they are able to then have fewer breaches and fewer financial losses due to cybersecurity incidents [3]. Further, with the advancement of artificial intelligence (AI), these systems can then be processed and categorized, enabling a pattern to be created that can help organizations spot and address threats quickly with less risk of infiltration [3].

Leveraging this with data security in the post-COVID world, it is important to consider it a top priority as many companies often push it down the list in preference of business continuity than actual cyber protection. With the switch to remote working, the habits and practices of companies are changing and so too are the rules of data security. This new normal of hybrid or remote workforces means ways for more accessibility but also more risk with many systems and servers not even having any access or authentication mechanism [1]. This on top of the fact that more advanced security techniques such as two-factor authentication and hard disk encryption are yet to be adopted by many corporations sets the scene for how vulnerable the technical frameworks are for business sectors that rely heavily on IT [1].

Remote working has become a norm in quite a few companies and with this becoming so common in our society the precautions needed to take place will only need to increase more given the fact that for many organizations it is no longer the size of the company that makes it vulnerable, but rather the security infrastructure itself that could compromise the businesses, big or small.

Sources

[1] Georgiadou, A., Mouzakitis, S. & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. Secur J. https://doi.org/10.1057/s41284-021-00286-2

[2] IBM. (2021). Cost of a data breach report 2021. IBM. Retrieved May 1, 2022, from https://www.ibm.com/security/data-breach

[3] Hounshell, L. (2022, April 29). Council post: Remote work is on the rise: Is your cybersecurity plan ready? Forbes. Retrieved May 1, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/04/29/remote-work-is-on-the-rise-is-your-cybersecurity-plan-ready/?sh=7b4bc442c289

05

Exploring Data, Privacy, & Smart Appliances

Miriam LIM

Department of International Business, University of California, San Diego

The convenience of modern technology comes at a cost with smart appliances; simple machines such as refrigerators and lighting can now be controlled through Internet technology at the user's convenience. The implementation of interconnected appliances is called a smart grid, which "is a traditional power grid with a communication network overlaid on top of the traditional power grid [1]." The smart grid is also referred to as the IoT network, which when connected online via home appliances, becomes a potential security threat to the users. These devices are able to collect a large amount of data, primarily regarding human behavior, which is all connected to the user's phone.

The security threats of the smart grid can be categorized into internal and external system threats. Internal threats are device deficiencies and can be categorized into four types: failure of home devices, power and Internet malfunction, software failure, and confidential data leakage. External system threats are those of devices being online on the Internet and also categorized into four branches: denial of service (DoS), malicious code injection, eavesdropping attack, and Man-in-the-Middle attack [2].

Internal threats as mentioned earlier are failures of the actual device themselves. Failure of home devices includes situations such as a security camera not being able to notify a user about a potential intruder in their backyard, or a smart light bulb turned on in the incorrect setting. Power and Internet malfunction highlights that these smart devices are unable to function without power or the Internet, and if the Internet is not running these devices cannot provide data to users [2]. Software failure is the vulnerability of devices to hackers due to poor authentication [2]. Confidential data leakage is when data collected by these smart devices is at risk due to poor encryption [2].

External system threats are risks to the smart grid being on the Internet. DoS "consists of flooding the home network by sending echo requests in a short time. Due to the hardware limits of the microcontroller (low memory and CPU), it can't manage a set of instructions in a short time which disrupts communication between home devices and prevents control access of the user [2]." Malicious code injection is code that hackers create to manipulate the system to invite unauthorized users onto the devices. Eavesdropping attacks are as the title suggests, not direct intervention but one of observation to collect information, also called sniffing attacks [2]. Eavesdropping attacks use networks such as Bluetooth or WSN's to steal data without intervening in the transmission process [2]. Man-in-the-Middle attack's are when two parties intercept the authentication process by having the first party send out the authentication request to the second party, who then manipulates the requests and sends it back out to the devices in order to get into the system and monitor

information [2].

With these threats in mind, it becomes increasingly important to monitor and check devices for vulnerabilities to keep data and individual security a priority. Education on data security becomes necessary as technology gets closer to intimate parts of individual's daily lives that appeared to be offline before.

