GDPR Extension for Internet of Things (IoT) Devices

Seung Jun Eom, Annabelle Gartner, Uday Samavenkata, Harshala Yadav

CS 578-A
Professor Susanne Wetzel
December 16, 2020

GDPR Extension for Internet of Things (IoT) Devices

December 16, 2020

Uday Samavenkata	Harshala Yadav	Annabella Gartner	Seung Eom
usamaven@stevens.edu	hyadav2@stevens.edu	agartner@stevens.edu	seom@stevens.edu

Phrase: “Smart home devices are snooping on you, and there are no sufficient privacy policies that protect you.”

Keywords: Privacy, Security, Internet of things, Smart home, GDPR, CCPA

Project Description: We are going to be evaluating current policies that protect IoT user’s privacy. The main policies in question are the GDPR and CCPA. We will analyze and see whether these policies meet sufficient standards to protect people's rights to privacy in an IoT system. To conclude our analysis of the failures of IoT systems in protecting IoT user’s privacy, we propose an IoT-specific extension to the GDPR that addresses the shortcomings that IoT devices have in protecting user privacy.

Responsibilities for group members:

All group members are required to help research the flaws of the GDPR and CCPA, and see how IoT devices are exploiting the flaws in them. From there, we split up the directions of the research in four ways. Seung will lead the initial research in finding the flaws in the GDPR and CCPA and see how these flaws would have to be addressed in the GDPR extension. Harshala will be researching related works to our research and distinguish our research from others, and analyzing the IoT system against Daniel J. Solove’s Taxonomy. Annabelle will focus on the economic concerns and bias against small companies that come with having a weak privacy policy for IoT devices. Uday will lead the proposal for the draft of the additional article that will be added to the GDPR, article 92(a). All of us are peer editing each other’s research so that the project stays coherent.

List of Deliverables:

- Research on additional literature to find more information
- Research on flaws of the GDPR and CCPA in relation to IoT devices
- Research related works and their impacts on the IoT industry
- Develop a possible way to hold companies/government more accountable
- Final report discussing findings and proposing a new IoT-specific GDPR article
- Editing and cleaning up final project

Research:

Research for this project began with an analysis of current privacy regulations that are either ratified or in review. The conclusion of this investigation allowed us to specify our research on two notable privacy regulations: the General Data Protection Regulation (GDPR), which created in 2016 and implemented in 2018, and the California Consumer Privacy Act (CCPA), which was signed into law on June 28th, 2018, and is set to become effective in 2020. These two particular regulations are the most important, as of right now, for two reasons. First, the GDPR has been in effect since 2018, which means there is actual data that can be extracted from its effects on real people that can be utilized to better future privacy legislation. Second, the CCPA is the first notable piece of legislation to be passed in the United States, and its repercussions will similarly influence any legislation that the US decides to implement on a federal level. Since we wanted to make sure that our references to these regulations were heavily privacy-based, almost all of our research was conducted using articles from reputable sources like the International Association of Privacy Professionals (IAPP) as well as the Institute of Electrical and Electronics Engineers (IEEE). In addition to these notable journals, our team also references research presented by experts to the Senate Judiciary Committee, such as Roslyn Layton's testimony titled "On the General Data Protection Regulation and the California Consumer Privacy Act: Opt-ins, Consumer COntrol, and the Impact on Competition and Innovation", which specifically focuses on what the American government can glean from the GDPR in order to enhance their future privacy legislation. Finally, our team also focused on reading and analyzing actual privacy legislation by reading the GDPR and the CCPA *itself* in conjunction with critical analysis on its efficacy. Our team made sure that rather than researching this topic through a singular lense, our research contained diversified opinion and information on the GDPR and the CCPA.

GDPR Eight Rights vs. Internet Connected Devices:

The GDPR is a European Union (EU) exclusive set of legislation that protects EU citizens' privacy rights. It was put into effect in May 2018 as an effort to expand the privacy rights of any natural persons that use a product or service that is offered in the EU [1]. Within the GDPR, there are eight fundamental rights that the EU guarantees to its citizens. To observe whether a particular ecosystem that deals with people's privacies is a safe space for them, the ecosystem can be put against these fundamental rights set out by the GDPR, and see if it protects these rights, or violates. When discussing IoT devices with respect to these eight rights, IoT devices unfortunately show that the IoT ecosystem either has inherent violations of these rights stated in the GDPR, or the GDPR does not cover IoT devices in specific, leading to IoT consumers not being protected by the legislation set forth by the GDPR. The following discussion will analyze the GDPR's eight rights one by one, and see how IoT systems stand up against these rights.

