

# DATA PRIVACY AND DIGITAL RIGHTS: PROTECTING PRIVACY THROUGH LAW SURVEILLANCE AND CONSENT

Sijuola Atanda Lawal

School of Law, IALS London, United Kingdom

## **ABSTRACT**

*In our increasing digital society, personal data has become a valuable commodity. The spontaneous increase of online services, social media, and connected devices has led to unprecedented data collection and processing. This article explores the evolution of data privacy and digital rights, examining key legislation such as the GDPR, CCPA, and NDPR, and analyzing the challenges posed by surveillance, consent, and data breaches. Through case studies like the Cambridge Analytica scandal and recent fines imposed on tech companies, this article further highlights the importance of data protection frameworks and the ongoing struggle to balance innovation with individual rights.*

## **KEYWORDS**

*Data Privacy, Data Protection, Digital Rights, Law Surveillance, Consent*

## **1. INTRODUCTION**

The essentiality of data has evolved into a full-blown digital revolution, which has transformed how we communicate, work, and live. With every click, swipe, and share, we generate data that can be collected, analyzed, and monetized. This data is shared amongst companies and governments and can be collected through social media, apps, and online services. While this data-driven economy offers numerous benefits, it also raises significant concerns about privacy, autonomy, and control over personal data. To regulate this, many jurisdictions have enacted strong data protection laws and regulations to fully ensure the safety and protection of digital privacy and digital rights. These laws and regulations include the European Union's General Data Protection Regulation (GDPR), the United States' California Consumer Privacy Act (CCPA), and Nigeria's Data Protection Regulation (NDPR) [1]. These laws establish new rights for individuals, such as the right to know what data is collected, the right to delete it, and the right to control how it is used. They also place duties on companies to be transparent and secure with personal data.

This article examines how digital privacy can be protected through law, oversight of surveillance, and meaningful user consent. We focus on the European Union (EU), the United States (US), and Nigeria as case examples. The EU has a fully established data protection law, which is entrenched in the GDPR, while the United States has a patchwork of privacy rules with strong state laws like the CCPA and no federal privacy law, while Nigeria has recently built a GDPR-style framework in the NDPR [2]. The main features of these data protection laws and how they give consumers control over their information will be explained, including how government and corporate surveillance practices can undermine privacy rights and how the law attempts to balance security with civil liberties. Finally, real-world case studies will be analyzed, including

the Facebook–Cambridge Analytica scandal, the Equifax data breach, and concerns around TikTok. Throughout this study, the relevance of technology law, consumer rights, and the public interest was emphasized.

## **2. DATA PROTECTION LAWS: GDPR, CCPA, NDPR**

Data protection laws aim to give individuals rights over their personal data and impose rules on organizations that collect it. Three influential laws are the EU’s GDPR, California’s CCPA/CPRA, and Nigeria’s NDPR. Although GDPR is an EU law, it affects U.S. companies with European customers, and it has inspired other laws worldwide. Each of these frameworks embodies the idea that personal data deserves legal protection and that individuals should have control over how their data is used.

### **GDPR (EU General Data Protection Regulation, 2018):**

The GDPR is widely considered “the toughest privacy and security law in the world,” affecting any organization anywhere that processes the data of people in the EU. It took effect on May 25, 2018, and introduced strict requirements [1][2]. For example, personal data processing must be lawful, fair, and transparent, and only for explicit, legitimate purposes. The law gives data subjects rights like access to their data, correction of errors, deletion (“right to be forgotten”), and data portability [2]. Violations can trigger hefty fines of up to €20 million or 4% of global revenue. GDPR also requires many organizations to appoint data protection officers (DPOs) and to perform privacy impact assessments. Importantly, GDPR defines “consent” for data use very stringently: it must be “freely given, specific, informed, and unambiguous” [3]. In practice, this means users must be fully told what data is collected and how it will be used, and they must actively opt in [2].

### **CCPA/CPRA (California Consumer Privacy Act/California Privacy Rights Act, 2018/2023):**

In the U.S., there is no single federal privacy law for most personal data (some sectors like health have rules). Instead, California led with its own law, the CCPA (effective January 2020), later amended by the CPRA (effective January 2023). The CCPA gives California consumers rights over their data. Under CCPA, businesses must inform consumers about what personal information they collect and how it’s used and shared [4]. Consumers have the right to know what data is collected about them, the right to delete data collected from them, and the right to opt out of the sale or sharing of their data. They also have a right not to be discriminated against for exercising these rights [4]. The 2020 CPRA amendments added the right to correct inaccurate personal data and the right to limit the use of sensitive personal information. For businesses, the CCPA/CPRA requires systems to respond to consumer requests and to provide clear privacy notices. CCPA is narrower than GDPR in some respects (e.g. it does not require prior consent to collect data, but lets consumers opt out of sales instead), but it still represents a major consumer-rights approach in the U.S. [5].

