International Journal of Frontline Research in
Engineering and Technology
Journal homepage: https://frontlinejournals.com/ijfret/
ISSN: 2945-4840 (Online)

(REVIEW ARTICLE)

Check for updates

Privacy Challenges in IoT: Assessing Data Protection Risks and Strategies for Secure User Adoption

Mildred Adwubi Bonsu [1] and Jochebed Akoto Opoku [2,*]

[1] *University at Albany, State Univ. Of New York.*
[2] *Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Ghana.*

International Journal of Frontline Research in Engineering and Technology, 2025, 04(01), 009-016

Publication history: Received on 07 September 2025; revised on 22 October 2025; accepted on 25 October 2025

Article DOI: https://doi.org/10.56355/ijfret.2025.4.1.0027

Abstract

The integration of the Internet of Things (IoT) into everyday life from connected appliances, smart wearables, to smart city infrastructure, generates an influx of personal and behavioral data. Although these technologies have the potential to enable efficient, personalized and thriving economies, they in turn raise challenging privacy issues that threaten user trust and inhibit long-term adoption. In the United States, the rapid pace of IOT innovation has exceeded the development of standard privacy protections, leaving a disintegration of technical defenses, corporate practices, and regulatory guidance. Analysis indicates that numerous IoT products entering the U.S. market embed broad data collection capabilities into their core functionality, often operating in ways that exceed the scope disclosed to end users. Controls for restricting or limiting such data flows are often hidden within complex settings or completely absent, while software maintenance practices leave known vulnerabilities unaddressed for extended periods for low-cost devices. This environment is reinforced by an uneven regulatory landscape in which manufacturers are not faced with unified national requirements for privacy-by-design or security hardening. Hence, this paper critically examines analysis of these privacy issues by analyzing the regulatory gaps, technical deficiencies and user-facing constraints that are driving IoT proliferation in the United States. It also discusses ways in which secure user adoption can be encouraged, ranging from technical protections to regulatory reforms and consumer empowerment, to highlight the pathways through which IoT can achieve its transformative potential without sacrificing user confidence or fundamental rights.

Keywords: Internet Of Things (Iot); Privacy Challenges; Data Protection; User Trust; Secure Adoption

1 Introduction

Once a domain-specific concept, today Internet of Things (IoT) has become a unique characteristic of the U.S. digital fabric and now plays an important role in shaping how Americans interact with their surroundings, enabling businesses to provide services and improving the operation of public infrastructures. By 2023, the number of connected devices in the average U.S. home was more than 15, including everything from voice-activated personal assistants and wearable health monitoring devices to car security systems and energy usage apps [1]. The industry forecast of IoT suggests that more than thirty billion Internet of Things devices are expected to be in use worldwide by 2030, and the United States will become one of such largest national markets [2].

This expansion is being driven by advances in wireless communication, reducing sensor costs, and a rising interest in automation and data-driven personalization [3].