Right to be Informed

The first right that the GDPR guarantees for its citizens is the right to be informed, where individuals have a right to know who is processing their personal data, found in article 5.1(a) of the GDPR. This should also mean that IoT customers should know who is responsible for the data collected by their wearables, smart speakers, etc. However, informing an IoT user what is happening with their data is not as straightforward for IoT devices. For one, IoT providers can choose to be vague in how they inform the IoT user about relevant personal data [2]. This is because the GDPR does not specifically specify whether it will be necessary to notify the user about relevant information on a timely basis to the user. The GDPR also does not state a protocol of how a clear communication line should be established between IoT users and IoT servicers, leading to IoT users not being able to be properly alerted about any changes that might have happened to the handling of their personal data. Maybe they are using a new collection algorithm, or a new database is implemented. But because there is no clear line of communication set up between the IoT provider and its customers, informing the user becomes vague and difficult.

Right to Access

The second right that the GDPR guarantees for its citizens is the right to access, where individuals have the right to access any personal data that has been collected about them, found in article 15 of the GDPR. The GDPR mandates a tool called the Data Subject Access Request (DSAR) in this article, which allows for EU citizens to request access to their data that a company may hold about them [3]. While this tool worked for EU citizens for other companies in different industries that collected data through other means, using this tool on IoT companies becomes difficult. In an IoT ecosystem, user data does not stay in place on one device, in fact, data will be jumping from one device to another, and this may happen even more times to arrive at the final destination where the user data will be stored [3]. So for customers to access all their data may not be possible as it is largely scattered, or it requires much more resources for companies to aggregate all of the user's data in one place, as compared to accessing the data from a single database.

Right to Rectification

The third right that the GDPR guarantees for its citizens is the right to rectifications, where individuals have the right to require organizations to correct inaccurate personal information, found in Article 16 of the GDPR. Building off the point that user data is scattered across multiple databases and devices, this also leads to difficulty in correcting individuals' data. Correcting data in one device would have to result in corrections to all of the other devices that got a hold of that data and are storing inaccurate personal data [4]. This again, becomes difficult to manage and will require more resources than usual to correct the personal data on all devices.

Right to be Forgotten

The fourth right that the GDPR guarantees for its citizens is the right to be forgotten, where individuals have the right to have their personal data deleted and prevent further collection, found in Article 17 of the GDPR. Erasure becomes a challenge for two main reasons. For one, the issue of data being scattered as discussed before becomes a hindrance for erasure, as data will be stored in many devices, making deletion of that data on all devices difficult. As for the second reason, IoT users are not usually aware of all the types of data that is being collected about them, so users may not be aware of what data they need to be deleting. IoT devices may have collected data that may be a breach of privacy for the users, but the user will not be able to erase the data about them without extra effort from the user.

Right to Restrict Processing

The fifth right that the GDPR guarantees for its citizens is the right to restrict processing, where individuals have the right to require organizations to restrict the processing of specific categories of personal data, found in Article 18 of the GDPR. This is a right that is especially particular to IoT devices. Countless news reports and investigations have found smart home speakers such as the smart speaker line from Google have been reported to have been collecting information outside of what Google should have access to. Google has been investigated for listening to audio that was not authorized by Google's smart speaker's wake word, "Ok, Google" [5]. Google was accused of listening to personal conversations, professional phone calls with private information, interactions between family members, and other sensitive information. Other companies that produce smart speakers such as Amazon and Apple also had similar accusations against them. Smart home speaker producers have been notorious for listening when they are not prompted to, and the GDPR is currently not protecting that right for citizens to protect their privacy in some sensitive regions of their lives.

Right to Data Portability

The sixth right that the GDPR guarantees for its citizens is the right to data portability, where individuals have the right to require organizations to transfer personal data to a recipient of their choice, found in Article 20 of the GDPR. When investigating IoT devices against this right, IoT devices show that

data portability is not an absolute right held up by IoT devices. The GDPR outlines specific conditions that need to be met before the right to data portability can be exercised. There must be explicit consent given by the user, and the personal data that is being processed is also being carried out by automated means [6]. This means that personal data that does not fall into this category would mean that the IoT user cannot exercise the right to data portability, leading to a failure of IoT devices in protecting this GDPR right for its customers.