### **NDPR (Nigeria Data Protection Regulation, 2019):**

Nigeria’s NDPR came into effect in January 2019 under the National Information Technology Development Agency (NITDA). It is modeled closely on the GDPR. The NDPR applies to any organization processing the personal data of Nigerian residents (much like GDPR’s extraterritorial reach) [6]. It mandates that organizations collect and process personal data only for lawful purposes, with consent when required, and implement security measures to protect data. The regulation requires businesses to appoint a Data Protection Officer (DPO) and report data breaches. It also grants Nigerian citizens rights similar to GDPR, such as access to their data

and correction of errors. As one analysis notes, the NDPR was “a significant milestone” in Nigeria’s privacy landscape, imposing “new compliance obligations on corporate entities.” However, enforcement has been uneven. One 2025 study argues that while NDPR has raised awareness and accountability, gaps remain in enforcement and clarity, which “hinder its full impact.”

Insert this in Section 2 after discussing all three laws.

Table 1. Qualitative comparison of key data protection laws in the EU (GDPR), California These laws illustrate a common trend: modern data protection laws recognize privacy as a right and set rule for consent and security. They are part of a broader international movement (for example, Brazil’s LGPD and similar laws in many countries). Importantly, they frame privacy not just as an abstract principle but as consumer rights: the right to know, to access, to delete, and to control personal data.

Feature	GDPR (EU)	CCPA/CPRA (California, US)	NDPR (Nigeria)
<b>Year Enacted</b>	2016 (enforced 2018)	2018 (effective 2020, amended 2023)	2019
<b>Jurisdiction</b>	EU-wide + extraterritorial scope	California residents (extraterritorial effects limited)	Nigeria and data controllers processing Nigerian data
<b>Consent Standard</b>	Freely given, informed, unambiguous, explicit	Opt-out model; no consent needed to collect data	Informed consent required before processing data
<b>User Rights</b>	Access, rectification, erasure, portability, object, restrict	Right to know, delete, opt out, correct (under CPRA)	Access, correction, deletion, and portability
<b>Enforcement Agency</b>	Independent Data Protection Authorities (DPAs)	California Privacy Protection Agency (CPPA)	NITDA
<b>Maximum Fine</b>	€20 million or 4% of global turnover	\$7,500 per violation	₦10 million (~\$12,000) or 2% of gross revenue
<b>Breach Notification Timeline</b>	Within 72 hours	"Reasonable" time	Within 72 hours
<b>Data Protection Officer</b>	Mandatory for large-scale processors	Not mandatory	Mandatory for some organizations
<b>Cross-Border Provisions</b>	Yes (explicitly detailed)	Limited scope	Emerging; not fully developed

### 3. SURVEILLANCE AND PRIVACY

Beyond commercial data rules, a major privacy concern is surveillance by governments and companies. Surveillance can help with security (e.g., to catch criminals or terrorists), but it can

also violate privacy on a massive scale. Both the U.S. and Nigeria have grappled with surveillance powers and the challenge of protecting rights.

### **Government surveillance (U.S. and Nigeria):**

In the United States, a series of laws have authorized extensive government data collection. For example, the Patriot Act (2001) and the FISA Amendments Act allow intelligence agencies broad monitoring powers, including warrantless searches of electronic communications under Section 702. Civil liberties groups argue this amounts to “mass, warrantless surveillance” of Americans and foreigners alike [7]. Only recently, the Supreme Court held that some forms of data collection (like cell-site location records) require a warrant, a step toward restoring Fourth Amendment privacy protections in the digital age. However, many surveillance practices remain controversial. Critics worry, for instance, that collected data could be misused to target dissidents or marginalized groups.