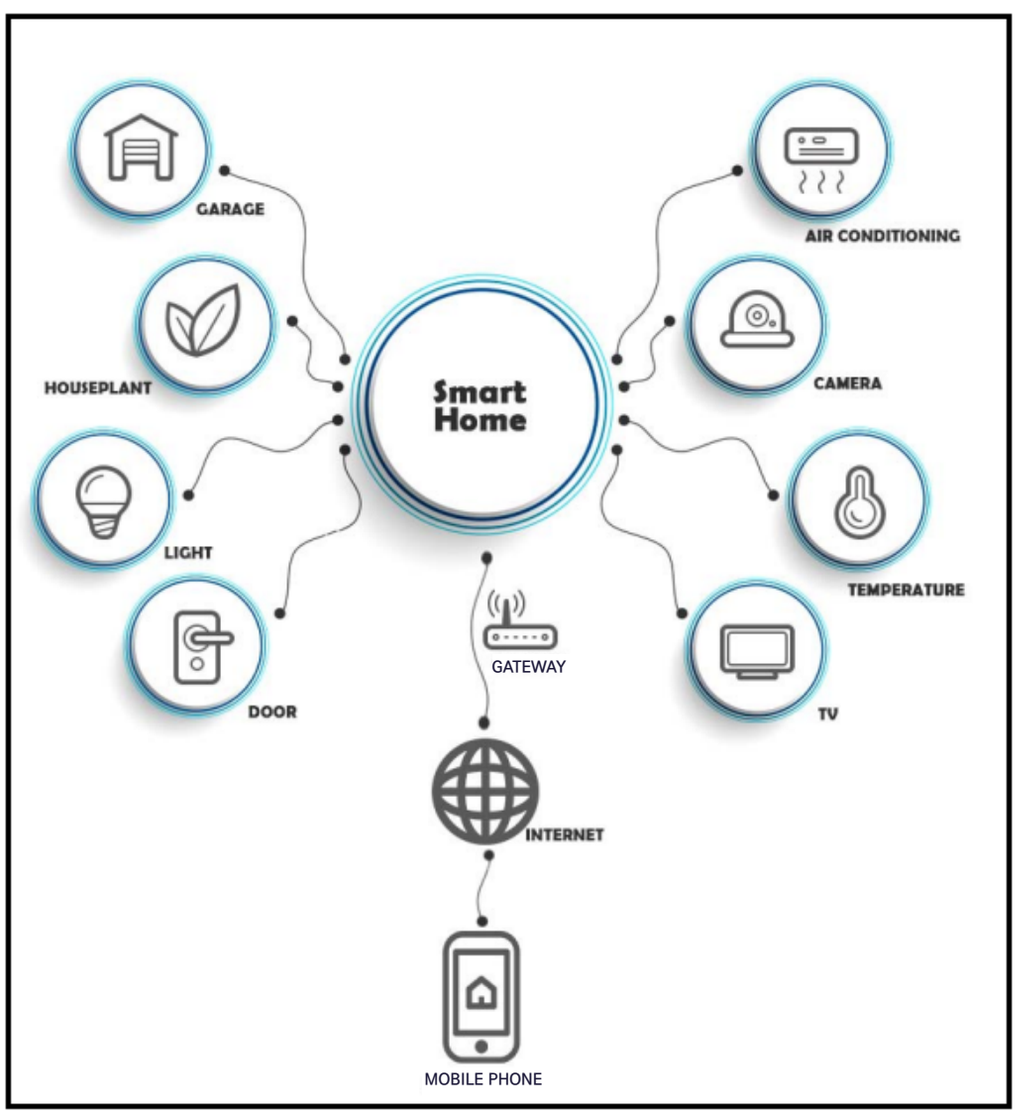


Fig. 1. Smart home-mobile phone system architecture.

Sources

[1] Goel, S., & Hong, Y. (2015). Security challenges in Smart grid implementation. SpringerBriefs in Cybersecurity, 1–39. https://doi.org/10.1007/978-1-4471-6663-4_1

[2] Notra, S., Siddiqi, M., Habibi Gharakheili, H., Sivaraman, V., & Boreli, R. (2014). An experimental study of security and privacy risks with emerging household appliances, 2014 IEEE Conference on Communications and Network Security, 2014, pp. 79-84, doi: 10.1109/CNS.2014.6997469.