* Corresponding author: Jochebed Akoto Opoku

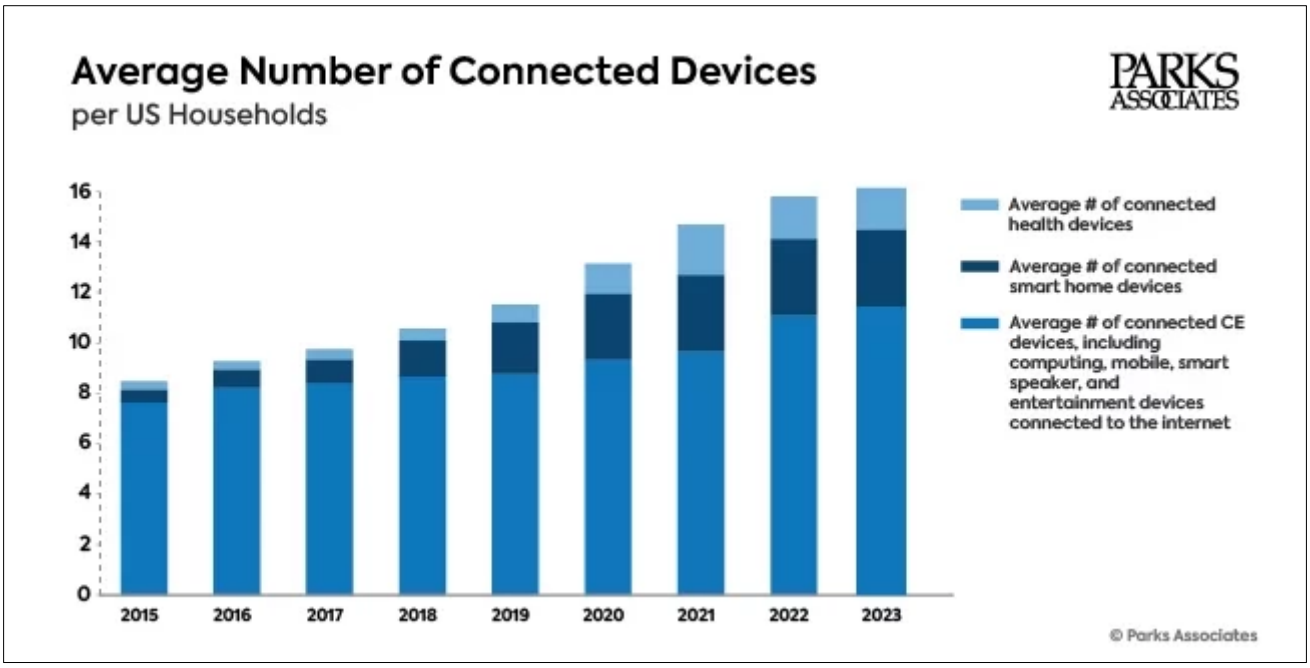

Figure 1 Parks Associates (2024) Parks Associates announces new research showing average number of connected devices per US internet household reached 17 in 2023

Nonetheless, the connective nature of innovation has also given way to unprecedented accessibility to personal and behavioral data about individuals. Internet of Things devices produce very precise data such as location history, biometric measures, and consumption habits that can be collected and fused together to create rich user profiles [4]. In the U.S., where this information isn't consistently governed by a single federal law, protections against this data varies widely based on state, sector and company policy. This fragmented regulatory environment and differing technical defenses across systems mean that practices like permanent background data harvest, obscure consent models, and a lack of regular security updates can thrive [5].

Privacy around personal data, in this scenario, is a principal part of the decision on the process and extent of IoT acceptance. Consumers are realizing that their personal information can be misused in all kinds of ways beyond the most obvious ones, like targeted advertising, unauthorized profiling, identity theft, and large-scale security breaches.

In this research, we examine the state of privacy and data protection threats within the IoT landscape in the U.S., based on reported vulnerabilities, along with regulatory case studies and market trends. The threat of silent data collection and cross-platform tracking looms ever larger, especially as IoT devices increasingly become an invisible part of daily life. The interplay of innovation with restraint is a critical challenge to decide and drive its growth and the current nature of interconnected living.

2 IOT Privacy Challenges in the U.S.

2.1 Personal and Behavioral Data in IoT

The U.S. consumer IoT devices can commonly generate streams of information that are much more detailed than the information that websites can capture with cookies or other tracking devices. Instead of just recognizing a device or browser, an IoT system can maintain a record of the location, lifestyle, and physical condition of an individual. An example would be a smartwatch that can monitor heart rate and sleep patterns, a smart speaker that can record voice commands and background conversation, and a smart thermostat that could record occupancy schedules each day [6]. Once this kind of unequal data stream is uploaded to the cloud of companies, it can be joined to a long-term behavioral impression of when a person is likely to go home, what a typical day looks like, or even sensitive health data. Most crucially, this massive data capture is not limited to gadgets that have a clear privacy concern, like cameras and microphones. An example of a connected vehicle integrates a sensor in the shape of infotainment stacks, which monitors the driving pattern, speed, and position, and transmits driving pattern, voice recognition, and address book to the car manufacturers and third parties. That is to say that not only the intensity with which a driver presses the brake pedal

matters, but also the type of music they play in their cars can become a part of an elaborate profile of behavior. Among all types of consumer devices, cars are the least privacy-friendly because almost all car manufacturers gather extremely personal information like sexual behaviors, facial expressions, genetic and health information, including sensitive geolocation and biometric information that can and frequently does end up being shared or sold with third parties like advertisers, insurance companies, or data brokers [7].