Similarly, in Nigeria, security concerns have driven surveillance expansion. The government has implemented monitoring of internet and phone communications, citing terrorism and unrest. Under Nigerian law, several statutes explicitly permit surveillance and interception. For example, the Terrorism Prevention (Amendment) Act 2013 allows interception of communications to prevent terrorism; the NCC Act 2003 lets telecom companies disclose customer data to authorities; and the Cybercrimes Act 2015 requires telecom firms to hand over encryption keys for law enforcement [8]. Even the Nigerian Constitution itself (Section 45) permits privacy restrictions for “public safety, order, and morality.” In practice, reports indicate that journalists, activists, and ordinary Nigerians often face monitoring or data requests from the state. One analysis note that “monitoring journalists, activists, and politically engaged civic society groups” has become common, raising fears of “digital repression and human rights abuse.”

Neither country’s laws are perfect. Nigeria’s NDPR nominally protects privacy as a fundamental right, but many older laws and practices allow state surveillance. As one analyst asks, can Nigeria “ensure national security without abusing citizens’ rights to privacy” when so many laws permit broad monitoring? In the U.S., legal safeguards like the requirement for warrants are evolving through court decisions and reforms (e.g., the USA Freedom Act of 2015 partially curtailed bulk phone data collection), but tensions remain between security agencies and privacy advocates.

### **Corporate Surveillance:**

Government surveillance gets media attention, but much of our personal data is actually collected by private companies. Every website visit, social media post, and smartphone app often tracks our behavior [9]. Companies build detailed profiles by combining browsing histories, location data, purchase records, and social connections. This “commercial surveillance” is often used for targeted advertising or recommendations [10]. In the U.S., tech firms have built surveillance-based business models; even in Nigeria, social media use and digital services create similar tracking. While these practices are usually covered by user agreements or privacy policies, critics argue that many people do not truly consent [9].

The potential for abuse is serious. For instance, algorithmic systems can discriminate. Recent research highlights that surveillance tools like facial recognition can disproportionately affect racial minorities due to biased algorithms and enforcement patterns. Communities of color in the U.S. have historically been over-surveilled, and new tech can amplify these disparities [10]. The Brookings Institution notes that “surveillance patterns often reflect existing societal biases” and enable “more precise discrimination” against marginalized groups. This means privacy is not just an abstract concern but also a matter of social justice.

To protect privacy, many advocate for legal limits. Some proposals include banning bulk data collection without warrants, requiring independent oversight of surveillance programs, and enforcing “privacy by design” in technology. In Nigeria, calls have been made to align all laws with privacy principles. Non-governmental organizations like Paradigm Initiative are raising awareness of digital rights.

Overall, surveillance presents a fundamental tension: security vs. liberty. Both in the U.S. and Nigeria, experts stress the need for proportionality and transparency. In Nigeria, one commentator warns that Nigeria’s numerous surveillance laws must be balanced so that “tracing the digital activities of journalists” is not done arbitrarily. In the U.S., many civil libertarians urge reform of laws like FISA to require warrants and greater judicial oversight. These efforts illustrate a key message: effective privacy protection requires scrutiny of surveillance powers, ensuring they do not override citizen rights.

#### 4. CONSENT AND DATA USAGE

Consent is a cornerstone of data privacy law. In theory, before a company collects or processes personal data, it should get the user’s consent. But *what counts as valid consent*, and do people really understand what they are consenting to?

Under laws like the GDPR, informed consent has strict requirements: it must be “freely given, specific, informed, and unambiguous.” This means a user must have a real choice (no coercion), and the company must clearly explain who is collecting the data, what data, why, and how it will be used. Users must also be able to withdraw consent easily [1]. For example, an employer cannot force employees to consent as a condition of employment, because that would not be voluntary.

In the CCPA and NDPR contexts, consent is also expected in many cases. CCPA requires opt-out consent (not sale of personal data), and NDPR requires consent or another lawful basis for processing. However, in practice, many websites use complex privacy policies and “terms of service” that few people read [10].

Studies show a big gap between formal consent requirements and actual user behavior. One survey reported that only about one in five Americans say they *always or often read* a company’s privacy policy before agreeing to it. Even those who attempt to read them find them confusing; privacy policies are often written in dense legal language [11]. A privacy researcher at Mercer University notes that many companies use “adhesion contracts” that favor the business over the user. For instance, hidden clauses have been found in some policies giving companies sweeping rights to user data. The Mercer study quotes a student observing that users have “no power” and privacy agreements often protect businesses “at the expense of the customer’s privacy, awareness, and power.”

