ABCs and IoT:
Understanding the Impact of IoT Devices on Vulnerable Children

By Emma Rogers

Presented to the University of Arizona Honors College

Thesis
in
The School
of
Government and Public Policy

College of Social and Behavioral Sciences

Bachelor of Arts in Political Science and Law Degree
Graduating with Honors in Political Science

May 2022

Advisor: Anne Boustead

ABCs and IoT:
Understanding the Impact of IoT Devices on Vulnerable Children

Abstract

The growing reliance on the internet has led to children being introduced to IoT devices and technology at an earlier age. The internet is always growing and with that comes more dangers to be cautious of. This research paper aims to determine what policies need to be in place to help protect children's interests while still respecting familial privacy. This research paper will look specifically into the added dangers that affect vulnerable children such as LGBTQ+ youth and abused children.

Research was conducted to determine the various IoT devices that children and adolescents are exposed to along with their corresponding vulnerabilities and dangers. Research showed that there is not enough privacy protection for children's online data and the current protections in place do not account for the vulnerable children population. Through this research, policy recommendations were made that would safeguard children from online commercial interests and parental monitoring.

Table of Contents

I. Introduction

The increased use of IoT devices within the home has added a new dimension to family relationships and dynamics. IoT devices have helped families stay connected and stay safe. However, there is always the possibility that someone that will find a way to abuse technology

and use it to harm. In a family, the parents are usually the ones who sets up these "smart home" devices and has access to all the data they collect. Children living in an abusive household now can be monitored by their abusers 24/7 through use of IoT devices. Policymakers need to update the laws that are in place to protect children from abusive households so that they are in line with the rapidly growing technological world.

Policymakers need to address the issues surrounding children's privacy in regard to the growing digital world. While several laws protect children's privacy from commercial threats, there are no laws that protect children from threats within the household. Most current privacy laws give the power to the parents to decide how their children's data is collected and used. These protections may backfire if the parent has negative intentions. Policymakers must address the gaps in policy that are needed to protect children from external threats and internal threats within the home.

In this paper, I discuss what policymakers on the state and federal level should do to safeguard the privacy of children and adolescents in the context of IoT devices and data within the household and outside. I will go over the many different types of IoT devices that children and adolescents are exposed to and review their security vulnerabilities. Through this research, I will look into the best policy recommendations that can help protect the children and adolescents from parental abuse relating to IoT devices. Additionally, I will specifically investigate the best way to protect the vulnerable children such as LGBTQ+ youth and abused children. I will compare and contrast different policies across the country and across developed nations.

II. IoT devices and Familial Monitoring

IoT devices are an aspect of day-to-day life, especially for younger generations. As IoT devices have immersed themselves into all aspects of life, it is virtually impossible to prevent

exposure of children and adolescents to these devices. In addition, there are a number of applications and IoT devices that are specifically designed to monitor children both inside and outside of the home. In this section, I review some IoT devices and apps that are frequently used for purposes of familial monitoring.

A. Life 360

Life 360 – one of the very first tracking apps – came out for Android devices in 2008. The developers of Life 360 describe it as "the #1 family safety membership" and advertise themselves as an app that grows with the family and their needs (Life 360 Homepage). The app is subscription based with three different paid tiers, and a free option with a couple features. The price ranges from $4.99 for the silver plan to $19.99 for the platinum plan (Plans & Pricing). The more expensive plan features have much more than an average tracking app would have. The silver and platinum plan includes roadside assistance, free towing, emergency dispatch, digital safety features, and other emergency services. All of the plans have features such as location history, crash detection, SOS help alerts, and driving reports (Plans & Pricing). These features become more complex the more you pay but are the foundation of the app and its creation.

At its onset, the app was primarily targeted to families as a way to ensure their children's safety. Life 360's website claims that they have over 35 million users within the United States. That means at least a third of American households uses the family tracking app (Hasinoff). The creator intended it to help ease parent's minds while their children are in public spaces. The concept of Life 360 came from Hurricane Katrina – a natural disaster which separated a lot of families with no way to communicate or know if they were safe (About Life360). This concept may have been created with good intentions, but it also creates opportunities for parents to

invade their children's' privacy. Many features that the app proudly promotes can be detrimental to developing children and adolescents, specifically those living in an abusive environment.

The CEO of Life360 has worked hard within the recent years to find ways to provide children whose families use the app with some forms of privacy. The CEO, Chris Hulls, has created accounts on different social media platforms to connect with the younger generation who have been subjected to the app. He uses these accounts to ask for feedback on ways to improve abuse done with the app (Hulls). Life 360 introduced the bubble feature. Life 360 bubbles allow for a "bubble" radius to be set so that an exact location is not available. The bubble can be set for up to six hours and can be as large as 25 miles (Perez). The creator of the bubble can also choose to pop the bubble before the time is up. As long as the child stays within the bubble radius, only their approximate location will be shared (Perez). Additionally, no location history will be saved as long as they do not go outside of the set radius. The one exception is if Life 360 detects a crash, the bubble automatically bursts. Life 360 boasts the bubble feature as a way for children to get a little extra privacy while still being able to ensure safety. However, anyone in the Life 360 circle can "burst" a bubble at any time. The bubble creator will be notified that the bubble has burst (Hurtado). This feature is only supposed to be used for emergencies, but it does have the potential to contribute to the cycle of parental abuse that is already happening with the app.

B. Smart Cars

Life 360 does not just stop with the application. For years, the CEO, Chris Hulls, has discussed ways to integrate his technology into other IoT devices, specifically the connected car. Back in 2014, BMW became a strategic investor in Life 360 and released statements about how they were planning on integrating it into their design (Connected Car). A couple years back, other car brands such as Ford added Life360 into one of their newer models. The connected car

goes far beyond Life 360. Most new cars produced today can be considered “connected.” In fact, the increase of IoT devices and software within automobiles has provided for a lot of additional safety features that are very attractive to parents of new drivers. There is technology that can report back to the owner of the car if the driver was going too fast, if they were wearing a seatbelt, and where they car is going/went, among many other things (Connected Car). Cars are now mobile computers and have many safety features.

Similar to Life360, these features can have many benefits under typical circumstances. It is normal for parents to be concerned about the new drivers in the family and these features can help ease their minds. The Connected Car has a lot of safety features that work for the children’s safety as they navigate a new skill, driving, without taking it too far like Life 360 does. The Connected Car targets safety issues that are easily correctable like not wearing a seatbelt or driving too fast. Neither of these features have the ability to easily track the driver of the car.

C. Wearables

Both the connected car and Life 360 are ways that parents can keep track of their children while outside of the home. To take it a step further, there are also wearable devices that parents can give to their children, which allow further tracking of their persons. One of the most popular wearables is the Apple Watch, a wearable device that is used for many different services but can track and collect data as well. People use Apple Watches to increase their gym productivity through their fitness and step counting feature. Apple Watches can also come in handy when multitasking since it can send your texts to the watch in real time. The Apple Watch has a lot of great features. Likewise, parents are getting Apple watches and other wearable devices for their children at earlier ages (Apple Extends the Apple Watch Experience to the Entire Family). These wearable devices can be used by parents as a way to always track their children and where

they are (Simpson). In addition, the Apple watch will connect data on the children and send it back to the parents. Apple watches can collect fitness data and health data, among many other things. Within the last year, Apple made it possible for Apple Watches to be set up to someone else's phone such as a parent. As reflected in Apple's marketing material for this feature, this means that a child can have an Apple Watch without having an iPhone and that it can all be tracked back to the parent's phone. This can be done through the "Family Setup" (Apple Extends the Apple Watch Experience to the Entire Family). There are many potentially useful features to the Apple Watch with its new family setup. Parents and guardians can track where their child is located, children can contact 911 or emergency services without having their own iPhone, and they can stay connected to the family.