2.2 Technical vulnerabilities: background collection, weak crypto, poor updates

Although IoT devices are convenient, they also have endemic technical vulnerabilities that can compromise privacy and security of users. Most importantly, a large number of devices have default credentials, usernames, and passwords that are set by their manufacturer, and users may not necessarily change. Mirai botnet, which was notoriously active in 2016, used this vulnerability to attack more than 380,000 IoT devices (primarily routers, cameras, and DVRs) in a large-scale distributed denial-of-service (DDoS) attack [8]. In addition to authentication problems, the IoT products also lack strong update and patching systems. Another major incident occurred in early 2024 when Wyze reported that they had a configuration issue with their cloud service and that the camera feeds of several users had been revealed to other users, which illustrates the privacy implications of backend vulnerabilities, despite their systems not being breached [9]. Similarly, interface and data transmission weaknesses are very common. Telemetry or credentials on some consumer devices are still being sent either in plaintext or using outdated encryption formats that can be easily decrypted. These technical weaknesses are not theoretical threats but have led to regulatory action. The Federal Trade Commission (FTC) in 2023 reached a settlement with Amazon Ring because of the lack of simple access controls. Privacy was grossly infringed upon when internal employees with contractors were revealed to have accessed private user video feeds without consent. The settlement demanded reimbursements of more than 5.6 million and greater security measures, indicating that irresponsible device controls can cause severe privacy violations [10]. To mitigate possible dangers of such nature, the U.S. government has presented the Cyber Trust Mark, which is a voluntary program of labeling cybersecurity of IoT devices. It gives the opportunity to display a unique shield logo (including a QR code) on compliant products to indicate to consumers that they have passed the minimum levels of cybersecurity, including secure updates and encryption. It assists consumers in making better choices regarding the products they introduce into their households, distinguishes reliable products in the market, and generates incentives to manufacturers to ensure even greater standards in cybersecurity. Although this is promising, the label is presently voluntary, and most of the devices targeted by it are beyond its access [11].

3 Regulatory landscape and oversight gaps

3.1 Federal Trade Commission

The Federal Trade Commission (FTC) is the major federal agency in the United States, which policies on unfair or deceptive data-handling and data-security practices of private companies. The exercise of the FTC authority has taken the form of enforcement, guidance documents, and public reports in a way that demonstrates the systemic failure of the IoT privacy practices and ensures organizations engage in improved practices [12]. However, the effort of the FTC is limited in a number of ways. Firstly, its authority is required when there has been a specified finding of deception or an unfair practice under Section 5 of the FTC Act. The FTC lacks authority to impose a comprehensive privacy law since it has not been granted an explicit omnibus privacy statute by Congress. The FTC can only act under the power granted to it by Congress and cannot impose any broad privacy rules on its own, but can instead rely on case-by-case unfair or deceptive practices [13]. Additionally, FTC is a reactive agency and only investigates when violations are reported. It has no ability to actively oversee or control the fast-expanding IoT industry. Staffing is also one of its key limiting factors. By the end of 2025, the workforce size of the FTC would have reached approximately 1,100 total employees, the smallest level the agency has reached in a decade, and the portion of that workforce dedicated to privacy and digital security matters is only a subset [14].

This decrease was highlighted by FTC Commissioner who stated that *"50 percent more employees at the beginning of the Reagan administration than we do today,"* despite the digital markets growing at a tremendous scale [15]. These resource limitations significantly hinder the agency's expansion of enforcement to new areas, including IoT.

3.2 State-level laws Inconsistencies

Without a comprehensive federal privacy law, the states have been the most active experimental sites of consumer privacy legislation. The CCPA/CPRA of California is the most sophisticated in relation to consumer rights i.e. right to access, deletion, portability, and an opt-out to sale/sharing of personal data, fused with administrative regulations and enforcement agency [16]. The Consumer Data Protection Act in Virginia (VCDPA) was adopted in 2023 and is based on

a controller-focused approach, which contains data protection assessment requirements and prohibits sensitive data processing [17].