This indicates a “consent paradox”: people are concerned about privacy but routinely click “Accept” without understanding the details. Worldwide surveys confirm it. The Pew Research Center found that Americans feel largely out of control over their data and worried about how companies and governments use it. In 2023, 71% of Americans said they worry about government data use (up from 64% in 2019), and 67% said they “understand little to nothing” about what companies do with their personal data. The vast majority (73%) believe they have little or no control over corporate data usage [12].

For digital rights, this weak consent is a problem. If companies collect data by design through hidden trackers or confusing opt-out boxes, can we say users truly agree? Critics argue that

consent is often a façade and that stronger privacy by default rules are needed. For example, many suggest data minimization (collecting only what is necessary) and requiring clear, prominent notices. In some cases, regulators are tightening consent rules and GDPR's standard is one of the strictest. In the U.S., California also passed the California Privacy Rights Act (2020), expanding rights, partly responding to the realization that previous laws (including CCPA) still left consumers feeling powerless [11].

In Nigeria, similar issues exist. Even with the NDPR, public awareness of privacy rights is still growing. A survey of Nigerians' perceptions found that many are unfamiliar with data protection laws and don't fully understand privacy terms (though open data on this is limited). One research summary notes that Nigerians' understanding of data protection is still developing, highlighting the need for education on digital rights.

Consent is legally required, but true *informed* consent is hard to achieve at scale. This challenge means privacy protections can't rely on consent alone. Laws like GDPR, CCPA, and NDPR therefore also impose substantive obligations on data handlers (e.g., data security, transparency) and grant robust user rights. For students and consumers, the takeaway is that one should read privacy notices when possible, use privacy settings, and support calls for clearer laws.

## **5. CASE STUDIES**

Real-world incidents bring these issues into focus. We examine three case studies that have shaped the debate on data privacy.

### **5.1. Cambridge Analytica (Facebook Data Scandal)**

The Cambridge Analytica scandal (exposed in 2018) is a textbook case of misuse of personal data without proper consent. Cambridge Analytica was a political consulting firm involved in the 2016 U.S. presidential election. It obtained Facebook profile data on tens of millions of users without those users' explicit permission [13]. An academic app, "this is your digital life" collected data from a few hundred thousand Facebook users who downloaded it for a personality quiz. However, due to Facebook's policy at the time, the app also gathered data from those users' friends, exploding the dataset to tens of millions of people. In total, "more than 50 million profiles mostly belonging to registered U.S. voters were harvested". This data was then allegedly used to build voter profiles and target political advertising [14].

The incident emerged when whistleblowers disclosed the data breach to the media. News outlets documented how Cambridge Analytica's work was directly tied to Facebook's lax data controls. As one report described, hundreds of thousands took the test for academic use, but unbeknownst to them or their friends, a massive pool of personal data was amassed and exploited. The incident highlighted a dangerous gap: users may consent to one use of their data (the app's stated purpose) but not be aware of extended uses [14].

The fallout was huge. Facebook CEO Mark Zuckerberg testified before Congress. Regulators launched inquiries: the UK Information Commissioner said it was "investigating the circumstances in which Facebook data may have been illegally acquired and used." In the U.S., Massachusetts's Attorney General opened a probe, and Senator Mark Warner said the breach showed that the "online political advertising market is essentially the Wild West," demanding better regulation [13].

Beyond politics, Cambridge Analytica underscored a general lesson: when data is collected under one pretext (like a personality test), it can be repurposed in ethically questionable ways if not tightly controlled. It was a wake-up call that personal data on social media can be weaponized. In practical terms, it spurred Facebook and others to tighten data access. Facebook announced changes to limit third-party app data (for example, after queries from journalists, Facebook suspended Cambridge Analytica from its platform). It also fueled support for stronger privacy laws like GDPR and CCPA [14].

## **5.2. Equifax Data Breach (2017)**

The 2017 Equifax breach is one of the most severe data breaches in U.S. history. Equifax is a major consumer credit bureau that holds financial and personal data. In September 2017, Equifax disclosed that hackers had compromised the personal information of 148 million Americans. This included highly sensitive data: full names, Social Security numbers, birth dates, addresses, and, in some cases, credit card numbers or driver's license numbers. Essentially, nearly half the U.S. population's data was exposed [15].

Why did this happen? Investigations found Equifax had failed to patch a known security vulnerability in its systems. Even worse, Equifax delayed discovering and announcing the breach for months. The exposed data made victims vulnerable to identity theft. Equifax's dominant market position (most Americans have an Equifax credit file) made the breach especially impactful.