Another product recently released by Apple was the AirTag. The AirTag is similar to the Tile Tracker which was invented a decade ago (Mayberry). Apple added many features to the idea of a personal item track that make it easier to use by users of other Apple products. The "Find My" app has a friend's section, a devices section, and now an items section where you can add the items you put your AirTag on. The Find My app will help direct you to the AirTag location by using sound and arrows directing you to the correct spot. It shows you how far away you are from the item and will notify you when you leave it somewhere (Mayberry). In theory, the AirTag is a useful way for people to keep track of their different items. However, it also makes it easy for individuals to covertly follow another person, which is a particular concern in the context of intimate partner violence (Carpenter). Parents on the internet have shown ways to sew and hide the AirTags into shoes and clothing items in order to track their children in a way that cannot be easily identified and removed like an Apple Watch (Peterson).

AirTags are small enough to fit into areas that could be hard to locate and find. Since the release, there have been many reports where people find AirTags that do not belong to them on their person, somewhere in their car, or in their belongings. Stalkers and abusers have used the AirTag to constantly surveil their victims (Carpenter). Apple created a feature that alerts your phone if an unknown AirTag is following you and will show you the route that the AirTag took with you (Mayberry). This helps you figure out where the AirTag could have been put in your possession and gives you instructions on how to disable it. However, Apple has had difficulties implementing this feature. Many people post that they have tried to follow the instructions to disable it, but you need to find the AirTag in order to do that and attempts to disable it almost always comes up with an error message regardless (Peterson).

D. Smart Home Devices

Within the home, surveillance devices such as the Google Home or Amazon Alexa collect data about everyone who lives or visits there (Chung). Devices such as the Google Home and Amazon Alexa are Intelligent Virtual Assistants (IVA) that are powered by Artificial Intelligence (AI) and have been around for several years now. IVAs are becoming more and more common within households since they came out in Fall of 2014 (Levy and Schneier). They connect to many different devices in the home such as a Nest Thermostat and smart lights to create a "smart home." Many people have them in every room in the house and use them for speakers, alarms, and smart home automation (Levy and Schneier). Both Alexa and the Google Home are meant to connect the entire house. They both allow third party entities to continue to add new features to the devices such as ordering a pizza or calling an Uber. These features are easily used, and children can have access to the internet well before they are supposed to.

All internet devices within the home create a risk. For example, Amazon Alexa's are vulnerable to hacks and if they are in the children's rooms, the hackers can get information about activities within the children's room (Eliot). Google Home and Amazon Alexa are not the only smart home devices that collect information from children and pose a great risk (Chung). The Ring Camera was invented back in 2012 as a smart doorbell and the company has grown exponentially since then. As of 2020, 16% of all homes in the United States have a video doorbell (Doorbell Cameras in the U.S. – Statistics & Facts, 2021). Ring Cameras began as increased security at the front door. Their flagship product was the ring doorbell camera and was one of the first IoT doorbell cameras ever. It had two-way communication ability, high-def cameras, and could connect back to someone's smartphone. It has a motion sensor and begins to record when there is movement or when someone logs onto the app on the smartphone. Ring also came out with a subscription service which allows for videos to be stored (Doorbell Cameras in the U.S. – Statistics & Facts, 2021). Without a subscription service, the videos can only be viewed in real time. Ring has expanded into home security and parents use them as an extra camera in their home and in their children's rooms.

Many parents have been using ring cameras and similar security devices as a way to monitor their younger children's movement. Baby monitoring has been around for a while and became much more popular following the kidnapping of the Lindenberg Baby in 1932 (Catlin). This first type was an audio monitor that used radio technology to ensure a baby's safety. In 1974, intercom technology was integrated into baby monitors and enabled two-way communication. In the 1990s, the first ever video baby monitoring devices were introduced with them becoming much more popular in the early 2000s. Since 2015, smart baby monitors have

become the norm with many households using things such as the Nanit Pro, Miku Pro, and the Ring Camera (Nelson).

Connecting anything to the internet poses a risk of getting hacked. Since the rise of IoT devices, there have been many reports of Ring cameras and Amazon Alexas within a child's bedroom being hacked by an outside source (Eliot). This raises the scary possibility that the parent is not the only one able to view video of their children. The ease of access to inside the home cameras allows for additional surveillance passed the age of the typical baby monitor use.

II. Familial Privacy and Child Development

A. Privacy is Important for Child Development

From a cultural perspective, familial privacy is very important in the United States, and it is widely believed that the government should have minimal say on what goes on behind closed doors. Parents should be able to decide what type of media their young children are exposed to and how to raise them (Diekema). Parental monitoring can be important to improve safety and ensure guidance. However, privacy is also imperative to a child's development. As they get older, children are supposed to gain more privacy which allows them to learn and grow in society (Parke and Sawin). If every decision in an adolescent's life is being made by their parents, then they will never learn how to manage their own life once they go out into the world. This will affect their ability to develop an independent life of their own, and they may continue to rely on their parents for everything. Children and adolescents should have some expectation of privacy that increases as they move through their teenage years (Parke and Sawin).

Privacy needs change as children age. In order to develop into a functioning independent member of society, it is important that children are given some sort of privacy as they are growing. There is a link between privacy and trust (Witmer). Parents and guardians who give more privacy to their children are more likely to be honest and open about what is going on with their life (Witmer). Parents need to find a balance between supervising their children and allowing the privacy needed for child development. Privacy helps build independence and self-confidence (Witmer) and enables children and adolescents to gain new ways of thinking, new hobbies, and new social interests.

Privacy is particularly important for the development of LGBT children, especially in homes where they are not being uplifted and supported. LGBT kids face an entirely different set of challenges and often do not have strong parental support. LGBT kids living in a household that is strongly against the LGBT community will have to hide a huge part of their life and identity. Since they do not have many trusted adults to learn about their sexuality, they often turn to the internet to meet people in similar situations and learn (Online Communities and LGBTQ+ Youth). In fact, 50% of LGBTQ+ youth have at least one close internet friend compared to just 19% of non-LGBTQ+ youth (Online Communities and LGBTQ+ Youth). These online communities help LGBTQ+ youth that do not have a strong support system or a loving home environment.

B. Developmental Damage from Loss of Privacy

IoT devices threaten the privacy of youth by exposing their sensitive information to their guardians or the individual who purchased the IoT surveillance devices. Having a fully surveilled home forces youth to lie and find work arounds to get their own privacy (Hasinoff). Children and adolescents need their own privacy, and most will find a way regardless of the parent's wishes.

Children and adolescents who were given more privacy while they were growing up, normally have closer relationships with their parents as they get older (Parke and Sawin). Ring cameras within bedrooms are becoming common and may make sense when a baby monitor is needed and when they are a toddler. After a certain age, surveilling a child's every move is detrimental to their development and to their trust (Suttie).

LGBTQ+ youth are particularly vulnerable to in-home surveillance, especially in households where they are not accepted for who they are. If LGBTQ+ kids do not feel comfortable telling their parents or guardians about their sexual orientation, there most likely is information about it on their phone or laptop that could expose them if found (Gutierrez). LGBTQ+ youth do not have access to the same resources that heterosexual youth have in terms of their changing bodies, sex life, and other coming of age information. LGBTQ+ youth are much more likely to utilize their phones are the internet to ask questions about their health. 81% of LGBTQ+ youth searched about health information on the internet, opposed to 46% of non-LGBTQ+ youth (Gutierrez). LGBTQ+ health is not taught in the majority of schools. Non-LGBTQ+ youth are taught about their puberty and health as early as elementary school. For this reason, LGBTQ+ youth's phones are particularly vulnerable to surveillance since there is a lot of information on their phones that would expose them to their parents (Gutierrez). Data privacy is crucial to the LGBTQ+ community.