The problem of state-specific law differences is not limited to technical drafting issues. They are different in the applicability threshold, definition of sale/sharing, definition of sensitive data, timelines and right of action of the private. Therefore, the outcome of this is the emergence of a patchwork effect that puts a strain on national device vendors and cloud services platforms to enforce and provide unequal consumer protection [18].

Recent events are enhancing these disassociations. Some other states passed privacy laws with various requirements between 2023 and 2025 including opt-out vs opt-in regimes and alternative criteria defining sensitive categories, which business in a countrywide operation must address with the responsibility of managing compliance burdens and inconsistency in redress options to consumers based on their states of residence [19].

3.3 Lack of a comprehensive federal privacy law

It has also been identified in various policy reviews and legal analyses that in the United States, no single U.S. federal law on human rights provides the definition of personal data and the provision of baseline rights and obligations [13, 20]. Congressional and White House data protection initiatives have resulted in rival legislative projects. Negotiations around preemption, private rights of action, and scope don't appear to be making any progress. The consequence is that the producers of devices and operators of platforms have to grapple with a patchwork of state regulations and sectoral federal legislation such as HIPAA and COPPA as opposed to a single strong federal standard on consumer IoT privacy. Such a fragmentation of regulators adds to the uncertainty, increases transaction costs, and creates the opportunity of regulatory arbitrage [21].

3.4 Impact of Fragmented Governance on User Protection

This disconnected regulatory environment of the United States has significant effects on consumer welfare as applied to IoT. A significant impact is geographic variation in rights and remedies. Indicatively, under the California Consumer Privacy Act, California consumers can request access, deletion, and opt-out of their sales of personal information [16]. Conversely, a consumer in a state not with similar laws does not have an equivalent statutory recourse, even in cases of being confronted by the identical device behaviors, establishing unequal protection across borders [18].

Secondly, manufacturers have to deal with the complexity of operations. IoT vendors must negotiate divergent requirements in consent, minimization, and record-keeping of data that differ among the states. Due to this, companies will have to either conform to the strictest accepted standard, which is more expensive to comply with, or just adopt the least strict set of rules and leave a large number of consumers unprotected. This inconsistency, as per the legal and industry analysis, can delay the launch of products, constrain updates, or fragment services supplied by jurisdictions, hence hindering innovation and failing to provide consistent protections [14].

Disassociation also leads to enforcement gaps in addressing evolving threats. Although some states have initiated inquiries into data brokers and discriminatory pricing, others do not even have the means to take action. This puts unequal enforcement strain of data-sharing practices and leaves detrimental practices in areas with reduced jurisdiction [22].

Finally, this approach creates a blind spot to sector-specific harms. A variety of cross-cutting risks in IoT, such as geofence-derived tracking of visits to reproductive health care facilities in the aftermath of U.S. Supreme Court decision of Dobbs in 2022, which overturned Roe v. Wade and enabled states to restrict abortion rights, insurer-level algorithmic profiling on the basis of telematics data, or long-term behavior inference from device telemetry, are not equally addressed. Even though some states have responded with actions, including enacted laws that ban geofencing disclosures around reproductive-health facilities, efforts to tackle the issue have been sluggish and, in many cases, they present inter-jurisdictional conflicts [23]. The lack of a unified federal system has forced consumers and organizations to navigate around grey areas where rights and protections are more geographical than universal concepts of privacy and protection.

4 Impact on User Trust and Adoption

4.1 Relationship between privacy safeguards, user confidence and Market Behaviour

Privacy protection is one of the key factors that define the level of trust and the adoption of IoT. In the 2024 NIST IoT Advisory Board report, a lack of trust in privacy and cybersecurity was recognized as a significant obstacle to IoT

adoption in the U.S., with a large proportion of the respondents indicating that they would adopt more widely if IoT devices in case are more secure and transparent about the use of their data [24].

During a user-centric survey of 325 smart homes, it was found that security and privacy issues account for relatively 76.2% of the variation in whether individuals adopted or rejected IoT smart home devices.