The breach led to legal consequences and discussions about consumer rights. By mid-2019, U.S. regulators and 48 state attorneys general announced a settlement of up to \$700 million with Equifax. Under this settlement, Equifax agreed to pay hundreds of millions for credit monitoring services and other relief to affected consumers (and fines of \$100 million) [16]. Despite the settlement, many criticized that the penalties were insufficient given the scale of the harm. EPIC's Marc Rotenberg testified that Congress should mandate privacy protections by law, arguing that relying on market self-regulation failed to secure Americans' data.

The Equifax case highlighted three points: first, financial and governmental data (like credit records) must be secured at the highest level since it is deeply personal. Second, it exposed the lack of a comprehensive U.S. privacy law. Some victims argued that an unbroken timeline (mandatory breach disclosure) and stricter safeguards (like mandatory encryption) could have prevented the harm. Third, it underscored the idea that privacy "must be mandated by Congress" since companies have not sufficiently protected data. In the aftermath, some lawmakers renewed calls for a U.S. data protection law, and some states (like Illinois) used their own laws (e.g. biometric data laws) to address specific harms [15].

## **5.3. TikTok and Social Media Privacy**

TikTok, the Chinese-owned short-video app, has been a flashpoint for privacy debates globally, and especially in the U.S. and Nigeria. TikTok's massive popularity (over a billion users worldwide) means it collects large amounts of user data (what videos are watched, location, device info, and more). Critics worry that because TikTok's owner is in China, the Chinese government could potentially access or influence this data [17].

In the United States, privacy and national security concerns converged. The Trump administration (2020) attempted to ban TikTok unless it divested to a U.S. company, citing fears of data spying. A judge briefly blocked that action. However, in late 2022, the Biden administration banned TikTok on federal government devices outright, a policy now adopted by

most U.S. states [17]. Public opinion is divided but notably cautious: a 2025 Pew survey found that 34% of Americans support a total TikTok ban (down from 50% in 2023), and many opponents of the ban say a ban would infringe free speech [18]. Importantly, among those supporting a ban, a majority cite data security concerns and TikTok's Chinese ownership as "major reasons." This shows that privacy and data security are central to the debate, not just politics.

In Nigeria, TikTok's story unfolded differently but with similar themes. In June 2021, Nigeria's government announced a ban on TikTok, officially because of worries that it was being used for "activities capable of undermining Nigeria's corporate existence." Many observers read this as targeting political dissent (TikTok was a platform for youth activism) as well as general influence. After about 2-3 months, the ban was lifted, and discussions began about regulating social media content. Nevertheless, Nigeria's concern echoed global worries: a foreign-owned app could influence local culture or politics, and its data might not be protected by Nigerian law [19].

TikTok's case studies illustrate the tension between digital innovation and privacy/security. While TikTok argues it has taken steps (like opening a "transparency center" in the U.S.) to address concerns, the app remains in legal crosshairs. U.S. legislators are considering laws to force data localization (keeping U.S. user data in U.S. servers) or limit certain apps. Nigeria, too, is updating its laws (the Data Protection Act 2023) to include stricter rules on data transfers and social media [20]. These real-world examples show that when personal data and national security overlap, privacy protections can become politically charged. Yet they also reinforce why clear data rules are needed globally.

## **6. PROTECTING DIGITAL PRIVACY: STRATEGIES AND REFORMS**

Given the challenges above, how can societies better protect digital privacy and uphold data rights? Researchers and advocates propose several strategies:

### **6.1. Strengthen and Enforce Laws**

The first critical step in protecting digital privacy involves strengthening and enforcing laws. In countries like the U.S. and Nigeria, there is a need for stronger data protection frameworks that comprehensively address the digital challenges of the 21st century. In the U.S., many privacy experts advocate for federal data protection legislation that complements state laws such as the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). A unified federal law would provide consistency and clarity across states, ensuring that privacy rights are universally upheld [20]. Meanwhile, emerging challenges like AI privacy, algorithmic transparency, and data portability should be included in these legal frameworks, as current laws are not equipped to handle these modern issues.

In Europe, the General Data Protection Regulation (GDPR) serves as a model for robust privacy protection. Its core provisions, such as the right to access, deletion, and breach notification, should be considered baseline rights that must be guaranteed on a global scale. Specifically, the GDPR provides individuals with clear rights over their data and demands that companies adopt data protection measures from the start of their processes, also known as privacy by design [16]. For example, requiring businesses to implement clear opt-in consent protocols before any personal data is collected would go a long way in enhancing user privacy and consent standards.