06

Privacy and Security in the Context of IoT

Rodrigo Ayala PADILLA

Department of Nanotechnology Engineering,
Western Institute of Technology and Higher Education - ITESO

The Internet of Things (IoT) is a promising and convenient technology that has undergone rapid growth over recent years. It refers to the interconnection of electronic devices over a wireless network, in order to generate fast, easy, and even self-regulated communication that allows the exchange of data between devices [1]. IoT has many potential applications in our daily lives, ranging from fields like home automation, transportation, environmental monitoring, manufacturing, and many other processes which can be made more efficient by the reduction of human intervention [2]. For instance, the heating system of a home could communicate with a user's vehicle and turn itself on in advance, warming the temperature of the house upon the user's arrival, and at the same time, allowing the user to set the desired temperature remotely [3]. However, with the increase of complexity and size in these types of networks, concerns about security and privacy vulnerabilities also arise [3]. The traffic and gathering of information, as well as the autonomy of the network's devices, becomes exposed to threats and possible cyber-attacks that put privacy at risk [4].

The fragility of IoT systems lies in the many possible failure points the network can have. Flaws in a

device's software, poor communication protocols, or unwitting user disclosure of sensitive information are some of the risks that make the network highly prone to cyber-attacks. If a node gets corrupted, the whole network is compromised [1]. In addition, IoT security also faces another concern derived from the network's infrastructure: the manufacture of IoT devices are produced on a large scale, and many IoT accessories also share similar or identical features, which could compromise the security of the whole system if corrupted and increase the probability of massive attacks [2].

For many experts, IoT is considered to be one of the most fragile points where a cyber-attack can occur [1], with some of the most common privacy and security violations being identification, tracking, profiling, and other types of inventory and data leakage [4].

Better security techniques that can prevent this type of threats are constantly being studied and developed, but in addition to security protocols such as encryption, trespasser detection, and defense mechanisms, it is also important to consider the user as a key element of preventive protocols [4]. As the technology evolves, the user should also generate an awareness on the proper use of IoT and be updated on the security habits and common practices. In order to prevent unwanted third-party involvement, users would benefit from having a general knowledge of the data being recorded, and, more importantly, to be aware to what extent they should be cautious and selective with the information disclosed through any device [4].

The IoT is a technology that will play an increasingly significant role in our daily lives, and although it is a promising innovation that could provide new solutions to our everyday issues, there is still much to be resolved in terms of security and privacy matters. The challenge lies not only in the technical solutions that can be designed to shield the network, but also in familiarizing and making the user aware of this new environment, with devices constantly gathering and sharing information.

Sources

[1] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

[2] Husamuddin, M., & Qayyum, M. (2017). Internet of Things: A study on security and privacy threats. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 93-97). IEEE.

[3] Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2), 1606-1616.

[4] Aleisa, N., & Renaud, K. (2016). Privacy of the Internet of Things: a systematic literature review (extended discussion). arXiv preprint arXiv:1611.03340.

07

The Nature of Data Security in the Context of Cloud Computing

Jinwon PARK

Department of Economics, UIC, Yonsei University

Cloud computing has expanded in its possibilities in the last few years. Under normal circumstances, cloud users believe the cloud providers to be trustworthy and use the services based on that belief. For example, an individual may upload photographs on iCloud and delete them on their iPhone to maintain handheld storage space. They confidently delete the pictures because they believe that those would be safely stored in the cloud and can easily be downloaded whenever desired. The same applies to enterprises; companies store their internal data on an external cloud under the premise that the data is secure.

However, what would happen if an outsider hacked the data, infringing upon security? Confidential data could be exploited by competing companies, and massive losses would be incurred. As for healthcare, data theft could cause serious harm to individuals since medical records contain personal material. Additionally,

with such widespread use of smart devices, individuals are vulnerable to privacy risks if the criminal gets access to their data. Thus, data security is essential when using cloud computing.