C. Privacy and Abuse

Child abuse is a huge issue in the United States, with at least 700,000 children being abused each year. At least 1 out of 7 children have been abused within the last year, and there were 1,750 deaths resulted from child abuse and neglect in 2020 (Fast Facts: Preventing Child Abuse & Neglect). There are many different types of abuse that may take place within in the

home, including physical abuse, emotional abuse, sexual abuse, and neglect. (Fast Facts: Preventing Child Abuse & Neglect). Child abuse is most prevalent in young children, with 2.7% of children being abused in some shape or form within their first year of life. Forty-six percent of all deaths that resulted from child abuse were for infants under the age of one. Additionally, two-thirds of all child abuse cases involve some type of sexual abuse. Seventy-eight percent of all child abuse is done by a parent (National Child Maltreatment Statistics). Child abuse and neglect is a huge problem in the United States and is only being exacerbated by the rise of monitoring and tracking devices.

Monitoring has become a major role in continuing abuse (Levy and Schneier). A child no longer has a safe place they can go to fully escape their parent's abuse. If a teen is required to have their phone tracked no matter where they are, this can lead to dangerous habits. It is better for a teenager to have a phone on them and be able to call for emergency help if needed. Many adolescents who are tracked unwillingly often leave their phones in certain places so they can go other places without being tracked. This places them in a more dangerous situation than they would have been in if they were not being constantly tracked. Children and adolescents will lie to their parents and find ways to go against their wishes regardless (The Learning Network). The increase in tracking within family relationships encourages the children to become sneaky and to find ways around being monitored.

Some degree of familial privacy is an important part of the free world. Many people agree that the government should not be involved in a family's day to day practices and decisions (Meyer). Parents should be able to decide how they raise their children and with what values. However, familial privacy does help perpetuate and cover up abuse. Child abuse can be covered up by the home-schooling system (Homeschooling & Child Abuse). Kids who are

homeschooled are not regularly seen by other adults and often are isolated from peers. Isolation is an important risk factor for child abuse and neglect. While most homeschooling families find ways to socialize their children, there are instances which cause the familial privacy issue to have many layers.

III. Methods

In this paper, I will be investigating how policymakers can address the issues with IoT devices and familial privacy. I will be looking into the different ways that parents and guardians use IoT devices in inappropriate or abusive ways, and whether existing laws help prevent that from occurring. I will be using case studies to undertake this investigation.

Because privacy laws vary across states and countries, I will be looking into the different privacy approaches taken by the different jurisdictions. I will be focusing on privacy laws that have been enacted by the US federal government, California, the European Union (EU), and the United Kingdom (UK). I will begin with US federal law because they apply across the entire country, including California residents. I chose California because they have long been involved in experimenting with privacy laws. Additionally, California has the largest population in the United States at over 39 million and has the largest state economy in the United States. If California were a sovereign nation, they would have the 5th largest economy in the world.

I will also be looking at the privacy laws in the EU and the UK. The UK and EU laws are very similar since the UK was a part of the EU until January 2020. Following Brexit, the UK implemented their own form of the GDPR which accounted for the demographic and geographic change. The United Kingdom has a population of over 69 million people. Following Brexit, the European Union population is about 447 million people.

For each jurisdiction, I will look at how their policy making would protect children across three dimensions: provide privacy for child development, prevention of child abuse, and privacy for LGBT kids. I decided to explore these specific dimensions because I want to find possible policy interventions for more vulnerable populations. There is a very thin line between beneficial familial privacy and a level of privacy that enables abuse.

IV. Results section

A. Federal Approach

The United States has several laws that deal with children's privacy on the internet. The main one is the Children's Online Privacy Protection Act, often referred to as COPPA. The act was initially passed in 2000s and was revised in 2013 to account for the world's growing reliance on the internet (Children's Privacy). COPPA's main focus is to require sites to request parental consent before collecting data or using any personal information of children under the age of thirteen (Children's Privacy). COPPA was passed to account for the large increase in online marketing to children. COPPA outright ban certain types of data collection, it but there are others for which it only requires parental consent (Children's Online Privacy Protection Rule ('COPPA')).

The policy rationale behind COPPA is that the parent is the regulator and protector of their child's data. COPPA applies to any online services or commercial websites directed to those who are 13 and younger. There are multiple things that an operator of a commercial website must do in order to comply with COPPA. Operators must have a clear online privacy policy that describes in-depth their practices regarding the collection of children's data. In addition, the operator must have a way to obtain verifiable parental consent and have a direct

disclosure for the parents regarding the practices. There also needs to be a way to give parents the choice of consenting to the online practices but prohibits the operator from disclosing any of that information to any third party involved. COPPA also requires that parents have access to their child's information and can review it to decide if it needs to be deleted or not. There also needs to be an option for parents to prevent any further collection of their child's data and information by an operator. Additionally, if parents do consent to the data collection practices then the operator must ensure the confidentiality, security, and integrity of the information. All children's information collected can only be retained for as long as it is relevant and necessary. Finally, a child's participation in an online activity cannot ask for any more information than is necessary for the participation (Children's Online Privacy Protection Rule ('COPPA')).

COPPA defines personal information as any type of identifying information. The rule includes protection for information such as first and last names, home or physical addresses that include the street name and name of the town, any type of online contact information, screen or usernames, telephone numbers, social security numbers, and photos, videos, or files that contains a child's image or voice (Children's Online Privacy Protection Rule ('COPPA')). In addition, the rule protects personal information that can be used as a persistent identifier to recognize a user over time across many different websites. COPPA requires all operators of commercial websites and online services that are directed to children under 13 to follow these guidelines (Children's Privacy). This also applies to operators of mobile apps and IoT devices.

COPPA defines a child as anyone 13 years of age or younger. This is meant to differentiate between adolescents and young children who need extra protection from the dangers of the internet (Children's Online Privacy Protection Rule ('COPPA')). However, teenagers between 13 and 18 years of age can often be at great risk of using the internet safely due to the

independence gained during that time. Children above the age of 13 are allowed to create accounts on different social media accounts according to the different platform's guidelines. Despite still being a minor and still developing, they are given the ability to fully immerse themselves into the digital world. COPPA assumes that only children under the age of 13 are vulnerable to the dangers of the internet when that is not the case. In fact, there has been recent legislation introduced that would change the COPPA age to anyone under the age of 18 (Lerman). This would be a beneficial step to protecting minors' privacy and not just children under 13. Most social media platform's terms of service state that the minimum age required to create an account is 13. Increasing the COPPA age will help protect minors as they start to utilize the internet more.

The United States has a number of consumer data privacy laws, but there is not an all-encompassing comprehensive act like the EU's GDPR. In addition to the Children's Online Privacy Protection Act (COPPA), there is the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Electronic Communications Privacy Act (ECPA), the Video Privacy Protection Act (VPPA), and the Federal Trade Commission Act which prohibits unfair and deceptive advertising practices. On the state level, only three states have signed comprehensive data protection acts: California (CCPA and CPRA), Colorado (ColoPA), and Virginia (VCDPA) (Klosowski).

All of the data privacy protections outlined in COPPA are there to protect children from commercial surveillance. COPPA requires that the owner/regulator of the children's data is their parent or guardian (Children's Online Privacy Protection Rule ('COPPA')). This allows for parents to ensure that their child is being safe on the internet. If a child does get access to the

internet, COPPA protects their data and allows for parents to get information collected by operators of commercial websites to be removed.

The COPPA commercial surveillance protections can have positive impacts on children's development. Despite the copious number of lessons that are taught in school regarding internet safety, children can often disregard them and engage in dangerous activities online. COPPA requires that commercial website operators give the parents the option to review any data that has been collected and allow them to have it deleted. This can benefit children because they have some room for error in terms of learning how to use the internet without it being detrimental.