In Nigeria, full implementation of the Nigeria Data Protection Regulation (NDPR) and the new Data Protection Act is essential. One of the key elements of the NDPR is empowering the Nigeria Data Protection Commission (NDPC) to investigate violations and impose penalties on offenders [17]. These laws are crucial in closing existing gaps in enforcement and ensuring that data protection laws are not merely theoretical but actively upheld in practice. Strengthening the legal framework in both countries requires cooperation between governments, regulatory bodies, and global organizations to address new concerns such as biometric data, cloud storage, and AI data ethics. States and countries must harmonize laws internationally, encouraging cross-border legal standards that can effectively tackle emerging issues like AI-driven surveillance and global data breaches.

## **6.2. Privacy by Design and Technology**

Another key strategy is the integration of privacy by design and advanced technological safeguards. Technological innovation plays a pivotal role in protecting privacy without relying solely on user consent, which can often be bypassed or misunderstood. One way to integrate privacy into the digital ecosystem is by adopting a data minimization approach, which involves collecting only the data necessary for the intended purpose, thus reducing the risk of breaches or misuse. For instance, companies should design their systems to collect minimal user data, process it securely, and retain it for only as long as necessary.

Further, technological safeguards such as end-to-end encryption are vital for protecting user communications. Encryption ensures that even if data is intercepted, it cannot be read by unauthorized parties. This is especially important in sectors like finance, healthcare, and social media, where sensitive personal data is regularly exchanged. In addition, differential privacy techniques can be employed to protect individual identities in datasets by adding statistical noise, making it harder to trace data back to specific users.

Regulators and privacy advocates should push for companies to adopt privacy by design philosophy, where privacy is embedded into the software development process rather than added as an afterthought. For example, mobile applications could default to the most private settings, and users could be required to opt-in for data sharing rather than opting out [20]. This approach would address growing concerns about privacy violations and provide users with more control over their personal data. In this context, browser and operating system developers should ensure that their systems automatically block third-party tracking cookies, fingerprinting, and other intrusive surveillance methods that compromise user privacy. Implementing these technological safeguards in practice will not only minimize risks but will also create a proactive privacy protection model where companies prioritize privacy from the beginning.

## **6.3. Transparency and Accountability**

To complement technological safeguards, transparency and accountability are essential strategies for digital privacy. Governments and companies must be transparent about how they collect, use, and store personal data. For instance, businesses should provide clear, concise privacy policies that avoid legal jargon and are understandable to ordinary users. Proactive disclosures of data breaches are crucial for building trust and allowing users to take corrective actions if their personal data is compromised. Transparency can also be improved through the introduction of privacy nutrition labels, which summarize key data usage practices in a format that users can easily understand immediately [18].

In addition to these measures, data protection authorities such as the Federal Trade Commission (FTC) in the U.S. and the Nigeria Data Protection Commission (NDPC) should actively publish

guidance and enforcement actions. This would allow the public to hold businesses accountable and ensure that violations of privacy laws are penalized effectively. Independent audits are also a powerful tool to ensure that organizations comply with privacy regulations. In countries like Germany, privacy impact assessments (PIAs) are mandatory for large-scale data processing projects. Similarly, Nigeria could implement mandatory impact reviews for projects involving the handling of sensitive personal data. By integrating these transparency and accountability mechanisms, we can create a system where users are not only informed about their rights but also have the means to hold companies accountable for their data protection practices.

#### **6.4. International Cooperation**

In our interconnected world, privacy protection can no longer be confined to national borders. As data flows freely across jurisdictions, international cooperation becomes essential for protecting digital privacy. One of the most significant frameworks for promoting cross-border privacy protection is the General Data Protection Regulation (GDPR). The GDPR's extraterritorial provisions, which apply to companies outside the EU that handle EU citizens' data, have set an important precedent for global data protection norms. Countries like Nigeria and the U.S. can learn from the GDPR and work together to align standards on privacy, data protection, and cross-border data flows [20].

The United Nations has recognized privacy as a human right, particularly through Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Regional agreements, such as the EU-U.S. data privacy frameworks and the African Union's draft data protection convention, could help align international data protection standards. By adopting similar frameworks, countries can ensure that privacy protections are consistent globally and that individuals' digital rights are respected, regardless of their geographical location.

