Challenges of Cross-National Legal Regimes: An Effort at Restructuring the Balance of Power during Data Breach and Loss of Privacy in the US

Emmanuel Adéníran
Yale University
emmanuel.adeniran@yale.edu

ABSTRACT

As a consequence of American provenance and history, its cultural and political landscape is such that its government rarely intervenes in making comprehensive governmental mechanisms in law to protect the cybersecurity and privacy of its citizens. The American federal government is mostly hands-off when there are situations that result in breaches of American consumers' private information resulting from exchanges between private parties. And because of that, consumers can find themselves in a disparate power relationship with large credit reporting corporations and generally have little to no recourse in the case of data breaches. However, such relationships are not identical around the world. Some different circumstances and approaches empower individuals. For example, in Europe and France, legal regimes allow fine-detailed interjections into the workings of privacy and cybersecurity affairs regardless of whether the parties are private or public entities. This paper demonstrates the power imbalance between credit reporting agencies and the American consumer. The paper also provides an assessment of the French Cybersecurity Strategy for legislative mechanisms that can bring about empowerment for the American consumer and provides ways for overcoming the impediments to legislative promulgation. And concludes with legislative recommendations to protect the privacy and cybersecurity of the victims of cyber breaches.

KEYWORDS

Credit Reporting Agencies, General Data Protection Regulation, Cybersecurity, Privacy, Data, Common Law and Civil Law Systems

1 INTRODUCTION

A series of data breaches have adversely affected ordinary citizens in the US. In assessing the impact of these breaches, several factors become apparent. First among them is that the American federal government's actions demonstrate that it is reluctant to intervene in the particularities associated with preserving its citizens' privacy and cybersecurity. Its legislative history regarding the protection and regulation of privacy is demonstrably ad hoc, limited, and haphazard in this regard. Examples abound, such as the Driver's Privacy Protection Act (DPPA) of 1994 [16], the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [7], Cable Television Protection and Competition Act of 1992 [3], the Video Privacy Protection Act (VPPA) of 1988 [19], the Cable Television Protection and Competition Act of 1992, the Fair Credit Reporting Act (FCRA) of 1970 [18], and the Gramm-Leach-Bliley Act (GLBA) of 1999 [1].

This ad hoc approach is apparent when it pertains to making comprehensive governmental mechanisms in law to protect the cybersecurity and privacy of its citizens, especially in situations that could result in loss of privacy private information breaches that come about as a result of exchanges between private parties. And because of that, individuals in a relationship with large corporations generally have little to no recourse during or after data breaches other than meager compensatory measures, which usually are lopsided and considerably in favor of the large corporations and against those individuals who would be victims of a breach or data loss [27]. There is even a worse power relationship: when data breaches involve data brokers or Credit Reporting Agencies (CRA) like Experian or Equifax, who are in the business of creating dossiers on people from information obtained from Furnishers. Furnishers are enterprises that extend credit lines or banks that provide CRAs with consumer information. The information usually includes dates when consumers' opened accounts, punctuality of bill payments, or delinquency. CRAs gather this information, along with other open-source information, to compile consumers' dossiers. CRAs, in turn, furnish these dossiers to third parties who use the information to determine creditworthiness, employability, insurability, tenancy, et cetera [5, 9].

In those cases when data breaches involve CRAs, consumers, whose activities ostensibly provide information on individuals' borrowing and bill-paying habits, usually do not supply these data brokers with their own personal information. Yet, the individuals have to deal with the consequences of data breaches of these data brokers' systems. Fortunately, there are other models of consumer-business relationships, and those relationships are not identical worldwide. There are many models of relationships with different circumstances and approaches that empower consumers due to alternative legislative regimes.

In reviewing alternative legislative regimes that allow fine-detailed interjections into the workings of privacy and cybersecurity affairs regardless of whether the parties affected are private or public, the aim was to find governments that posture governmental agencies in a significantly more interventional way than is done in America. The French system is sufficiently interventional but not so different that it is entirely incompatible with the American system. Further, the focus is on aspects of the French Cybersecurity Strategy, particularly because, as a country with an established single national data protection authority, the Commission Nationale de l'informatique et des libertés (CNIL) [13], the French leverage the existing General Data Protection Regulation (GDPR) [25] European framework to protect its citizens from data breaches and privacy exploitation

aggressively. The French also believe that "the fundamental instruments of sovereignty are already indistinguishable from the tools of technological power" [21]. Consequently, the French have postured arms of the government as aggressively more interventional than is done in America.