Right to Object

The seventh right that the GDPR guarantees for its citizens is the right to object, where individuals have the right to consent or withdraw consent to the processing of their personal data, found in Article 21 of the GDPR. Before using an IoT device, IoT users have to accept a user policy and privacy policy. In that policy is where the manufacturer would have specified what types of data the IoT device is allowed to collect, what data needs to be protected for the user, etc. But oftentimes, the policy that is set in stone will specify the certain categories of data that would be covered by the privacy policy [3]. While these policies are great in protecting the rights explicitly stated in the policy, this leaves out the data that was not specified in the policy. This becomes an issue for IoT users because the privacy policies that are set in place are static, and it does not match the dynamic nature of IoT devices. IoT devices have shown that they have the ability to access multiple categories of data, so a static policy will not allow users to object to what data will be collected or used. Thus, the consumer does not have the choice to object or consent with the data that was not covered by the initial privacy agreement, leading to IoT providers to have full control in that area.

Right to Avoid Automated Decision Making and Profiling

The last right that the GDPR guarantees for its citizens are the rights in relation to automated decision making and profiling, where individuals have the right to opt-out of the use of their personal data by automated systems, found in Article 22 of the GDPR. Going back to the point that was made before, users may not be aware of the categories of data that was made available to the IoT device if the type of data that was breached was not known by the user. This leads to the user also not being aware when the IoT device uses that data in an automated system [7]. If users are not aware of whether their data was made available to the automated systems, they also cannot express their right to be forgotten/erased.

Economy and GDPR

One of the largest components behind the United States' inability to nail down *federal* privacy regulations is the estimated cost of compliance and its detrimental effects on businesses. Economic experts have researched real business practices of tech companies that are concerned with the security and privacy of IoT devices, but are also realistic in their utilization in business. The unfortunate precedent is the EU's Privacy Regulations (the GDPR), which have created significant challenges for the enterprises who are subject to it. For example, GDPR mandates that companies appoint a data protection officer (DPO) to "spearhead compliance". According to economist Sarah Rausch, a DPI is "almost a unicorn of a role" since "you need the chops of a lawyer, some computer science knowledge, ability to coordinate large organizational change, awareness and education in the workforce and an ability to talk to regulators too". While this is only one unwieldy expectation as a result of GDPR, Rausch continues by presenting several business issues that seem to block the creation of federal law. The biggest issue is compliance, which is the number one concern regarding the implementation of privacy and security regulations in business. There are too many potential legal risks associated with adopting privacy and security laws federally, since they would continuously be subject to change and would be too costly to keep up with. Additionally, these laws would have to be written in a way that people without technical knowledge would be able to understand them, which is something that associate director of security and privacy at Protiviti is especially concerned with. Technical writers with this type of knowledge are also a large cost for companies that are attempting to remain compliant. If employees do not understand the laws themselves, they cannot ethically be subjected to the consequences of breaking these regulations.

Speaking strictly in terms of privacy in business practices, it seems as though companies in the US are actually very interested in adopting some sort of privacy regulation, but can not do it in a cost-effective way. The money that is lost in this context is not due to the lack of data a company will be able to use if privacy policies are enacted, but because of the fear of being fined for accidentally breaching a regulation. These companies are also concerned with the wellbeing of their employees as well, and are unsure of how to best educate their employees in regards to privacy in order to protect them from potential legal fines as well.

According to the International Association of Privacy Professionals (IAPP), the estimated cost of GDPR compliance for the average firm of about 500 employees is approximately $3 million dollars, which for many technology companies is not a prudent investment. In fact, this lofty amount is more than likely to illicit bankruptcy from smaller tech companies who are emerging in the field, and are not as developed as tech giants like Google, Facebook, and Amazon. This is the other significant component of the GDPR's weakness: its bias towards larger companies, and its scrutiny towards smaller ones.

Nobel Prize Economist George Stigler observed that "regulation is acquired by industry and operated for its benefit", which means that larger firms have welcomed GDPR eagerly because it functions as a method of insulation from competition. This concern has, however, already come to fruition in the European Union. According to Roslyn Layton, who has worked at Denmark's Center for Media and Information Technologies at Aalborg University to research privacy and security technologies, small ad tech competitors in the EU have lost about one-third of their market share, which Google, Facebook, and Amazon have increased their market share in the EU. This is speculated to be the result of the high cost of GDPR compliance that can only be mitigated by large tech giants. In the US, where federal lawsuits are already being held against tech giants like Google for holding monopolies, the GDPR would only strengthen these companies' monopolies and allow them to shape technological privacy to their will. This is especially true as of December 9th, 2020, since the FTC has filed a suit against Facebook for Illegal Monopolization, alleging that "the company is illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct". The IAPP has also stipulated that Fortune 500 firms have reportedly earmarked $8 million for GDPR upgrades. This amount is *only* for EU regulation, and the IAPP asserts that the total GDPR compliance costs for US firms alone could reach $150 billion, which is one-third of annual e-commerce revenue in the US. These numbers are a clear indication that the practice of privacy regulation is business as we see it now is a rich man's game-setting clear boundaries between innovators who will be stifled by the crippling costs of compliance that the GDPR compounds. As of today, less than half of eligible firms are fully GDPR compliant, and one-fifth say that full compliance will never be possible.