Moreover, cross-border cooperation is also vital for law enforcement access to data. While protecting privacy is paramount, ensuring that law enforcement agencies can access data in a legally compliant manner for legitimate investigations is equally crucial. Countries should establish clear legal processes for mutual legal assistance treaties (MLATs), which balance privacy rights with the need for effective law enforcement. In this way, digital privacy can be protected while ensuring that data is available for legitimate governmental investigations.

#### **6.5. Public Awareness and Civil Society**

Finally, public awareness and the active participation of civil society organizations are essential for achieving improved digital privacy. Educational campaigns should be launched to inform individuals about their digital rights, how they can protect their personal data, and the importance of privacy settings and encryption tools. For example, in Nigeria, groups like Paradigm Initiative are advocating for digital rights education and legal reform. In the U.S., organizations such as the Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) are leading the charge to defend privacy rights through litigation, lobbying, and advocacy [21].

Public pressure has already led to significant changes. Following the Cambridge Analytica scandal, social media giants like Facebook changed their privacy policies, and several U.S. states enacted new privacy laws. This illustrates the power of civil society and public pressure in driving reforms [17]. To continue this progress, governments and organizations must work to build awareness and empower citizens to take control of their digital privacy.

## 6.6. Balance with Other Interests

Finally, privacy protections must be balanced with other societal interests, such as security and public safety. This requires carefully crafted laws that clearly define the limits of surveillance and ensure that data collection programs are not misused. In Nigeria, the Data Protection Act criminalizes certain data abuses but also emphasizes the protection of whistleblowers and journalists, thereby safeguarding freedom of expression. In the U.S., surveillance programs are often debated in Congress to ensure that privacy protections are not undermined in the name of security [21].

By striking a balance between privacy and security, countries can ensure that privacy laws serve their intended purpose without being overly restrictive or harmful to public safety. This balance is vital for maintaining democratic values and fundamental freedoms.

## 7. CONCLUSION

In an age where data is a major commodity, protecting data privacy and upholding digital rights is a fundamental challenge. The GDPR, CCPA/CPRA, and NDPR represent significant legal efforts to give individuals control over personal information and to enforce accountability on data processors. The United States and Nigeria, despite very different legal traditions, are both adapting to a data-driven world by strengthening consumer rights, though each still has gaps to fill. The risks of ignoring these issues are clear in cases like Cambridge Analytica and Equifax: when personal data is misused or inadequately protected, the consequences are widespread and damage trust [16].

At the same time, technology and governance must evolve in tandem. Surveillance capabilities can aid public safety, but without transparency and checks, they can erode the very liberties they claim to defend. Meaningful consent remains elusive for most users, suggesting that relying solely on “clickwrap” agreements is insufficient. We need a multi-faceted approach: robust laws and enforcement, user-friendly privacy tools, data ethics in technology design, and an informed public.

The journey toward strong digital rights is ongoing. Experts continue to debate ideal solutions, from federal privacy legislation in the U.S. to more comprehensive data protection frameworks in Africa. What is certain is that as data grows ever more central to daily life, so too does the importance of defending privacy [14]. Protecting digital privacy serves not only individual interests but also the public interest, supporting free expression, democracy, and consumer confidence. In this way, data protection laws and digital rights belong at the intersection of technology law, consumer rights, and public interest law. By learning from case studies and continuing to improve legal and technical safeguards, societies can work toward a future where the benefits of a connected world are enjoyed without sacrificing fundamental privacy.

## REFERENCES

- [1] Local Government Association, “The General Data Protection Regulation (GDPR) Guidance for members,” 2018. Available:[https://www.local.gov.uk/sites/default/files/documents/The+General+Protection+Data+Regulation+\(GDPR\)+Guidance+for+Members.pdf](https://www.local.gov.uk/sites/default/files/documents/The+General+Protection+Data+Regulation+(GDPR)+Guidance+for+Members.pdf)
- [2] GDPR, “General Data Protection Regulation (GDPR),” General Data Protection Regulation (GDPR), 2016. <https://gdpr-info.eu/>