In assessing the French approach [20], immediate solutions would bode well in implementation in the US. However, because of the different forms and processes of both countries' civil government, constitutions, and political culture, it would be difficult to transplant intact legal frameworks or legislation from France to the US. Consequently, there is a discussion of those impediments, ways to reconcile them, and recommendations for implementing them.

2 BACKGROUND

To foster understanding the problem-space, briefly reviewing data breaches and their impacts at large can be helpful. There are various data breaches of varying impacts on many cohorts of victims. The harms across them are similar and preponderate around creditworthiness, employability, insurability, tenancy, reputational damage, and the anxiety experienced due to these impending risks. A focus on those breaches whose victims are ordinary individuals, not corporations or governmental entities, is illustrative of the impact of the problem. Particularly breaches associated with data brokers and dossier compilers, like Equifax and Experian.

2.1 Breach of Equifax's Systems

In the case of Equifax, for the services it provides to consumers whose information it has aggregated, it provides an online platform for consumers to dispute the accuracy of one's own credit report dossier. Equifax's online platform is a web application that used Apache Struts to create the online application. That framework was under the maintenance of the Apache Software Foundation. On the 7th of March 2017, the Apache Software Foundation announced the discovery of a vulnerability of its Struts. Apache issued a patch to remediate the vulnerability on the same day. The following day, the 8th of March 2017, the Department of Homeland Security (DHS) notified the three main CRAs, Equifax, Experian, and TransUnion, of the vulnerability [23]. On the 9th of March, Equifax distributed an internal communique instructing its systems-security administrators to apply the remediating patch issued by the Apache Software Foundation. However, Equifax's systems security administrators neglected to apply the patches as instructed. Instead, the administrators chose to scan their systems to detect any related vulnerability. The administrators indicated their tool found no associated vulnerabilities on their systems. Perhaps because the vulnerability was not yet being exploited or the administrators had not programmed their scanning tool to discover the announced vulnerability.

Nearly 4 months later, on July 29th, the systems security administrators noticed suspicious traffic traversing their network associated with the web application used to implement the online dispute portal. At that point, Equifax's systems security administrators finally applied the patch as advised by the Apache Software Foundation. However, the following day, on the 30th of July 2017, Equifax's systems security administrators continued to notice further suspicious network traffic and activity and resolved to bring down the online dispute portal. More than another month passed before Equifax commissioned a third party to perform a forensic investigation, which, in turn, revealed that there had been a significant breach of consumer information that resided on their systems. On the 7th of September 2017, Equifax finally informed the public that it had discovered a data breach that affected around 145 million US consumers. The announcement indicated that the accessed information included first and last names, social security numbers, dates of birth, addresses, and other identification numbers such as driver's license numbers [6].

Equifax is an example of a powerful enterprise that essentially gets away with being neglectful. As part of its business model, it is a multibillion-dollar company externalizing its business risks onto people who did not directly sign up for its services. It is invading people's privacy by collecting and aggregating personal information. Then due to Equifax's fault or negligence in keeping the private information safe and secure, people's sensitive information has been in possession of unauthorized hackers due to a data breach. The information obtained in the data is very revealing of the consumers. Data brokers or entities in possession of sufficient consumer information can combine and analyze data about consumers to make potentially sensitive inferences [5, 9]. Hackers could glean consumers' patterns of life, their preferences, genders, sexualities of unwitting individuals from the stolen private information. Those whose information was stolen do not have a recourse to sue for the loss of private information as statute protects companies like Equifax [9]. Companies like these mostly get away with little repercussions for their neglect. In most cases, as was the case during this breach, Equifax offered two years of credit monitoring service. However, those hackers who obtained the private information can wait at least three years before they ever use the data or sell it on the dark web. The FTC reached a data breach settlement with Equifax for $425 million, an amount that pales in comparison to the impact bore by the victims of the hack [10, 27].