Results from GDPR Research

Overall, the GDPR shows that it can provide protections that work in a generalized manner, giving board and overarching protections. It does cover fundamental rights that are indeed protected in other areas that use privacy and personal data. But the discussion of IoT devices in regards to the GDPR shows that the GDPR is not specific enough to cover the privacy concerns specifically raised by IoT devices.

CCPA vs. Internet Connected Devices:

Similar to the GDPR, California put into legislation what would be considered their own version of the GDPR for California residents.

The CCPA was made effective as a law by 2020, making this a more recent law compared to the GDPR. It was meant to be its own version of the GDPR for California residents, deriving a lot of the rights protected by the GDPR into the CCPA. Like the GDPR, the CCPA guarantees certain privacy rights, but the difference between the CCPA and the GDPR is that the CCPA covers four fundamental rights, while the GDPR covers eight. The rights covered by the CCPA are the right to be informed, the right to erasure, the right to opt-out, and the right to nondiscrimination. The first three rights correspond

to three of the eight rights covered by the GDPR, but the right to nondiscrimination is a right that is not explicitly covered by the GDPR [8]. As the fallacies of the fundamental rights that were covered by the GDPR was covered in-depth, it is much more important to note how the CCPA overall falls short in comparison to the GDPR, as the GDPR covers more fundamental rights than the CCPA, and the CCPA is much more restrictive in what type of data is covered by their scope, and who is protected by the CCPA.

Flaw One: Broad Definitions of CCPA

While the GDPR covers a broad definition of data, defined as "data from which a living individual can be identified or identifiable," the CCPA actually states that it exempts specific medical and publicly available government records in its scope [9]. The CCPA does not specify any special protections for the type of data that would fall under these categories, leaving California residents to be unprotected in that sense. By leaving out of its scope some areas of data, the CCPA compromises the privacy of users.

Flaw Two: Discrimination in Protection

The CCPA is also very limiting in the types of people that are covered by the legislation. The GDPR gives a broad definition of who is covered by the GDPR, providing data protection to any natural persons regardless of their nationality or place of residence, so as long as the consumer is using a product or service that is offered by the EU [1]. On the other hand, the CCPA specifies that only legal persons residing in California are protected by the CCPA, meaning that all non-residents are excluded from this legislation, dividing California's population between those who are covered by the CCPA, and those who are not.

Results from CCPA Research

Based on these two observations, it becomes clear that the CCPA falls short in comparison to the GDPR. This makes it really easy for a company that produces IoT devices solely for the California market to get around regulations that would otherwise hinder their operations and protect user privacy. If it is the case that this company does not service any persons that are associated with the EU, the company would not have any legal obligations to abide by the legislation set for by the GDPR. The company can get away with not providing the same comparable amount of rights that are covered by the GDPR, they have more flexibility in the type of data that does not need much protection, and they do not have to worry about providing the same level of privacy protections to non-residents living in California versus a legal resident of California.

Related Works:

Works related to GDPR and CCPA regarding IoT devices include – "The Security of Connected Devices Act" and "IoT Cybersecurity Improvement Act of 2020".

"**The Security of Connected Devices Act**" [9] went into effect on January 1, 2020, covering manufacturers of IoT devices which must adhere to this cybersecurity law. In contrast to the current law, the earlier one for connected devices required a business to take necessary action to ensure that all customer logs or records containing personal records must be disposed of by either shredding, erasing or making the records unreadable. The earlier law also stated the business operating out of the state of California must implement and maintain reasonable procedures and practices appropriate to protect the personal information from unauthorized access, abuse, or defamation [12]. The consumer taking benefits of the service can institute a civil action to claim damages in case of violation by the business. Although, the law fails to clearly mention the penalty for the same. The current law states that manufacturers must provide reasonable security and specifically, it should meet the following requirements –

· The preprogrammed password is unique to each device manufactured

· The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

Moreover, the law applies only to California at the moment and can only be enforced by the attorney general, a city attorney, a county counsel, or a district attorney. However, there are several shortcomings in this law –

· No penalty for violating the law
· Hard to prove a violation occurred
· Enforcement is delegated exclusively to California Attorney General, city attorneys, county counsels, and district attorneys
· The law does not apply to connected devices already subject to federal security standards.