COPPA gives the power to the parent to be the regulator and protector. This is beneficial in most familial relationships, but the needs of vulnerable children should also be considered when laws are put into place. The interests of abused and LGBT children may conflict with the behavior of their parents. If an abused or LGBT child is not safe in their home, they might turn to the internet to feel less alone.

COPPA makes parental surveillance and control easier since it gives parents the ability to be the regulator of their children's information. COPPA does not discuss the individual protections of the children separately from their parents. Since COPPA gives the parents the ability to regulate the data how they see fit, it is easier for parents to be in control of their children and to continue surveillance at a greater scope. Online data can share a lot about an individual and someone else having access to your own data increases vulnerabilities. Parents who are already excessively surveilling their children can look into a whole new dimension with their children's data.

COPPA does not have much impact on parental surveillance as a whole because the United States values familial privacy. The United States was built on freedom as a fundamental

right. Ensuring that parents can make their own decisions about their children without the government intervening is important to a lot of the population. For this reason, COPPA does not have much impact on child development in that aspect. However, it does impact child development but not discussing parental surveillance as it is harming vulnerable youth.

By allowing parents to be the commercial internet gatekeepers, abused, LGBT kids and other vulnerable children, were not thoughtfully considered when COPPA was developed. COPPA has many benefits that add protection to children's information on the internet and help supplement a caring parent's efforts. However, COPPA does not consider the children under thirteen who are either abused or living in a bad situation. LGBT kids whose family does not support them are going to turn to the internet to learn more about themselves and communicate with likeminded individuals. This means that LGBT youth are more vulnerable to the dangers of the internet because they will likely try to be secretive. Abusive parents can use secrecy as a way to take more power from their already vulnerable child.

B. California's approach

California is often at the forefront of adopting new laws and regulations. By passing the California Consumer Privacy Act (CCPA), California became one of three states that have their own state level comprehensive data protection act. This act gives the consumer more ownership of the data that gets collected on them (California Consumer Privacy Act (CCPA)). California consumers have the right to know what data is and has been collected about them, have the right to have most data collected on them deleted, and the right to opt out of the sale of their personal data. In addition, California has a separate law that is specific to the privacy and security of IoT devices (California IOT Security Law Cheat Sheet).

In 2018, California became the first state in the nation to pass an IoT security law that required all connected devices in California to have reasonable security measures designed to protect the user's privacy (California IOT Security Law Cheat Sheet). The reasoning behind the legislation was to protect smart home device users from unauthorized access to the information that the IoT devices collect. The law went into effect on January 1st, 2020, and covers "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address" (Sysman). This definition is very broad and includes everything from Smart TVs, computers, Apple watches, and Smart Home devices. As technology becomes more advanced, the list of connected devices will only become longer.

California's IoT Security Law describes reasonable security measures as features that are "appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure" (Sysman). The law's description of reasonable measures is incredibly vague and could cause confusion on the manufacturer's end. The manufacturers could be violating the law without truly knowing. Some people have criticized the law being as being overly broad, as this could hurt businesses and hinder innovation (Hübschmann). The law does not specify the penalties for noncompliance and does not state what the maximum penalty officials can seek. In addition, the law does not allow for private entities to sue under California law and enforcement is delegated to the California Attorney General, city attorneys, county counsels, and district attorneys (California IOT Security Law Cheat Sheet).

This legislation does not include any IoT security and privacy protections specific to children. However, California has previously passed numerous laws that specifically address children's safety and privacy while online. In 2013, the Privacy Rights for California Minors in the Digital World was passed. The law prohibits online companies from marketing products that are not supposed to be used by anyone under 18 to minors. It also prohibits companies from collecting data on minors to be used for the marketing of these same products (Bill Text SB-568). There is also the "right to be forgotten" clause which states that California residents under the age of 18 have the ability to have any information collected on them online permanently deleted. This law is often referred to as the California eraser button law (Bill Text SB-568).

In 2015, the Student Online Personal Information Protection Act was passed. This law prohibits online service companies who contract with K-12 schools and students from sharing any information that was gathered (Legal Overview: Key Laws Relevant to the Protection of Student Data). This includes simple identification such as name, birth date, and student identification numbers, along with online behavioral data and activity. In addition to these basic protections, educational service companies are not allowed to use their platform to advertise or target students for any purpose other than the actual educational service (Legal Overview: Key Laws Relevant to The Protection of Student Data).

The Student Online Personal Information Protection Act. also known as the SOPIPA, has many loopholes for online companies to work around. For example, Google is not allowed to use their educational programs to collect information and target students on programs such as Google Classroom. However, the SOPIPA does not block Google from collecting information on students when they navigate outside of the educational programs and go onto the internet. Students who are logged in and use Google to search for outside websites are having behavioral

data collected on them used for various purposes including advertisement (Legal Overview: Key Laws Relevant to The Protection of Student Data).

The California Constitution requires that parents are able to opt their children out of classroom technology and requires the school to provide an equal alternative (Legal Overview: Key Laws Relevant to The Protection of Student Data). California wants to ensure that students have equal access to education while still allowing parents to protect the privacy of their children. California guarantees that all students in the state have equal access to education and that was solidified in the 1992 case, *Butt v. California*. In April of 1971, Contra Costa County announced that they would be shutting down the schools 6 weeks earlier than usual and parents of students in the country sued the state. The parents claimed that California is required to ensure that each student in the state receives an equal education and ending the school year that much earlier would be detrimental to the success of the students (Legal Overview: Key Laws Relevant to The Protection Of Student Data). This case solidified that California is responsible for educating every student equally, explaining the need to find alternatives for children whose parents do not want them using technology.

Most laws regarding IoT privacy and security in California are in place to help protect the consumer from commercial surveillance. They help limit the amount of information that large companies are able to keep on consumers and prohibit a lot of data collection on people under the age of 18. These laws are vague but make it harder to conduct commercial surveillance on both adults and children. The IoT security laws require all IoT device manufacturers to take reasonable measures that are designed to protect the user's privacy. This means that the manufacturers must take additional steps in order to follow the guidelines of the California law and it makes it harder for commercial surveillance in general.

Most of the policies relating to IoT device privacy and security address the issues with commercial surveillance but fail to address the ongoing issue of parental surveillance and control. In fact, some of these policies actually could make it easier for parents to control their children. Parents in California can decide whether or not their child uses classroom technology. This means that their child would not have the easiest access to learning about other views and experiences in the world. In addition, parents have the power to completely erase their child's digital footprint which could be erasing a part of their identity. This is especially harmful to the LGBT youth whose identity is strongly linked to their online persona.

While parents should be able to decide what their child can do within reason, prohibiting their child using technology will hinder their success and keep them consistently behind their peers. Abusive parents can keep them from using technology until the age of 18 which would be detrimental to the rest of their lives (Pisanu). With how quickly the world is becoming more and more digitized, children who do not get firsthand classroom experience with technology are going to be at a disadvantage to their peers. Technology is being used as early as preschool and children are taught how to use the internet safely throughout all of elementary school. If children are barred from learning the dangers of technology early on, they are at high risk for issues later on when they inevitably have to use the internet (Jacobs). There is a delicate balance between holding back a child's development and ensuring that parents have a right to knowing and deciding what type of technology their children are introduced to.

Abuse is often found and reported through the school systems. Parents can homeschool their children if they are against the substitutions that are given for the classroom technology (Legal Overview: Key Laws Relevant to The Protection Of Student Data). This could increase parental control/surveillance since the abused child would no longer have an escape at school

(Coleman). In addition, the eraser law allows for parents to completely scrub the internet of any information regarding their child. In households that are not supportive of the LGBT+ children, sometimes their online presence is the only time they can actually be themselves. If parents can choose whether they want to scrub the internet of their child's digital footprint, that is erasing their identity. This is especially significant for LGBT+ kids, but also important for kids in abusive households. Many kids living in a tough environment look to the internet to connect with others who are also going through similar abusive situations. While there is not a lot of policies that are in place to protect the vulnerable youth population, the privacy and security laws relating around commercial surveillance actually make it easier for the abuse to continue.