2.2 Breach of Experian's Systems

In the case of another data broker, Experian, there was another breach that consumers bore the brunt of the burden. On Sept. 15, 2015, Experian discovered an unauthorized party had accessed T-Mobile data housed on their server. Experian claimed that the Hackers did not access Experian's consumer credit database and that Hackers obtained no credit card or banking information. They further detailed that the unauthorized access was in an isolated incident over a limited period of time. The announcement stated that the hack included access to a server that contained personal information for consumers who had applied for T-Mobile's postpaid telecommunications services between September 1st, 2013, through September 16, 2015. Further stated was that hackers accessed records containing names, addresses, Social Security numbers, dates of birth, and identification numbers like driver's license, military ID, or passport numbers. Experian claimed that they were notifying the individuals who may have been affected and, as usual, offered free credit monitoring and identity resolution services for two years following the breach [12]. Needless to say, there is a problem of externalization of business risks onto powerless consumers on the part of CRAs like Experian and Equifax. However, externalities are not the only root causes of the problem. There are

other underpinning reasons why these CRAs can externalize their business risks onto consumers who are not their direct customers. The elements of the problems are structural and require a holistic approach to resolve them effectively to shift the balance of power to a more equitable state.

3 ELEMENTS OF THE PROBLEM

Regarding achieving equity in the balance of power between large corporations like Equifax and the ordinary consumer whose activities are mainly to borrow money and pay bills, the problems that are germane to the issue need to be addressed. Understanding and addressing the problem could shift the balance of power in the relationship between consumers and CRAs toward a more equitable state. The fact that victims of these data breaches usually have no recourse of value has been established. Also established is the business model of CRAs being heavily dependent on the externalization of business risks that the CRAs shift onto powerless consumers who are not even direct customers of the CRAs. In most cases, they have not agreed to have dossiers about themselves created and stored by these CRAs. However, there are further problems. When breaches occur, CRAs rarely lose money, and any reputational damage is not relevant as ordinary consumers do not usually transact with CRAs. The Furnishers and third parties who are actually customers of the CRAs rarely abandon the CRAs. Further, the creditworthiness information industry is effectively an oligopoly, dominated by a small group of CRAs. Further, necessities like electricity and internet access often require a creditworthiness check. So, another significant problem is the inability of ordinary consumers to realistically opt out of the network effects of the creditworthiness information industry. Another problem is the disunited and somewhat inconsistent set of laws governing the collection, use, and protection of creditworthiness information.

3.1 Discordant Laws

Discordant statutes can result in confusion, paralysis of the enforcement agencies, and errant litigation that often create barriers to achieving the important legislative objectives. The enactments of two laws, the Fair Credit Reporting Act (FCRA) and the Gramm–Leach–Bliley Act (GLBA), demonstrate the fact that there is a piecemeal approach to the protection of privacy and that there is a need for reconciliation of the authorities and aims of the laws.

3.1.1 FCRA. The FCRA is one of the US government's preliminary attempts to provide a legislative structure to protect consumers' information and its use in the era of digitization. Consequent to an amendment to the FCRA passed in 2003 (Fair and Accurate Credit Transactions Act (FACTA)), the FCRA provides authority for the regulation of Consumer Reporting Agencies (CRAs) and those entities who provide and use consumer reports and information. The FCRA applies to how CRAs can use and share the information [17]. Still, according to a Government Accountability Office (GAO) report, all 50 states also have laws about consumer creditworthiness reporting, which have similar requirements to those in FCRA. Further, the same report from the GAO states that all 50 states have laws requiring enterprises that operate in the creditworthiness information industry to notify consumers in the event of a data breach of their systems. However, those laws are said to have varying requirements from state to state. The varying requirements include the timing or method of notification of consumer and which of the affected consumers must be notified Office [24].

3.1.2 GLBA. The GLBA was enacted, as stated in its long title, to "enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, insurance companies, and other financial service providers, and for other purposes" [1].