The current law and the preceding one are therefore quite vague on its applicability, definition of connected devices, scenarios covered under the law, and the definition of reasonable security.

The second related work which was researched is the "**IoT Cybersecurity Improvement Act of 2020**". This bill, now a public law – signed by the President on December 4, 2020, is specific to only IoT devices used by the federal government. Specifically, the act requires that National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) take necessary steps to ensure all internet connected devices purchased by the federal government must conform to the minimum-security guidelines issued by the National Institute of Standards and Technology. The NIST is tasked with developing and publishing guidelines for all federal agencies on the appropriate use and management of IoT devices. OMB is required to review agency information security policies and principles provided by NIST using their standards and make recommendations as necessary. The NIST is supposed to review and revise the policy every five years if deemed suitable. The OMB is responsible to update any policy or principles to complement the changes recommended by NIST. The NIST is the responsible party to develop and publish guidelines regarding security vulnerabilities intended for agencies, contractors, and subcontractors. The OMB shall develop and oversee that the vulnerabilities guidelines, policies, standards listed out by the NIST are implemented. Any federal agency is prohibited from procuring, obtaining, and using an IoT device as listed in the guidelines devised unless necessary for national security or for research purposes subject to a waiver. The Act complements California's IoT device security law (Cal. Civ. Code §§ 1798.91.04–1798.91.06). The Act was hoped to provide guidelines to both the public and private sector.

Our research proposes recommendations to satisfy the shortcomings from all the existing policies [10]. Some of the proposed recommendations are that the IoT manufacturers are to be responsible to get the consent of the user buying or using the IoT device. The user need not be responsible to micromanage the device as in to ensure privacy. In case of data breaches or breach of law the responsible party should be subject to appropriate fine. The consumer is to be provided full control of data and be provided with logs if requested for. Another fine recommendation comes in the form of privacy labels which would summarize security details into keywords. The keywords together would constitute a privacy label on the IoT product to help the user with informed decision making.

Daniel J. Solove's taxonomy:

The "Taxonomy of Privacy", suggested by Daniel J Solve, attempts to account for the consequences that arise from infringements of privacy [11], is the framework that very closely applies to the world of Internet of Connected Devices (IoT), and is helpful to understand the threats posed to IoTs. Solove's taxonomy comprises four categories – Information Collection, Information Processing, Dissemination of Information, and Invasion. Each of these major categories are sub-categorized into categories at a more granular level. Let us see the possible threats to IoT dominant in the different phases of the taxonomy.

Threat of Identification

Identification is defined as the act of revealing a person's digital identity by associating data found in a data lake. An IoT device is a product meant to track data events and collect logs of data for analysis or querying and providing an answer. While doing so, humongous amounts of data is collected and stored to a centralized repository. This stage of data transfer is categorized under the data processing in Solove's taxonomy. The threat of identification is most prominent in the data processing stage where the subject of the data does not have a control over it. Also, specifically for IoT devices, this threat materializes in the interaction and collection phase. For example, facial features, fingerprints, and voice samples can be used to identify a person even though they might exist along with troves of data of other people. Evolving technologies, interconnection and interaction features aggravate the threat of identification.

Threat of Localization and Tracking

This is the act of locating and recording a person's location in time and space. Tracking a person requires identification at the least to assign the tracked metrics to a particular user. Tracking is possible through GPS, cookie tracking, and mobile device-based tracking. In such scenarios, the person being tracked has an uneasy feeling of being tracked and does not have a sense of control over it – it being due to unaware of its disclosure, or if information is used and combined in an appropriate context. Although, it is not a privacy issue if the subject being tracked is in the physical proximity of the tracker, this is a valid threat when the process is beyond the subject's control. This kind of threat mainly appears in the processing phase in Solove's taxonomy and might also appear in the interaction phase. Specifically, for IoT devices, this kind of threat is aggravated as the IoT devices have access to the user's personal lives inside their homes and wherever the person travels at all times. Moreover, data collection is becoming efficient at its task and mostly done so without the user noticing. Another reason why this threat is valid is because in the case of IoT devices the user interacts to feed data and receive a response which leaves data trails that put the user at risk of identification.