C. European approach

The European Union (EU) currently has one of the toughest privacy and security law. The General Data Protection Regulation (GDPR) was introduced in the European Parliament in 2016 and went into effect for the entirety of the EU in 2018 (What Is GDPR, the EU's New Data Protection Law?). While the GDPR was passed in the EU, it applies to any organization that targets and collects data on European Union citizens around the world. The GDPR has harsh fines in the millions of euros and penalties for those who do not comply with it (What Is GDPR, the EU's New Data Protection Law?). The regulation is very far reaching and large, which can be daunting to smaller organizations with limited resources.

There are many different sections of the GDPR. Article 5.1-5.2 discusses the protection and accountability principles for anyone that processes data. These seven principles are lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability (What Is GDPR, the EU's New Data Protection Law?). Accountability is a huge part of the GDPR because the data controllers have to

show that they are GDPR compliant. If there is no way to show compliance, they are not GDPR compliant. Companies are also required to implement "appropriate technical and organizational measures." This means that the companies need some type of technical measure whether that is end-to-end encryption or two-factor authentication (GDPR Official Legal Text). The organizational measures can include more staff training, limiting access to personal data, or adding more data privacy policies to the employee handbook. Article 25 of the GDPR emphasizes that data protection must be by design and by default (Official Legal Text). The organizations need to ensure that they are ensuring data protection in the design of any new product, activity, or service.

The GDPR also has sections that discuss children's data and parental consent, often referred to as the GDPR-K (GDPR-K: Children's Data and Parental Consent under the GDPR). The GDPR-K is often compared to the Children's Online Privacy Protection Act (COPPA) in the United States. GDPR-K has very similar requires to COPPA and emphasizes parental consent and transparency. Article 8 of the GDPR governs the process of obtaining consent for children and the validity of their consent (GDPR-K: Children's Data and Parental Consent under the GDPR). One major difference between the GDPR-K and COPPA is the age of who is considered a child. Under COPPA, a child is considered anyone under the age of thirteen while the GDPR-K applies to anyone under the age of sixteen. The GDPR-K does give leeway to the member states to decide whether they want to lower the age of consent to thirteen; however, the age cannot be lowered past thirteen. In terms of consent from a child, it is only valid when there is also consent from a parent or guardian (GDPR-K: Children's Data and Parental Consent under the GDPR). In fact, Article 8.2 requires that there is a reasonable effort to verify parental consent when it comes to the processing of child data (Official Legal Text). The GDPR-K has one exception for parental

consent, and it is if there is therapy or counseling offered directly to the child. There are six countries that have kept sixteen as the age of consent and those include Germany, Hungary, Lithuania, Luxembourg, Slovakia, and The Netherlands (GDPR-K: Children's Data and Parental Consent under the GDPR).

The GDPR was not the first time the European Union considered data privacy protections. The EU has emphasized the right to privacy in lots of different legislations that have been created since the European Convention on Human Rights in 1950, which states that "everyone has the right to respect for his private and family life, his home and correspondence" (What Is GDPR, the EU's New Data Protection Law?). Throughout the years following this, the EU emphasized the right to privacy. This carried over when the internet was invented, and technology progressed. The EU recognized the world's increasing reliance on the internet in the early 1990s and introduced the European Data Protection Directive in 1995 (What Is GDPR, the EU's New Data Protection Law?). The European Data Protection Directive established very minimal data privacy and security standards, but it was enough for the member states to base their own policies around it. The internet kept expanding and by 2011 the need for more data privacy protection expanded greatly. They began to work on a better approach to personal data protection and started to update the European Data Protection Directive.

The GDPR not only applies to European Union member states but also applies to anyone who processes personal data of EU citizens. Article 3 of the GDPR explains that the "regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (Official Legal Text). This means that a company in the United States that sells something or offers a service to EU citizens must be GDPR compliant. In addition, if a

company/organization can track cookies and IP addresses in the EU, they need to be compliant (What Is GDPR, the EU's New Data Protection Law?). There are a few exceptions to this as it does not apply to "purely personal or household activity." The GDPR applies to organizations who are engaging in "professional or commercial activity." This means that regular household communication is not subjected to GDPR compliance. The other exception is for smaller businesses and organizations that have fewer than 250 employees (What Is GDPR, the EU's New Data Protection Law?). The GDPR does not completely exempt these businesses from being compliant, but it frees them from some of the strict record-keeping requirements.

A major part of the GDPR is the substantial fines that imposed on businesses, big or small, that are noncompliant. All GDPR fines under Article 83 apply to all types of businesses but they are flexible and scale with the size of the firm (What Are the GDPR Fines?). The GDPR also lays out which type of fines carry a more severe penalty. The less severe infringements which include any violation governing controllers and processors, certification bodies, and monitoring bodies, have fines up to £10 million or 2% of the annual revenue, whichever one is higher. The more severe infringements include anything that goes against the basic principles of the GDPR such as its right to privacy and its right to be forgotten. These infringements carry much higher penalties with the fines being up to £20 million or 4% of the annual revenue, whichever one is higher. The more severe penalties come from violations governing Article 5, 6, 7, 9 12-22, and 44-49 (What Are the GDPR Fines?).

The penalties for the GDPR have a wide range of fines that can be imposed. These fines are regulated by the data protection regulator in each member state in the EU. These regulators use different criteria to determine whether a fine is needed and what the number of fines will be (What Are the GDPR Fines?). There are 10 different criteria in place to determine the fines that

apply to a violation of the GDPR, including the gravity and nature of the infringement, the intention, whether there was any attempt to mitigate the damage, any precautionary measures already in place and compliant, any prior infringements of the GDPR, how cooperative the firm is, what type of personal data is affected, whether the firm notified anyone regarding the breach, whether their prior codes of conduct had been certified, and any other aggravating or mitigating factors. It is important to note that regardless of how many violations the organization has, they will only penalize the most severe one (What Are the GDPR Fines?). These large fines are in place so that there is a huge cost to companies that are not GDPR compliant.

The United Kingdom (UK) has a privacy and security law also called the General Data Protection Regulation (GDPR). The EU and UK GDPR are very similar in many ways, as the UK followed the EU GDPR until Brexit in 2020 (Data Protection and Brexit). For this reason, a lot of the policies are the same with just some domestic changes to account for no longer being a part of the European Union. Companies in the UK who also process data in the European Union must be compliant with the UK post Brexit GDPR as well as the EU GDPR.

The GDPR-K section is very similar to COPPA in the ways it protects children from commercial surveillance. It makes it harder for commercial surveillance on children because it gives parents the power to intervene with this surveillance, similar to COPPA. Despite the GDPR setting the age of consent online as sixteen, The GDPR-K allows for each member state to change the age to be higher than thirteen. This benefits more children and adolescents by keeping their protection from commercial surveillance until a later age.

Protecting children from commercial surveillance will inevitably have a positive impact on child development. The consent and transparency needed from parents as described in the

GDPR-K helps protect children's data as they grow up. This ensures that children have someone else making their internet-based decisions so that it does not impact them later in life.

The abused and LGBT children population have different vulnerabilities that result in politics having a greater impact on them. Parents having the ability to consent and control their children's data makes the average child safer. However, children who are being abused or living in a household that does not support their sexuality may have interests that conflict with their parent's interests. Parents who are not looking out for their child's best interest can create a dangerous internet experience for them.

The GDPR-K does make it easier for parental surveillance since it gives the parents the right to be in charge of their children's internet usage. Parents get to decide what to consent to and what sites that the child can be going onto so this increases their surveillance to include online. The GDPR-K does not explicitly give parents the right to absolute surveillance, but it does allow for them to be in control of their child's internet usage. This allows for the parents to consent to what sites they are allowed to use, if any at all. If children do not get exposed to the internet in a safe manner, they will not be on the same developmental level as their peers (Walch and Sabey).