3.2 Disunity of Authorities

Also relevant is the purposes of the entities invested with the authority to exercise powers under the FCRA and GLBA. There are many. However, the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) are two of the primary enforcement agencies of the FCRA and, in many ways, the GLBA, and are germane entities whose purviews and authorities under the FCRA and GLBA are intertwined, misplaced, and in need of reconciliation.

3.2.1 FTC. The FTC, whose stated mission is "protecting consumers and competition by preventing anticompetitive, deceptive, and unfair business practices through law enforcement, advocacy, and education without unduly burdening legitimate business activity," was established in 1914 the passage of the Federal Trade Commission Act. One of its stated strategic goals is to protect consumers from unfair and deceptive practices in the marketplace. It has powers to administer consumer protection laws, including industry-wide trade regulation rules and the Equal Credit Opportunity Act [11].

According to a GAO report, since 2008, FTC has settled 17 enforcement actions against CRAs related to consumer reporting violations of the FCRA. However, the FTC does not have civil penalty authority for violations of requirements under the GLBA, which, unlike FCRA, includes a provision directing federal regulators and FTC to establish standards for financial institutions to protect against any anticipated threats or hazards to the security of customer records. To obtain monetary redress for these violations, FTC must identify affected consumers and any monetary harm they may have experienced. However, as previously discussed, harms resulting from privacy and security violations can be difficult to measure. They can occur years in the future when hackers eventually decide to use the stolen data, making it difficult to trace particular harms to specific cybersecurity breaches. As a result, the FTC lacks a practical enforcement tool for imposing civil monetary penalties that could help deter CRAs, from violating the data security provisions of GLBA and its implementing regulations.

3.2.2 CFPB. The CFPB, which was created in response to the financial crisis of 2007–08 and the subsequent Great Recession, was established under the Dodd-Frank Wall Street Reform and Consumer Protection Act for consumer protection in the financial sector. Since its inception, the agency has been employing technological instruments to keep financial entities dealing with consumers under careful observation and track how financial entities use automated algorithmic tools to target consumers[2].

Even though it is the position of the CFPB that it "was created to provide a single point of accountability for enforcing federal consumer financial laws and protecting consumers in the financial marketplace" [4]. It is unable to prosecute this mandate effectively. One of its mandates is "rooting out unfair, deceptive, or abusive acts or practices by writing rules, supervising companies, and enforcing the law." The CFPB is also responsible for supervising larger CRAs. Large CRAs are those enterprises with more than $7 million in annual receipts from consumer creditworthiness reporting. However, the CFPB lacks the data needed to identify all CRAs that meet this threshold. Consequently, according to a GAO report, since 2015, the Consumer CFPB has only had four public settlements with CRAs for alleged violations of FCRA. The alleged violations included unfair, deceptive, or abusive practices. The CFPB also too narrowly views empowering consumers as the ability of consumers to navigate their financial choices and shop for the deal that works best for them. There is little that is empowering in the case where the options are effectively suboptimal choices and deals for the consumer or where the strong arm of CRAs leaves consumers with little choice as to what happens when their private information has been breached [4].

There is recognition that there needs to be legislative reconciliation to make comprehensive governmental mechanisms in law to protect the cybersecurity and privacy of US consumers. Legislative efforts are attempting to reconcile discordances and disunities of laws and authorities at the federal level.

4 DOMESTIC LEGISLATIVE EFFORTS

The primary federal laws governing the personal information that CRAs hold has led to significant conflicts among statutes and has adversely impacted how agencies implement and enforce them. The Courts have not developed novel approaches to resolving the inconsistencies and conflicts in a manner that harmonizes statutes while concurrently enabling the protection of consumers. However, legislative efforts have attempted to reign in some amount of perversity in the application and use of the powers and the legislative intentions of the FCRA and GLBA protection of consumers.