Threat of Profiling

Profiling is defined as the threat of compiling information reports about an individual to calculate interests based on other profiles having similar choices using correlation. This type of method is most common and used in subscription-based businesses, e-commerce, newsletters, and advertisements. It is also used for internal optimization based on customer demographics and interests. The threat appears in the information dissemination phase while the data is being utilized by third parties. This also applies well to the world of IoT devices as IoT devices are straightforward pipelines gulping consumer data in the form of video feed, voice samples, choices, keywords. IoT devices also have a slight edge over other data collection mediums in that they have access to quality data as the data feed is directly in close proximity to the consumer and personal identifiable information in the case where the consumer inputs data. Although there are efforts to protect consumer privacy and assurances on the part of business, there still exists a fine balance to satiate the needs of the business in complementing the need to satisfy the user and maintain privacy.

Privacy-violating conveyance

This threat refers to the violation of privacy by means of public medium in an attempt to distort a person's image in the society. The context in which this applies to IoT devices is that the attacker might try to intimidate the consumer by disclosing private information over smart devices based in a private or a public location to dishevel the person's identity or reveal misinformation to damage his or her reputation. Although disclosures of such kind are not quite apparent, IoT devices have vulnerabilities using which attempts have been made by hackers to attack users in the past. This kind of threat is bound to grow in the near future with the rise of IoT based devices being adapted by the mass consumers. Filtering of private-sensitive personal data is the key to address this threat. Another way this threat can be mitigated by the use of scoping is by intending that an IoT device accurately disseminates information solely to the intended party.

Proposed Policy Extension:

To deal with the problem that current policies are not effective enough to deal with the amount of personal information IoT devices collect, our solution to the problem is a policy extension. We propose an official article extension that is to be added to the GDPR called article 92a (shown at end of section) which would give consumers more privacy protections when they use IoT devices. To first construct this extension, we had to learn the format of the GDPR. The GDPR is split into 10 chapters each consisting of multiple articles concerning privacy rights. We felt that our mock article would best fit in chapter 9 (Provisions relating to specific processing situations) because IoT devices need a more specific ground for better privacy protection. Our article covers 7 main additions to the GDPR: informed consent, right to be forgotten, accessible data for IoT users**,** micromanagement by consumer, logs, fines, and an IoT label. The reasoning behind why we included these 7 additions are below.

Informed vs Broad Consent (Number 1 of Article)

The problem with consent involves the two different definitions of consent, broad and informed consent. The GDPR doesn't explicitly say which consent should be used, or the definition of the types of consent. Broad consent is when the average person's knowledge on the subject provides consent, while informed consent is when the person has done research and knowledgeable on the subject before consenting. Our proposed addition to the GDPR requires that the company creating the IOT device will be required to explain the difference between informed consent and broad consent and explain the possible privacy implication of IOT devices. Furthermore they should provide resources such as links or reading references so that a person concerned for their privacy can better judge whether or not the product is for them. It also should also include that withdrawing consent does not differentiate between the right to hold data, or the right to use data. This should clearly be explained in IOT policies and is mentioned in our extension [13].

Right to be Forgotten (Number 2 of Article)

Right to be forgotten is also a major issue, as there is no efficient way to locate all the data spread between IoT devices and the information learned by third parties. If a person wishes for their information to be deleted from use, all the related third parties with which the information has been shared must be deleted. Therefore there needs to be an efficient way to locate a person's data for it to be removed and this can be difficult with big data [13]. Though it is possible, it is difficult to confirm whether all of a person's data has been deleted. This concept that total erasure is not completely assured should also be clearly explained in the IoT policies. Our proposed extension covers the idea of right to be forgotten as well and how the consumer will need to be provided this information.

Accessible Data for IoT Users (Number 3 of Article)

A big issue that we found with data storage on IoT systems is that data is not always stored in a central database, it can also be stored across multiple IoT devices. This can either mean that devices all have copies of the same piece of data concerning a user, or each device has fragments of data that collectively represents the user. As a result of data being scattered, it becomes difficult to ensure the GDPR's rights such as the right to access and the right to erasure. It should be guaranteed that despite whatever method that companies decide on to store user data, the user should not face any trouble with having complete control over their data. Our article guarantees the transparency of the used of their data in this manner.