Vulnerable children are at a greater risk with the GDPR-K and the parental rights from it being abused. Parents can determine what they consent to on the internet and if LGBT kids are trying to learn more about their sexuality, the parents will find out. The GDPR-K does not discuss the way the policy affects vulnerable children.

V. Discussion Section

A. Overview of Key Points

Legal protections seem to be focused on protecting children from commercial surveillance by giving power to parents. As is summarized in Table 1 below, each jurisdiction discussed has their own policies and acts that lay out the different protections from commercial surveillance for children.

Table 1: Review of Legal Protections for Children

	Federal	California	EU/UK
Child Development	COPPA is largely about protecting children from commercial interests. COPPA gives parents the ability to regulate internet usage and data collection. This can make an impact on vulnerable children and their development when parents are neglectful.	California's Constitution stating that parents can opt their children out of classroom technology usage can hinder development in the digital world Children will feel left out from their peers if their parents opt them out and this could cause some social developmental delays If children are barred from learning how to use the internet and technology, when they turn 18, they will not know how to safely navigate Preventing your child from being able to participate in classroom activities can lead them to be a target for	The GDPR is similar to COPPA and protects children from commercial interests. This helps protect the average child's data from being monetized without parental consent.

		bullying which will also prevent development.	
Abused Children	COPPA gives parents the role as "regulator" when it comes to their children's data. Children living in abusive homes cannot freely use the internet without worry about their parents abusing them based on the sites they visit. Abused children do not have parents who are looking out for their best interest so giving the abuser the ability to regulate their child's internet usage can help perpetuate abuse.	Parents who do not approve of the equal alternative to classroom technology can pull their child out of the public school system and homeschool them. A lot of child abuse is discovered and reported on through the school system Children who are living in abusive households often find school and online channels as a safe space. Restricting access to their peers and to the internet can help perpetuate abuse	The GDPR does not explicitly. give parents the right to their children's data like COPPA does. The GDPR does not have any protections that would help abused children from having data access by their parents/abusers.
LGBTQ+ Children	COPPA does not take into account the different types of households that these children reside in. Many parents in the US do not support their child being LGBT and can use the information granted through COPPA negatively.	The Eraser Button law gives parents the ability to completely delete their children's online identity. LGBT children living in unsafe households often have a different persona online where they can truly be themselves. The parents have the ability to completely scrub their child's true identity. Allowing for parents to control what sites their children have access to gives parents the ability to prevent LGBT kids from interacting with other LGBT kids online.	LGBTQ + youth are also more vulnerable in terms of their online data. The GDPR does not have anything explicit that would help LGBTQ+ youth from abusive households.

In the United States, the Children's Online Privacy Protection Act ensures that no company can obtain data from those under thirteen without a verifiable way to get consent from their parent or guardian (California IOT Security Law Cheat Sheet). This helps protect children who are at vulnerable ages from being deceived by unfair online data practices without fully understanding what they entail. COPPA ensures that parents have control and the final say about what data can be collected on their child and how that data can be used. This is a great way for parents to be able to ensure their child is being safe and protected while on the internet. Children, especially under the age of 13, have underdeveloped brains and cannot consent to internet practices that they do not understand. By allowing the parents or guardians to take control, children can learn how to safely use the internet without the risk of losing their privacy and data.

The GDPR is the European Union's version of COPPA, and they share many similarities. However, they were written with different focuses in mind. The GDPR focuses on data protections for all citizens while COPPA focuses on children's data protections. The EU does not have their own independent law that focuses only on children's data, but it does get addressed in the GDPR-K. The GDPR outlines the collection, use, and disclosure of data as it relates to all citizens. It also outlines the additionally needed protections when it comes to children's data. COPPA is much narrower in focus and is specific to unfair data practices with children's online data. At the end of the day, both COPPA and the GDPR-K are basic children's online data protections and do not go far enough to combat the rapidly growing internet.

California is one of the few states that have moved beyond COPPA and increased legal protections for children's privacy. There are no laws specifically regarding children and IoT device privacy and security. However, the Privacy Rights for Minors in a Digital World Act goes

beyond COPPA and ensures that those under the legal age have additional protections. This act was passed in 2013 before IoT devices were fully on the market and helps to prohibit marketing of items that are not supposed to be used by anyone under the age of 18 to minors (California IOT Security Law Cheat Sheet). Additionally, this act also has the right to be forgotten clause which is often referred to as the eraser button law. This is beneficial because it allows for parents to decide what can be on the internet and what needs to be deleted if it is data from their child. Another California act in place to help protect minor's data is the Student Online Personal Information Protection Act. This act accounts for the rapidly increasing use of the internet and technology in the classroom. Children spend more than half of their waking hours at school away from their parents and need the same protections there.

However, these practices can put vulnerable children at more risk. Children living in abusive or unsafe households do not have the luxury of their parent always looking out for their best interest. COPPA, and the other similar acts, only work when the parent has good intentions when being the regulator of their child's data. Many children are living in households where they need to be protected from their parent or guardian and these policies do not address that. LGBTQ+ youth also face additional vulnerabilities because their online data can tell a lot about their hidden sexuality, especially if their parents are strongly against the LGBTQ+ community. California's eraser button law gives parents to delete their children's online persona. This is especially harmful for LGBTQ+ youth because the internet could be the only place that they feel like they can truly be themselves and connect with others.

As children's lives become more and more digitalized, data protection needs to continue to improve as it shapes their development. Both the GDPR-K and COPPA are basic children's online data protection policies that do not go in depth but are a great place to start. It is

important to acknowledge that there is a necessity to adapt strong protections for children's online data because they are being raised with the internet. Children are exposed to the internet at an early age and online data is collected on them from an early age. Parents being able to regulate how their children use the internet will allow for them to learn safe online habits. It is also necessary for parents to know what is being collected on their child because they are responsible for them until they turn 18. These data protection laws give parents that ability which is great. Under California's Student Online Personal Information Protection Act, children have another level of online protection while at school. Children spend over half of their day at school surrounded by technology. Smart technology is continuing to completely change education in the United States and SOPIPA protects children by preventing the companies from using the collected data to their benefit. The protection while at school helps the children who do not have anyone looking out for their best interest while at home

Until a certain age, children's brains are not fully developed and need the guidance and support from their parents or guardians. Because of this, parental surveillance to some extent is beneficial and can positively impact child development. As children get older, their expectation of privacy grows, and parents need to accept the change for them to learn as an independent functioning member of society. Having some degree of separation from their parents is important especially throughout the teenage years. There is no legislation that accounts for the need for privacy from their parents during the late teenage years. Parents are given the ability to decide what they think is appropriate or not appropriate for their child to partake in until they turn 18. However, most parents are looking out for their children's best interest and do want to ensure that they are learning how to be a functioning adult.

All of these policies surrounding children's online data privacy do the bare minimum for protection from commercial interests. Protecting minor's data from being exploited by online website operators is beneficial for child development but that is only one side of it. Giving parents the ability to decide what children can be exposed to allows for some to fall behind developmentally. Children need to interact with their peers in order to keep up with them and parents are given the right to prevent their children from this. School is where most social development happens and children that are home schooled miss out on a huge part of growing up. Children with helicopter parents can also be painted as an outcast. If a parent is very strict about what their specific child does, the other kids might be worried that their own parents will hear about what they are doing as well- even if it is just normal teenage activity.