4.1 Data Breach Prevention and Compensation Act:

In May 2019, Senators and Representatives of the House reintroduced the bicameral Data Breach Prevention and Compensation Act intending to hold large credit reporting agencies accountable for cybersecurity breaches involving consumers' private data. The bill, if passed, would establish an Office of Cybersecurity at the FTC, empowered to conduct annual inspections and supervision of cybersecurity at CRAs. Further, the bill would allow for the imposition of liability penalties for breaches involving consumers' private data. The penalties would begin with a base penalty of $100 for each consumer who had one piece of personal identifying information (PII) compromised. Another $50 for each additional PII was compromised. In practical terms, the bill would have required Equifax to pay a $1.5 billion penalty for the breach of its systems due to their failure to protect consumers' private data. The bill aims to compensate affected consumers by enabling the FTC to direct up to 50% of the penalties levied against CRAs to the victims of data breaches. The bill also attempts to rectify the externalization of business risks that the CRAs shift onto powerless consumers by increasing the penalties to be paid in the cases of deplorable cybersecurity posture or in the case where a CRA's system has been breached but fails to notify the victims and the FTC of the breach promptly. Another important requirement of the bill would be to shore up the authorities of the FTC by empowering the FTC to levy civil penalties pursuant to the GLBA [26]

4.2 Corporate Executive Accountability Act:

In April 2019, Senator Warren introduced the Corporate Executive Accountability Act, which aims to make executives of large corporations accountable by holding them criminally liable if their enterprises commit crimes or civil violations that cause harm to large numbers of people. The bill would make leaders of corporations accountable for their enterprise's violations if the violation "affects the health, safety, finances, or personal data of 1% of the American population," which is likely to have the effect of stronger due diligence on the part of the executives in averting such violations. Further, the bill would create a permanent investigative unit within the Department of Treasury to conduct financial crimes investigations by repurposing the Special Inspector General to prosecute financial crimes. The bill aims to require executives at banks larger than $10 billion in market capitalization to certify that there has been no criminal conduct or fraud committed by any elements of the enterprise, thereby removing the veil of ignorance if malfeasance is found subsequently. It attempts to integrate the judiciary by putting deferred prosecution agreements under the purview of judges, with the aim of having judges ensure that such judge-supervised agreements are in the interest of the public. Although this bill is not limited to CRAs, it would impact the business climate and behavior of CRAs through their executives [14]

Even if these bills became laws, they would be insufficient to the task because they do not address the core of the problem, which is mainly the need for a more holistic approach to leveling the balance of power and increasing accountability of the CRAs through single national authority, such that their business model no longer relies heavily on externalities based on shifting business risk onto consumers who are not customers of the CRAs. The French seem to have elements of this approach implemented or in promulgation.

5 THE FRENCH APPROACH

The French believe that "the fundamental instruments of sovereignty are already indistinguishable from the tools of technological power." To that end, they have taken advantage of the GDPR European legislation to expand the mandate for protecting its citizens from what they consider cybermalevolence, which includes excessive exploitation of personal data [21].

5.1 Leverages the GDPR

The French National Commission on Informatics and Liberty (CNIL) leverages provisions within the GDPR to ensure that Databrokers do not fraudulently or surreptitiously collect or curate private information. CNIL was established and derived its authority from the enactment of La Loi Informatique et Libertés, known as the Data Protection Act (DPA)[13]. DPA specifies the national leeway of the

French concerning its ability to enforce the safeguards authorized by the GDPR, and CNIL is the single national data protection authority through which the French seek to protect its citizens from privacy exploitation.

5.2 Rebalanced Relationship

Article 1 of the DPA centralizes technology to the service of each person. The idea is to rebalance the relationship between the individual and the data controllers/brokers. Article 38 stipulates that any natural person is entitled, on legitimate grounds, to object to the processing of any data relating to herself. Further, a natural person is entitled to object, at no cost to herself, to the use of the data relating to herself for canvassing purposes, particularly for commercial ends. In the European Commission's draft Data Governance Act, the spirit of centralizing the fundamental rights of data protection, privacy, and property of the consumer and her is enshrined. The Act, as clarified in the explanatory memorandum, defines data broadly as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording." The memorandum goes on to state that "the measures are designed in a way that fully complies with the data protection legislation, and actually increases in practice the control that natural persons have over the data they generate" [8].