Additionally, McKinsey in its research found that approximately 30% of the executives in business and consumer sectors who were surveyed consider cybersecurity as their concern, and 40% of them are willing to increase their spending on IoT by at least 25%, if IoT security risks were mitigated. This highlights that there is an inherent link between investment and adoption behavior and privacy protection [25].

Consumer adoption and market activity in the IoT Sector are shaped by the absence of uniform privacy protection throughout the U.S. Where safeguards vary across state borders or differ across regulating jurisdictions, there is a tendency to lose the confidence of consumers due to uncertainty as to whether their rights are being adequately protected. This ambiguity is a hindrance to adoption and has repercussions in the strategies where the vendors of IoT choose to bring products to market. Firms must incur the cost of competing compliance requirements, which may result in delayed updates or restrict functionality in some jurisdictions or encourage companies to adopt the lowest common denominator standard, leaving some consumers unprotected [24].

Overall, these observations indicate the disconnection between safeguards and confidence and the way it contributes to the distorted market behavior and inefficiency in IoT adoption. Instead of a unified trajectory, one can observe a much more disjointed pattern of market acceptance in the U.S. as a result, driven as much by regulatory geography as consumer demand or technological preparedness.

Future Directions for Secure User Adoption

For secure user adoption, a combination of technical and regulatory consistency and meaningful user empowerment is essential. In the absence of these pillars, even a well-designed system is likely to experience limited adoption because consumers remain wary of privacy breaches and security vulnerabilities, along with unclear governance structures.

4.2 Technical Safeguards

At its core, robust technical measures are indispensable to promote trust in connective ecosystems. Privacy-by-design is an approach that requires that security be embedded into the architecture of a system rather than being considered an addition. The IEEE (2025) highlights that privacy should be the default setting, ensuring that devices limit data gathering and provide end-to-end protection regardless of the user settings [26]. Data encryption during transit and rest also enhances resiliency, given that IoT devices are likely to be used over insecure networks.

Another important safeguard has to do with automatic updates, which are authenticated. According to Yang [27], insecure or irregular firmware updates provide platforms to highly vulnerable devices and pose long-term risks to both the consumer and service provider. Automation ensures that vulnerabilities will be patched in time, while cryptographic signatures prevent manipulation of updates by adversaries. These types of technical commitments demonstrate to the users that security is not a reactive process but a continuous process, which in its turn further reinforces confidence for increased adoption.

4.3 Regulatory Reforms

Disassociated governance, however, cannot be compensated for by technological design. With the lack of a unified privacy framework in the US currently, this leaves consumers with unequal protections depending on their jurisdiction and puts too much burden of compliance on vendors, which leads to legal uncertainty and prevents immediate product deployments. To ensure that all aspects of data protection achieve uniformity in rights, duties, and application, analysts propose a federal minimum law to establish uniformity in the protection of data at the national level [13]. This would not only protect consumers but also develop a consistent legal framework would make compliance easier in situations where the manufacturer would serve multiple markets.

Federal harmonization of standards is also an intermediate measure in the face of absence of federal action. As observed by Reuters [14], efforts to align state privacy legislation including standardizing definitions of sensitive information, and consent procedures can reduce regulatory friction and ambiguity. Reduced divergences and harmonized rules establish clearer expectancies which gives users clear and predictable expectations and gives the market an indication that protection are real and enforceable.

4.4 User Empowerment

Finally, sustainable adoption depends on the empowerment of users to make informed decisions. Research has shown that the privacy settings need to be noticeable and editable to make the users more likely to embrace the technologies of IoT. Deceptive consent flows and confusion erode trust and deter adoption. Based on guidance is provided that usability and trust can be enhanced by proposing intuitive controls, including plain-language privacy dashboards [28] .

In addition to user interface design, awareness campaigns also matter a lot to educate users on the consequences of connected devices. The work of the Electronic Privacy Information Center (EPIC) proves that with the help of specialized outreaches, it can educate stakeholders about data rights and security practices. The project of the EPIC Health Privacy and Equity aims to educate the public about the gathering and utilization of health information, focusing on disadvantaged communities, and informing citizens about their rights to control their data [29]. Customers are more willing to accept IoT when they believe that they possess the knowledge and tools to manage their data.