Additionally, many college students who do not have the normal teenage experiences while still living at home get into more dangerous situations in college. This is seen most in college when it comes to alcohol and drug exposures. College students who experimented with alcohol in a safer setting know how to handle the issues that come with drinking. Alcohol safety is important to learn about before heading off to college, even though college age students are not legally able to drink until 21. Parents who assume that their child will abstain from drinking until their 21st birthday are naïve and putting their child at a greater risk. Internet safety is also important to learn before turning 18. The world has become so reliant on the internet, and it is borderline inappropriate for parents to not allow their children to experience it while still being a minor. If children are not given access to learn the dangers, they will be prone to unsafe internet habits. Freedom and responsibility are needed in order for children to develop into functioning members of society. The policies in place do not address the negative impact on child development.

Additionally, these bad things can be worse when dealing with vulnerable children. For example, abused children can now never escape their abuser since they can be tracked 24/7. School used to be a haven for children coming from toxic households, but current laws allow for parents to home school with few regulations. Schools are one of the biggest places that abuse is discovered and reported so the increase in home schooling inevitably will increase abuse.

Also, LGBTQ+ children are at a greater risk of harm from these policies since they are already such a vulnerable population. LGBTQ+ children often feel ostracized in their own home and look to the outside for hope and strength. When parents are able to completely isolate their child from outside influence, LGBTQ+ youth lose out on an important part of their development.

B. Policy Recommendations for Arizona

Arizona should adopt a unified framework that expresses the restrictions behind the collection and use of children's data. The entire country is behind regarding online data protection, but Arizona does not have anything further than COPPA. While notice and consent are needed and necessary, there needs to be a system in place that goes beyond notifying the user with an excessively long document. There need to be policies by design that kick in that are there to protect vulnerable children from their parent's interests. Providing a 100-page document written in language only an expert in the field can understand is not sufficient for anyone. Arizona needs to make a user-friendly guide to explain where everyone's data is going, especially minors.

COPPA needs to expand further passed parental consent and address the issues surrounding vulnerable children's family situation. There needs to be a line drawn between whether parental surveillance is a safety issue versus the parent needing excess control over their child. The United States values familial privacy, but this allows for abused children to slip through the

cracks. COPPA needs to place limitations on how much parents can surveil their children because it is not safe for all children. Getting rid of a degree of familial privacy increases accountability for all.

Policies need to be enacted in Arizona that will specifically protect the most vulnerable children such as LGBTQ+ youth. The current policies in place are not even enough to protect the average child and their online data, especially in Arizona. LGBTQ+ youth have added vulnerabilities in terms of online privacy that need to be accounted for when policies are being created. LGBTQ+ youth's online browsing history most likely can expose their sexual orientation because the internet is a huge resource for them as they learn more about their selves and their sexual orientation. Data that is not kept private has the ability to put LGBTQ+ youth in real danger if they do not have a supportive family and home life. Arizona needs a taskforce in place to determine the best method for protecting LGBTQ+ youth from online dangers since they are the most vulnerable. There needs to be an option for children's data protection that does not include giving unlimited access to the parent or guardian. The government should monitor data breaches and should regularly audit the website operators to ensure compliance. Policies need to be in place to protect LGBTQ+ online data because if an unsupportive parent finds out, they could become abusive.

Abused children are also at a greater risk and they must be considered when new legislation is introduced. Arizona needs to address the issues with home schooling and covering up abuse. Arizona needs a specific committee to regulate home schooled children which should include weekly welfare checks and progress reports. Additionally, Arizona should keep a data base of all parents or guardians who have been accused of child abuse and not allow them access to their child's data. There should be a court appointed regulator of the child's data since the parent is

not fit to regulate it. Arizona should research the dangers of tracking children and if they find it necessary, they should place regulations on it.

V. Conclusion

The current laws regarding online data privacy are in place to protect children from being commercialized and gives all the power to the parent or guardian. This includes restrictions on what data can be collected on them, from sites like Club Penguin and Webkinz. The current laws in place are there to prevent the monetization of children. Allowing parents to decide what works for their family is okay when the parents have their children's best interest at heart. However, these laws can make things worse for the vulnerable children, making them even more vulnerable.

LGBTQ+ youth and abused children are in a unique position because what works for the masses will not work for them. The government should have the authority and ability to enact legislation that would take away some parental rights because total parental rights is dangerous to the vulnerable children.

There are no laws set up to handle this issue and in order for there to be a whole new dimension of privacy has to be introduced. Laws need to be created with the most vulnerable population in mind since they are the ones that get affected by them the most, even if they are the minority. The current protections are not even enough for the general population but are actually harming the abused and LGBT children who are living in toxic households.

Works Cited

Parke, R. D., & Sawin, D. B. (1979). Children's Privacy in the Home: Developmental, Ecological, and Child-Rearing Determinants. Environment and Behavior, 11(1), 87–104. https://doi.org/10.1177/0013916579111004

Chung, Hyunji et al. "Alexa, Can I Trust You?." *Computer* vol. 50,9 (2017): 100-104. doi:10.1109/MC.2017.3571053

Hasinoff, Amy Adele. "Where Are You? Location Tracking and the Promise of Child Safety." Television & New Media, vol. 18, no. 6, Sept. 2017, pp. 496–512, doi:10.1177/1527476416680450.

Levy, Karen and Schneier, Bruce, Privacy Threats in Intimate Relationships (June 6, 2020). Journal of Cybersecurity 6: 1-13 (2020), Available at SSRN: https://ssrn.com/abstract=3620883

Brian Simpson. "Tracking children, constructing fear: GPS and the manufacture of family safety." Information & Communications Technology Law, 23:3, 273-285, DOI: 10.1080/13600834.2014.970377

"Apple Extends the Apple Watch Experience to the Entire Family." *Apple Newsroom*, Apple, 15 Sept. 2020, https://www.apple.com/newsroom/2020/09/apple-extends-the-apple-watch-experience-to-the-entire-family/.

"California IOT Security Law Cheat Sheet." *JD Supra*, 18 Dec. 2019, https://www.jdsupra.com/legalnews/california-iot-security-law-cheat-sheet-75568/.

"Children's Online Privacy Protection Rule ('COPPA')." *Federal Trade Commission*, 1 Dec. 2020, https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

"Children's Privacy." *EPIC*, https://epic.org/issues/data-protection/childrens-privacy/.

"Connected Car." *BMW*, BMW, 14 Dec. 2021, https://www.bmw.com/en/innovation/connected-car.html.

"FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule." *Federal Trade Commission*, 19 Dec. 2012, https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over-their-information-amending-childrens.

"GDPR-K: Children's Data and Parental Consent under the GDPR." *Clarip*, https://www.clarip.com/data-privacy/gdpr-child-consent/#:~:text=Contact%20us%20Today!-,GDPR%2DK%3A%20Children%27s%20Data%20and%20Parental%20Consent%20under%20the%20GDPR,and%20consequences%20of%20data%20sharing.

Gutierrez, Carlos. "Data Privacy Is Crucial for the LGBT Community." *Stay Safe Online*, 5 Feb. 2018, https://staysafeonline.org/blog/data-privacy-crucial-lgbt-community/.

"Hijacked Nest Devices Highlight the Insecurity of the IOT." *CSO Online*, CSO, 4 Feb. 2019, https://www.csoonline.com/article/3338136/hijacked-nest-devices-highlight-the-insecurity-of-the-iot.html.

Jodka, Sara H. "The Internet of Toys: Legal and Privacy Issues with Connected Toys: Insights." *Dickinson Wright*, Dec. 2017, https://www.dickinson-wright.com/news-alerts/legal-and-privacy-issues-with-connected-toys.

"Legal Overview: Key Laws Relevant To The Protection Of Student Data." *Electronic Frontier Foundation*, 14 Nov. 2017, https://www.eff.org/issues/student-privacy/legalanalysis.

Levy, Karen, and Bruce Schneier. "Privacy Threats in Intimate Relationships." *SSRN*, 1 July 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620883.