Micromanagement by Consumer (Number 4 of Article)

In our proposed policy extension, we say that IoT devices should not have to be micromanaged by the user to provide an ample amount of privacy protection. We clearly state this in our extension with the example of turning off the IoT device so that it is not collecting data. Since IoT devices are always collecting data, whether it be something they hear such as "Hey Google" or video recordings from the

Ring doorbell, they should not need to be constantly at the control of the user to guarantee that they have enough privacy protection. It is up to the developer to make sure that this IoT device has enough privacy implementation in place so that the user does not need to constantly worry about their lives being recorded in a private area such as a home. At the same time, if the user wishes to micromanage the device, there should be ways to allow for this as well. It should not be requirement by the user.

Logs for Consumers (Number 5 of Article)

Logging possible interactions with the data and providing them to the consumer will better protect their privacy as they will have more knowledge to decide the privacy implications of the IoT device. The logs provided to the consumer will include where the data was used, why the data was used, if the data was exported to a third party, and if the producer of the product made money off the consumers data. Our goal with this requirement in the extension is for more transparency between IoT products and the consumer. The consumer will be able to have more control and awareness about what their data is used for. This in addition will lead the consumer to better understand exactly what information about them is collected as well providing a better understanding for the consumer.

Fines (Number 6 of Article)

One major issue with the GDPR is the economic impact it has on their business [15]. Many smaller businesses are negatively affected by strict privacy regulations and are subjected to many fines. In regards to IoT, the fines should be based on the size and profitability of the company, rather than an explicit fine to deal with the problem, especially since IoT devices collect large amounts of personal data. Companies should report the total number of users as well as the potential cost of a data breach so that an appropriate fine can be determined. The main objective of putting this in our article is so that smaller companies making IoT devices are not essentially shut down because they can not deal with the fines. Large companies such as Google have been notorious for invading people's privacy yet the fines they get barely affect their business because of how much money they make.

Iot Privacy Label (Number 7 of Article)

The contents of the Iot privacy label will include all the critical information about the privacy and security of the device. Some of these include: A privacy rating and a security rating for the device from an independent privacy assessment organization, type of data that is being collected, type of sensor on the device, whether or not the device is getting cryptographically signed and critical automatic security updates, and the frequency of data sharing. This information on the IoT privacy label would give consumers more information about privacy implications while using an IoT device [14]. This is a critical part of our policy so that consumers can quickly gain knowledge about the privacy implications of the IoT device. When they purchase the device and look at this label, they will immediately be able to determine the amount of privacy they have while using the device.

The below is our final product of an article we propose should be in the GDPR

Art. 92a GDPR

Specific IoT (Internet of Things) standards to be followed

1. IoT producers are required to give informed consent to the user. They will be required to explain the difference between broad consent and informed consent. This will be done by providing links and other reading sources so that people can learn more about possible privacy implications regarding IoT devices. Withdrawing consent does not differentiate between the right to hold data, or the right to use data must be clearly explained to the consumer.

2. Right to be forgotten may not be completely possible when using IoT devices if the data is outsourced to different companies. Can delete data if asked, but no guarantee that the user's data will be 100 percent off related databases.
3. IoT producers are required to ensure that the user can have full control over their data. This should be ensured despite the company's methodologies of how to store their user's data, whether it is centralized or scattered.
4. IoT devices should not have to be micromanaged by the user to provide an ample amount of privacy protection. However there should be manual options for the consumer if they do wish to micromanage their Iot device. Micromanagement is defined as the constant obligation of the user to be concerned for their privacy while using the device. For example, constantly turning off IoT devices should not be the job of the consumer but rather the producer when not in use.
5. IoT devices should provide users with logs on how/where their data was used, why the data was used, if the data was exported to a third party, and if the company made any money off using the data.
6. Fines and penalties should be determined appropriately. Companies should report the total amount of users as well as the potential cost of a data breach. This information should be used to calculate fines and penalties for lack of GDPR compliance, rather than a standard set of fines and penalties for all companies, regardless of size.
7. IoT privacy label
    (a) An IoT label is required with every commercially available device that can connect to the internet. The label should contain all pertinent information regarding privacy and security risks
    (b) Label must include type of data that is being collected, type of sensor on the device, whether or not the device is getting cryptographically signed and critical automatic security updates, and frequency of data sharing
    (c) The label should contain a privacy rating, given out by a third-party organization that reviews all IoT products. A higher rating will indicate sufficient privacy protections for consumers, while a lower rating indicates insufficient privacy protections.