5 Conclusion

This study reveals the benefits expected of IoT, that is, high efficiency, convenience, and greater connectivity, which are inextricable from privacy threats triggered by the massive collection and extensive interconnections on a global scale. Without coherent and reliable safeguards, consumer trust diminishes, adoption slows, and the very possibility of IoT as a driver of innovation is undermined.

What becomes evident in this analysis is that none of the technical, regulatory, or societal factors can individually bring about a reliable introduction of the IoT. With privacy-by-design principles, encryption by default, and automatic patching, these are only as good as harmonized, enforceable, and forward-looking policy frameworks. Similarly, legislation and policy can only be effective if they are put into actual practice that will confer authority to users in making decisions on how their data is being used. Trust cannot be achieved with a compliance checklist; trust is developed with transparency, consistency, and meaningful user agency.

Hence, technical safeguards are required to be incorporated as a default, and regulatory frameworks must seal the prevailing patchwork of protections. Empowerment of users should also ensure that people are not just subjects whom data is gathered on but participants in the digital ecosystem. It is a balance that must be achieved through long-term cooperation between policymakers, the industry, civil society and consumers themselves. Provided these mutually reinforcing efforts are undertaken with focus and consistency, a future IoT can be the place where innovation thrives but not at the expense of privacy, but rather in alignment with it.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Parks Associates (2024) Parks: Average U.S. Internet Home Had 17 Connected Devices in 2023, 10 January. Available at: https://www.parksassociates.com/blogs/in-the-news/parks-average-us-internet-home-had-17-connected-devices-in-2023

[2] Jinesh (2025). How Many IoT Devices Are There in 2025? [All You Need To Know], 4 June. Available at: https://autobitslabs.com/how-many-iot-devices-are-there/

[3] Kumar, N. (2025) Internet of Things (IoT) statistics: Market and growth data, 5 July. Available at: https://www.demandsage.com/internet-of-things-statistics/

[4] Moustati, Imane and Gherabi, Noreddine and El Massari, Hakim and Saadi, Mostafa. (2023). From The Internet of Things (IoT) to The Internet of Behaviors (IoB) for Data Analysis. 634-639. 10.1109/CiSt56084.2023.10409989.

[5] DLA Piper (2025) United States privacy law: A patchwork of federal, state, and sector-specific protections. [online] Available at: https://www.dlapiperdataprotection.com

[6] Bugeja, J., Jacobsson, A., and Davidsson, P. (2016, August). On privacy and security challenges in smart connected homes. In 2016 European intelligence and security informatics conference (EISIC) (pp. 172-175). IEEE.

[7] Prevost, S., and Kettani, H. (2019, October). On data privacy in modern personal vehicles. In Proceedings of the 4th International Conference on Big Data and Internet of Things (pp. 1-4).

[8] Eustis, A. G. (2019, May). The Mirai Botnet and the importance of IoT device security. In 16th International Conference on Information Technology-New Generations (ITNG 2019) (pp. 85-89). Cham: Springer International Publishing.

[9] Abuhussein, A., Alsubaei, F., Shiva, S., and Sheldon, F. T. (2016, June). Evaluating security and privacy in cloud services. In 2016 IEEE 40th annual computer software and applications conference (COMPSAC) (Vol. 1, pp. 683-686). IEEE.

[10] Agnihotri, A., and Bhattacharya, S. (2021). Ring: The New Amazon Subsidiary and the Social, Privacy, and Security Issues It Generates. SAGE Publications: SAGE Business Cases Originals.

[11] Caven, P., Gurjar, A., Zhang, Z., Ma, X., and Camp, L. (2025, April). Usability, Efficacy, and Acceptability of the US Cyber Trust Mark. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (pp. 1-35).

[12] Davis, I. M. (2019). Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads. Emory LJ, 69, 781.