- [3] W. G. Voss and H. Bouthinon-Dumas, "EU General Data Protection Regulation Sanctions in Theory and in Practice," *Santa Clara computer and high-technology law journal*, vol. 37, no. 1, pp. 1–96, 2021, Available: [https://www.researchgate.net/publication/348419137\\_EU\\_General\\_Data\\_Protection\\_Regulation\\_Sanctions\\_in\\_Theory\\_and\\_in\\_Practice](https://www.researchgate.net/publication/348419137_EU_General_Data_Protection_Regulation_Sanctions_in_Theory_and_in_Practice)
- [4] R. Bonta, "California Consumer Privacy Act (CCPA)," State of California - Department of Justice - Office of the Attorney General, 2024. <https://oag.ca.gov/privacy/ccpa>
- [5] J. Lee, "CCPA/CPRA: Consumers Bear the Burden as Companies Bear the Crown," *UC Law SF Scholarship Repository*, 2024. [https://repository.uclawsf.edu/hastings\\_international\\_comparative\\_law\\_review/vol47/iss2/5](https://repository.uclawsf.edu/hastings_international_comparative_law_review/vol47/iss2/5)
- [6] NITDA, "NDPR Creates 2,686 Jobs, As NITDA Presents First Data Protection Performance Report – NITDA," *Nitda.gov.ng*, 2020. <https://nitda.gov.ng/ndpr-creates-2686-jobs-as-nitda-presents-first-data-protection-performance-report/3681/>
- [7] S. Boykin, "The Separation of Powers, 38 U. ARK. LITTLE ROCK L. REV.," 2015. Available: <https://lawrepository.ualr.edu/cgi/viewcontent.cgi?article=1944&context=lawreview>
- [8] T. Shvyryda, "GRG," *GRG*, 2022. <https://www.gorstra.com/africa-desk/public-surveillance-in-nigeria>
- [9] A. E. Aiello, A. Renson, and P. N. Zivich, "Social Media– and Internet-Based Disease Surveillance for Public Health," *Annual Review of Public Health*, vol. 41, no. 1, 2020, doi: <https://doi.org/10.1146/annurev-publhealth-040119-094402>.
- [10] G. M. Dickinson, "The Patterns of Digital Deception," 2024, doi: <https://doi.org/10.2139/ssrn.4948722>.
- [11] B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner, "Americans' Attitudes and Experiences with Privacy Policies and Laws," *Pew Research Center: Internet, Science & Tech*, 2019. <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>
- [12] J. Harper, "Inside the Beltway: Bobby Jindal now backs Donald Trump, his former presidential rival," *The Washington Times*, 2023. <https://www.washingtontimes.com/news/2023/oct/18/inside-beltway-bobby-jindal-now-backs-donald-trump/>
- [13] N. Confessore, "Cambridge Analytica and Facebook: the Scandal and the Fallout so Far," *The New York Times*, 2018. Available: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- [14] I. Ur Rehman, "Facebook-Cambridge Analytica data harvesting: What you need to know," 2019. Available: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5833&context=libphilprac>
- [15] Electronic Privacy Information Center, "EPIC - Equifax Data Breach," *archive.epic.org*, 2017. <https://archive.epic.org/privacy/data-breach/equifax/>
- [16] Federal Trade Commission, "Equifax Data Breach Settlement," *Federal Trade Commission*, 2024. <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>
- [17] M. Minges, "National Security and the TikTok Ban," *American University*, Jan. 23, 2025. <https://www.american.edu/sis/news/20250123-national-security-and-the-tik-tok-ban.cfm>
- [18] C. McClain, "Fewer Americans now support TikTok ban, see the platform as a national security threat than in spring 2023," *Pew Research Center*, 2025. <https://www.pewresearch.org/short-reads/2025/03/25/fewer-americans-now-support-tiktok-ban-see-the-platform-as-a-national-security-threat-than-in-spring-2023/>
- [19] International Press Centre, "Freedom of Expression – Page 2," *Ipcng.org*, 2023. [https://www.ipcng.org/category/freedom-of-expression/page/2/?filter\\_by=popular](https://www.ipcng.org/category/freedom-of-expression/page/2/?filter_by=popular)
- [20] B. O. Jemilohun, "AN APPRAISAL OF THE INSTITUTIONAL FRAMEWORK FOR DATA PROTECTION IN THE UK, USA, CANADA AND NIGERIA," *Journal of Asian and African Social Science and Humanities*, vol. 1, no. 1, pp. 8–26, 2015, Available: <https://www.aarcentre.com/ojs3/index.php/jaash/article/view/17/198>
- [21] Electronic Frontier Foundation., "Warrantless Surveillance Under Section 702 of FISA | American Civil Liberties Union," *American Civil Liberties Union*, 2024. <https://www.aclu.org/warrantless-surveillance-under-section-702-of-fisa>