Kumar et al. (2018) suggested that maintaining "Confidentiality, Integrity, and Availability (CIA)" is crucial to protecting data security. Confidentiality means that the data should not be revealed to other unauthorized parties under any circumstances. The data in transit or stored in the cloud should not be tampered with by unauthorized parties, indicating integrity. Finally, availability signifies that the data should be available to the cloud consumer without delay or denial [3]. As for individual endeavors, users could increase data literacy and grow data awareness to protect their data from misuse. They should refrain from arbitrarily publishing private information that could be susceptible to criminal acts [4]. Cloud users could also regularly back up and keep track of their data location [3].

Cloud computing can help individuals, employees, and business in various fields to facilitate storing and sharing of personal data. However, there could be incidents of data leakage or infringement upon privacy. Thus, along with the corporate responsibilities of the cloud providers, individual users should acknowledge the potential problems and act to prevent any damages.

Sources

[1] Hogan, M., & Sokol, A. (2013). NIST Cloud Computing Standards Roadmap Version 2. NIST Cloud Computing Standards Roadmap Working Group, NIST Special Publications 500-291, NIST, Gaithersburg, MD, 1-113.

[2] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy? IEEE Cloud Computing, 5(1), 31-37.

[3] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

[4] Zhang, D. (2018, October). Big data security and privacy protection. In 8th International Conference on Management and Computer Science (ICMCS 2018) (Vol. 77, pp. 275-278). Atlantis Press.

08

Digital Footprint and Privacy: Do You Want a Cookie?

Lilit NIKOLAYAN

Department of Korean Language and Literature, Yonsei University

Who doesn't love cookies, right? But today we're going to talk about not the delicious food we all eat in the morning with coffee, but small data files that save time, while allowing us to access our favorite websites easily - without the need to enter passwords every time [1]. Most of us just simply accept those "cookies" and move on, but what is a cookie actually? Are they a threat to people's privacy?

IoT has rapidly gained popularity over the past few years due to the fact that those technologies are applicable to various purposes, including communication, transportation, education, and business development [2].

Concerned about it, Toby Walsh, professor of AI at UNSW in Sydney, mentions "the problem is that we are connecting ourselves, our homes and our workplaces to lots of Internet-enabled devices: smartwatches, smart light bulbs, toasters, fridges, weighing scales, running machines, doorbells and front door locks. And all these devices are interconnected, carefully recording everything we do [7]."

Yes, we indeed use various applications that give us pieces of advice about everything, including possible diet routines based on our personal information, apps that remind us to drink water to stay hydrated, and count the steps we take every day to lose weight and stay in shape. But what steps do we have to take to not lose our privacy while we do so?

The federal law securing our electronic information was passed in 1986, making it older than the world wide web itself [3]. Yet, every time we visit a new site, we get an instant notification that the page is using cookies to track us and we have to accept them in order to have access. Of course, we can read the policy before accepting, but how many of us actually do? Almost none. It is true that cookies can indeed be helpful for many reasons, such as keeping you logged in or remembering your preferences based on the sites you frequently visit. And that is how and why we get surprised sometimes about just how well the Internet "knows" us and our preferences.

In fact, cookies are just small pieces of personal information stored about you, alerts that are supposed to improve our social privacy. But do they protect it or take it away from us? Does the law work or is it just another way to follow our digital footprints?

According to Shane Green, CEO of private data sharing platform digi.me, cookies are pretty useless. If you don't accept them, sometimes the website won't work, but most of the time it will. Therefore, they're quite similar to those annoying pop-up ads we get on our screens every time we're online [4].

However, in recent years, consumer opinions on cookies and other forms of personalized third-party tracking have changed. Following scandals like Cambridge Analytica, when it was discovered that Facebook gave unauthorized and unfettered access to personally identifiable information (PII) of more than 87 million individuals without their consent to the data firm Cambridge Analytica [5], there has been a growing awareness in society about the extent to which tracking is intrusive, and how it can be used to perpetuate preconception and inequity.