Mayberry, Travis, et al. "Who Tracks the Trackers?: Circumventing Apple's Anti-Tracking Alerts in the Find My Network ." *ACM Conferences*, 1 Nov. 2021, https://dl.acm.org/doi/abs/10.1145/3463676.3485616.

"GDPR Official Legal Text." *General Data Protection Regulation (GDPR)*, 2 Sept. 2019, https://gdpr-info.eu/.

"SB-327 Bill Text." *Bill Text - SB-327 Information Privacy: Connected Devices.*, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327.

Sysman, Dean. "Council Post: California's IOT Security Law: Why It Matters And The Meaning Of 'Reasonable Cybersecurity'." *Forbes*, Forbes Magazine, 20 Nov. 2019, https://www.forbes.com/sites/forbestechcouncil/2019/11/20/californias-iot-security-law-why-it-matters-and-the-meaning-of-reasonable-cybersecurity/?sh=ad326841e2d7.

"Tracking Children, Constructing Fear: GPS and the Manufacture of Family Safety." *Taylor & Francis*, https://www.tandfonline.com/doi/abs/10.1080/13600834.2014.970377.

"What Is GDPR, the EU's New Data Protection Law?" *GDPR.eu*, 13 Feb. 2019, https://gdpr.eu/what-is-gdpr/.

Witmer, Denise. "Why Teens Need Privacy From Their Parents." *Verywell Family*, Verywell Family, 27 Mar. 2022, https://www.verywellfamily.com/why-does-my-teen-need-privacy-2609615.

"National Child Maltreatment Statistics." *American SPCC*, 24 Feb. 2022, https://americanspcc.org/child-maltreatment-statistics/.

"Fast Facts: Preventing Child Abuse & Neglect." *Centers for Disease Control and Prevention*, Centers for Disease Control and Prevention, 6 Apr. 2022, https://www.cdc.gov/violenceprevention/childabuseandneglect/fastfact.html.

"California Consumer Privacy Act (CCPA)." *State of California - Department of Justice - Office of the Attorney General*, 28 Mar. 2022, https://oag.ca.gov/privacy/ccpa.

"Plans & Pricing." *Life360*, 24 Mar. 2022, https://www.life360.com/plans-pricing/.

Perez, Sarah. "Family-Tracking App Life360 Launches 'Bubbles,' a Location-Sharing Feature Inspired by Teens on Tiktok." *TechCrunch*, TechCrunch, 6 Dec. 2021

Hurtado, Kaitlin. "Teens Can Hide Exact Locations from Parents on Tracking App." *Parentology*, 23 Sept. 2021, https://parentology.com/life360-bubbles/.

Nelson, Margaret K. "Watching Children: Describing the Use of Baby Monitors on Epinions.Com." Journal of Family Issues, vol. 29, no. 4, Apr. 2008, pp. 516–538, doi:10.1177/0192513X07310319.

"Doorbell Cameras in the U.S. – Statistics & Facts, 2021." *SafeHome.org*, 1 Apr. 2022, https://www.safehome.org/doorbell-cameras/statistics/.

Catlin, Roger. "After the Tragic Lindbergh Kidnapping, Artist Isamu Noguchi Designed the First Baby Monitor." *Smithsonian Institution* , Smithsonian Institution, 20 Dec. 2016, https://www.smithsonianmag.com/smithsonian-institution/after-tragic-lindbergh-kidnapping-isamu-noguchi-designed-first-baby-monitor-180961454/.

Peterson, Mike. "The AirTag Stalking Problem Is Only Partially Apple's Problem, It's Mostly Law Enforcement's." *AppleInsider*, AppleInsider, 7 Jan. 2022, https://appleinsider.com/articles/21/12/31/the-airtag-stalking-problem-is-only-partially-apples-problem-its-mostly-law-enforcements.

Klosowski, Thorin. "The State of Consumer Data Privacy Laws in the US (and Why It Matters)." *The New York Times*, The New York Times, 6 Sept. 2021, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

"Data Protection and Brexit." *IT Governance*, https://www.itgovernance.co.uk/eu-gdpr-uk-dpa-2018-uk-gdpr.

"What Are the GDPR Fines?" *GDPR.eu*, 13 Feb. 2019, https://gdpr.eu/fines/.

"Bill Text SB-568." *Bill Text - SB-568 Privacy: Internet: Minors.*, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

Hulls, Chris. "Videos." TikTok, 2021, https://www.tiktok.com/@life360ceo.

Carpenter, Jacob. "Domestic Violence Advocates Worried Stalkers Would Use Apple's Airtags." *Fortune*, Fortune, 7 Apr. 2022, https://fortune.com/2022/04/07/apple-airtags-stalking-harassment-tracking/.

Eliot, Lance. "Alexa Shockingly Tells 10-Year-Old Girl to Put a Penny into an Electrical Socket, Which Provides Important Lessons for AI Self-Driving Cars." *Forbes*, Forbes Magazine, 30 Dec. 2021, https://www.forbes.com/sites/lanceeliot/2021/12/29/alexa-shockingly-tells-10-year-old-girl-to-put-a-penny-into-an-electrical-socket-which-provides-important-lessons-for-ai-self-driving-cars/?sh=372cdcb23f2c.

"Online Communities and LGBTQ+ Youth." *Human Rights Campaign*, https://www.hrc.org/resources/online-communities-and-lgbtq-youth.

"Homeschooling & Child Abuse." *Coalition for Responsible Home Education*, 25 Apr. 2022, https://responsiblehomeschooling.org/advocacy/policy/abuse-in-homeschooling-environments/.

Lerman, Rachel. "New Bill Would Update Decades-Old Law Governing Children's Privacy Online, Add Protection for Teens." *The Washington Post*, WP Company, 29 July 2021, https://www.washingtonpost.com/technology/2021/07/29/coppa-update-teenagers-online/.

Hübschmann, Ida. "What You Need to Know about the US and California IOT Security Laws." *Nabto*, 20 May 2021, https://www.nabto.com/us-and-california-iot-security-laws-guide/.

Jacobs, Hannah. "How and When to Limit Kids' Tech Use." *The New York Times*, The New York Times, https://www.nytimes.com/guides/smarterliving/family-technology.

Coleman, Rachel. "Why We Have to Talk about Homeschooling and Child Abuse." *Coalition for Responsible Home Education*, 23 Mar. 2021, https://responsiblehomeschooling.org/why-we-have-to-talk-about-homeschooling-and-child-abuse/.

Pisanu, Angela. "Lack of Technology in the Classroom Hinders Literacy and Work-Readiness." *Education Business UK*, 25 Apr. 2019, https://educationbusinessuk.net/news/25042019/lack-technology-classroom-hinders-literacy-and-work-readiness.

Diekema, Douglas S. "Parental Decision Making." *Parental Decision Making*, UW Department of Bioethics & Humanities, https://depts.washington.edu/bhdept/ethics-medicine/bioethics-topics/detail/72.

Suttie, Jill. "Life Stages of Trust." *Greater Good Magazine*, Berkeley, https://greatergood.berkeley.edu/article/item/life_stages_of_trust.

Walch, Ronde and Sabey, Alyssa (2020) "Parental Monitoring of Adolescent Social Media Use and Emotional Regulation," *Family Perspectives*: Vol. 1 : Iss. 1 , Article 12 https://scholarsarchive.byu.edu/familyperspectives/vol1/iss1/12

The Learning Network. "What Students Are Saying about Parental Surveillance, Living without Wi-Fi and Vibrant Youth." *The New York Times*, The New York Times, 20 Mar. 2020, https://www.nytimes.com/2020/03/19/learning/what-students-are-saying-about-parental-surveillance-living-without-wi-fi-and-vibrant-youth.html.

Meyer, David. "The Paradox of Family Privacy." 53 *Vanderbilt Law Review* 525, March 2000, https://scholarship.law.vanderbilt.edu/vlr/vol53/iss2/2