[13] Kerry, C.F., Morris, J.B. Jr., Chin, C.T. and Turner Lee, N.E. (2020) Bridging the gaps: A path forward to federal privacy legislation. Available at: https://www.brookings.edu/wp-content/uploads/2020/06/Bridging-the-gaps_a-path-forward-to-federal-privacy-legislation.pdf

[14] Reuters (2025) 'US FTC chair seeks to trim agency by around 10%', Reuters, 15 May. Available at: https://www.reuters.com/business/world-at-work/us-ftc-chair-seeks-trim-agency-by-around-10-2025-05-15/

[15] U.S. House Committee on Appropriations (2024) FTC Budget Hearing [FY2024], transcript. Available at: https://www.govinfo.gov/content/pkg/CHRG-118hhrg54689/html/CHRG-118hhrg54689.htm

[16] Bonta, R. (2024) California Consumer Privacy Act (CCPA). Updated 13 March. Available at: https://cdn.lawreportgroup.com/acuris/files/Cybersecurity-New/Gordon%20QA%20California%20Consumer%20Privacy%20Act%20(CCPA).pdf

[17] Code of Virginia (2025) Title 59.1, Chapter 53: Consumer Data Protection Act. Virginia General Assembly. Available at: https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

[18] Yannella, P.N. and Dickens, T. (2024) New state privacy laws creating complicated patchwork of privacy obligations. Reuters, 7 June. Available at: https://www.reuters.com/legal/legalindustry/new-state-privacy-laws-creating-complicated-patchwork-privacy-obligations-2024-06-07

[19] Jodka, S. (2025) The privacy tug-of-war: States grappling with divergent consent standards. Reuters, 27 March. Available at: https://www.reuters.com/legal/legalindustry/privacy-tug-of-war-states-grappling-with-divergent-consent-standards-2025-03-27

[20] DLA Piper (2025) Data Protection Laws of the World. Available at: https://www.dlapiperdataprotection.com/

[21] Madigan, L., Shenoi, S., Gallagher, M. and Brisuda, C. (2025) 'United States: states fill the gaps in the absence of a federal privacy law', Global Investigations Review, 31 July. Available at: https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/united-states-states-fill-the-gaps-in-the-absence-of-federal-privacy-law

[22] Roth, E. (2025) 'Hundreds of data brokers might be breaking state laws, say privacy advocates', The Verge, 25 June. Available at: https://www.theverge.com/news/693109/eff-privacy-advocates-state-investigate-data-brokers

[23] Xavier, S., Frey, A. and Phillips, S. (2025) 'Protecting reproductive health data: State laws against geofencing', Reuters Legal / Legal Industry, 2 January. Available at: https://www.reuters.com/legal/legalindustry/protecting-reproductive-health-data-state-laws-against-geofencing-2025-01-02

[24] Megas, K. and Kahn, A., (2024). IoT assignment completed! Report on barriers to U.S. IoT adoption. [online] National Institute of Standards and Technology (NIST). Available at: https://tinyurl.com/3f2b4m2z

[25] Caso, J., Cole, Z., Patel, M. and Zhu, W., (2023). Cybersecurity for the IoT: How trust can unlock value. [online] McKinsey and Company. Available at: https://tinyurl.com/4rr4a76v

[26] IEEE, 2025. What is Privacy-by-Design and why it's important? [online] IEEE. Available at: https://tinyurl.com/2p9ccu3e

[27] Yang, G., 2022. An overview of current solutions for privacy in the Internet of Things. Frontiers in Artificial Intelligence, 5, p.812732. doi:10.3389/frai.2022.812732.

[28] Sharma, V. and Mondal, M. (2022) 'Understanding and Improving Usability of Data Dashboards for Simplified Privacy Control of Voice Assistant Data', Proceedings of the 31st USENIX Security Symposium, Boston, MA, August 2022, pp. 3379-3395. Available at: https://www.usenix.org/conference/usenixsecurity22/presentation/sharma-vandit

[29] EPIC (2024) EPIC Launches New Project to Reimagine Health Privacy and Equity in the Digital Age, Electronic Privacy Information Center, 12 December 2024. Available at: https://epic.org/press-release-epic-launches-new-project-to-reimagine-health-privacy-and-equity-in-the-digital-age-in-with-support-from-the-robert-wood-johnson-foundation/