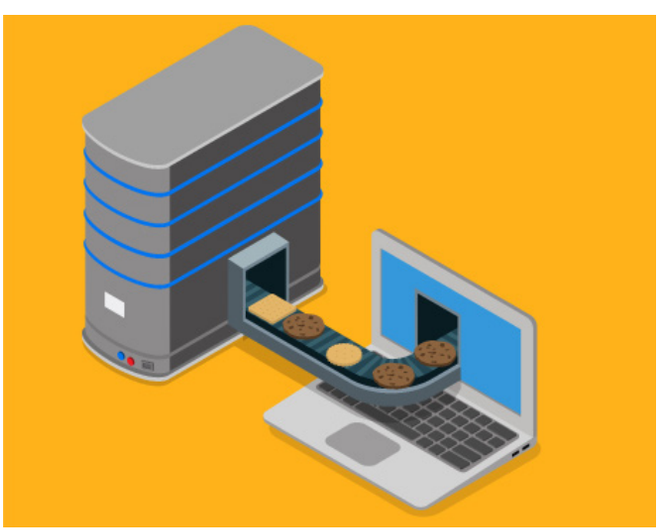
Therefore, the Safari browser has blocked some third-party cookies since 2017, and all of them since 2020. Firefox has also blocked some third-party cookies since 2019, and launched Total Cookie Protection in 2021 which stores cookies in separate "cookie jars," preventing information from being shared between websites. Despite originally being planned for 2023, Google Chrome will start blocking third-party cookies only in 2024, which is almost a year later than anticipated. Yet, it seems like Internet tracking isn't going away, only the methods are constantly changing. For example, Google announced it is replacing cookies with a new feature called "Topics [6]."

So questions arise: what can we do? How can we protect our personal data?

Professor Walsh, while talking about Internet-enabled devices, suggested an alternative plan that requires all digital services we use to provide four changeable levels of privacy. According to this plan, in the first level, apart from your username, email, and password, they don't keep any information about you.

In the second level, they do collect certain information for the purpose of providing you with a better service, but they do not share this information with anyone. The third level is when the information stored about you may get shared with subsidiary companies. And the last, fourth level, is when your personal information is considered public. The professor mentions that this way, everyone can change the level of privacy with one click from the settings page. Any changes are backdated, therefore, if you choose Level 1 privacy, the company must delete all information they currently have on you, beyond your username, email, and password [7].

Being monitored 24/7 every day, it is in fact hard to secure our privacy. So are we stuck with cookies and Internet tracking? The answer is yes. Can we stop the process? No. At least, not in the near future. Unless we stop using the Internet entirely and start making our own cookies, simple ones. Homemade, in the oven – harmless and without any form of tracking.



08

Sources

[1] Lynn, B. (2021). Will the End of Internet 'Cookies' Bring More User Privacy? Science and technology. https://learningenglish.voanews.com/a/will-the-end-of-internet-cookies-bring-more-user-privacy-/5809138.html

[2] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

[3] Calabrese, C. (2010). Electronic Privacy Law is Older Than the World Wide Web — It's Time for An Upgrade. ACLU. https://www.aclu.org/blog/speakeasy/electronic-privacy-law-older-world-wide-web-its-time-upgrade

[4] Stewart, E. (2019). Why every website wants you to accept its cookies. Recode. https://www.vox.com/recode/2019/12/10/18656519/what-are-cookies-website-tracking-gdpr-privacy

[5] Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer, 51(8), 56-59.

[6] Guinness, H. (2022). Cookies are going away, but internet tracking may still be here to stay. Popular science. https://www.popsci.com/technology/cookies-internet-tracking/

[7] Walsh, T. (2022). How to preserve our privacy in an AI-enabled world of smart fridges and fitbits? Here are my simple fixes. The Conversation. https://theconversation.com/how-to-preserve-our-privacy-in-an-ai-enabled-world-of-smart-fridges-and-fitbits-here-are-my-simple-fixes-180245

Barun ICT Global News

Publisher: Beomsoo KIM
Editors: Seungyeon WON, Alexandra STEPHENSON
Translators: Kyongju YU, Yeeun SHIN, Nahye HONG
Designer: Subin LEE

June 2022

** Please note that any external contributions to the Global News do not represent Barun ICT's official views.*

YONSEI UNIVERSITY

Barun ICT Research Center

Barun ICT Research Center, Yonsei University
50 Yonsei-ro, Seodaemun-gu, Seoul 03722, Korea
+82-2-2123-6694 | www.barunict.org

https://www.instagram.com/barunict/
https://www.facebook.com/barunict/