The above is our final product of an article we propose should be in the GDPR

Challenges:

While working on this project, there were many obstacles that we had to deal with. The initial problem was how to evaluate the GDPR and CCPA. Since both documents are long and packed with a lot of information, it is difficult to evaluate the flaws immediately. It took us quite some time to find sources and understand the GDPR and CCPA before we could make a policy that grants consumers more IoT privacy. After finally understanding the flaws in both these primary documents, we needed to figure out a way to solve the problem of IoT privacy regulation not being strong enough in current legislation. We determined the key flaws from the GDPR and had each point on our article address a different flaw. We also used some related works such as the IoT label to further create more privacy rights for the consumer. We finally had to choose whether to create our own policy, or supplement existing policies. We decided that instead of creating our own policy, which would end up being extremely redundant to the GDPR because a lot of the same ideas would be used, we decided to instead create a policy extension to the GDPR. We choose to extend the GDPR over the CCPA because the GDPR has a bigger scope since it involves all companies affiliated with Europe, rather than only California for the CCPA. Also the GDPR has stricter privacy regulations compared to the CCPA and it would be more influential to extend the GDPR rather than the CCPA. After creating the draft, we needed to make it more specific to give clarity on the privacy objectives when IoT devices are in use. Overall, after creating this policy after doing thorough research on IoT devices and the two big policies CCPA and GDPR, we created an article that would definitely strengthen the privacy of IoT users and lead to a more privately connected world.

References

[1] "What is GDPR, the EU's new data protection law?," GDPR.eu, 13-Feb-2019. [Online]. Available: https://gdpr.eu/what-is-gdpr/. [Accessed: 15-Dec-2020].

[2] A. Botsi, "Legal Aspects: The GDPR & IoT," in The European Watch on Cybersecurity & Privacy, 2020.

[3] D. Bastos, F. Giubilo, M. Shackleton, and F. El-Mousa, "GDPR Privacy Implications for the Internet of Things", 4th Annual IoT Security Foundation Conference, London, rep.

[4] "Right to rectification," ICO. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/. [Accessed: 15-Dec-2020].

[5] X. Harding, "Google Home Records Far More Than Users Realize, Report Says," Fortune, 11-Jul-2019. [Online]. Available: https://fortune.com/2019/07/11/google-home-listening-recording/. [Accessed: 15-Dec-2020].

[6] "Data portability under the GDPR: the right to data portability explained," *i*, 10-Jun-2020. [Online]. Available: https://www.i-scoop.eu/gdpr/right-to-data-portability/. [Accessed: 15-Dec-2020].

[7] Westbase.io, "GDPR and IoT: The Implications and Considerations," Westbase Technology | Better Connected, 22-May-2018. [Online]. Available: https://www.westbase.io/gdpr-and-iot-implications/. [Accessed: 15-Dec-2020].

[8] A. Marini, A. Kateifides, and J. Bates, "Comparing Privacy Laws: GDPR v. CCPA," 2020. [Online]. Available: https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf. [Accessed: 2020].

[9] "Bill Text," Bill Text - SB-327 Information privacy: connected devices. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327. [Accessed: 15-Dec-2020].

[10] Gross, Grant. "Potential Impact of Two IoT Security and Privacy Laws on Tech Industry." HPE, Hewlett Packard Enterprise Development LP, 19 Dec. 2018, www.hpe.com/us/en/insights/articles/potential-impact-of-two-iot-security-and-privacy-laws-on-tech-industry-1812.html.

[11] J. H. Ziegeldorf, O. Garcia Morchon, and K. Wehrle." Privacy in the Internet of Things: threats and challenges." Security and Communication Networks 7.12 (2014): 2728-2742 https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.795

[12] **S**B-327 Information privacy: connected devices https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327

[13] E. Politou, "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions," *Validate User*, 26-Mar-2018. [Online]. Available: https://academic.oup.com/cybersecurity/article/4/1/tyy001/4954056. [Accessed: 10-Nov-2020].

[14] P. Emami-Naeini and Y. Agarwal, "Ask the Experts: What Should Be on an IoT Privacy and Security Label?," *Ask the Experts: What Should Be on an IoT Privacy and Security Label? - IEEE Conference Publication*, 18-May-2020. [Online]. Available: https://ieeexplore.ieee.org/document/9152770. [Accessed: 10-Nov-2020].

[15] S. L. Rausch, "Privacy and Security: Current Challenges and Best Practices," *Security Magazine RSS*, 08-Jul-2019. [Online]. Available: https://www.securitymagazine.com/articles/90455-privacy-and-security-current-challenges-and-best-practices. [Accessed: 20-Nov-2020].