5.3 Categorically Broader Approach

The French interpretation results in a categorical and broader approach to capture the instances of privacy definitions and infringement. The French approach brings clarity and responsibility for the Data brokers. In other words, there is more accountability and less bureaucracy to hide behind, and there are other requirements of the CRAs that have to be implemented to demonstrate they comply applicable elements of the GDPR. Further, they have a single unified national body that provides a one-stop-shop with sufficient authority to enforce the accountability or the infringement of rights of individuals.

5.4 Single National Data Protection Authority

Article 44 of the DPA empowers the CNIL to supervise the implementation of personal data processing protection mandates. The Article allows for all supervisory functions at any place, premises, surroundings, equipment, or buildings used for processing consumers' personal data [13].

5.5 Supervisory and Enforcement Authority

Article 34 gives CNIL the power to dictate, to some extent, the technical requirements a Data Broker must have in place to remain authorized to broker consumers' personal information. The Article stipulates that the data controller shall take all useful precautions regarding the nature of the data and the risks of the processing, preserve the security of the data and, in particular, prevent their alteration and damage or access by non-authorized third parties. It further states that decrees taken upon an opinion of the CNIL may determine the technical requirements of data brokers, including their systems' requirements [13].

5.6 Accountability and Penalties

Article 45 of the DPA allows the "Formation Restreinte" a committee of CNIL to issue an injunction to an offending enterprise to cease the processing, which can have the effect of stopping an enterprise from continuing to engage in the violating activity, even if the activity is, as a matter of routine business processes, a core function upon which the enterprise relies. Similar to the reintroduced Data Breach Prevention and Compensation Act of the US Congress, Article 45 allows for the imposition of a financial sanction under the conditions provided in Article 47. In concurrence with the introduced Corporate Executive Accountability Act of the US Congress, Article 45 of the DPA states that offenses against the Act's provisions are punishable and sanctionable by Articles of the French Criminal Code, which includes imprisonment and fines [13].

5.7 Deficits of the French Approach

However, the continuous interactions with the consumers on each data processing activity amounts to a burden on consumers. Further, for the consumer to be an informed participant, it relies on a certain level of familiarity with data and technology, which is usually not widespread across the population of consumers. Hence, the preferred approach when adopting European or French approaches would be a categorized approach to consent rather than the approach where individuals have to consent to each request to use/collect private information. Further, simply identifying what might be legislative solutions is not a practicable and enduring solution to the problem. The main obstacle to improving US individuals' privacy is not that American legislators do not know what to do. Rather, the legislative climate and economic incentive structures that we hold dearly complicate the approach we might take to enact effective legislation. One among many complicating factors is the different legal frameworks between both countries.

6 BARRIERS AND CHALLENGES

Simply identifying what might be legislative solutions is not a set of practicable solutions to the problems. Some other barriers and challenges would stand as obstacles to promulgating legislation to improve US consumers' privacy and balance of power concerning their data brokers. Legislative landscapes and economic incentive structures complicate the approach we might take to enact effective legislation. Some of the significant barriers and challenges to transplanting legal frameworks into the US system include the US's cultural, electoral, legislative, constitutional, and judicial landscape.

6.1 Electoral-Legislative Landscape

For many reasons, including its provenance and history, most legislators of the US have preferred what can be termed as the economic sectoral approach to addressing the protection of its constituents' private information through legislative action. Essentially, the approach relies on a combination of least interventional legislation that empowers minimalist governmental regulation and significant deference to the particular private industry's sectoral self-regulation. The US rarely has any sector of its economy that is exclusively under governmental regulation. Rooted in the American laissez-faire economic ideologies, successive federal administrations have been staunch proponents of frameworks that foist the

private sector as leaders in crafting, implementing, and enforcing self-regulation in reaction to the various emergent technological advancements.

6.2 Cultural and Constitutional Landscape

The First Amendment to the Constitution of the United States, which forbids Congress from abridging the freedom of speech of individuals or the press, is viewed as pivotal and is used to limit governmental intervention in the affairs of private individuals, including exchanges between private enterprises and consumers [22]. According to the Supreme Court ruling in *Stanley v. Georgia*, the First Amendment to the Constitution of the United States protects against governmental intrusions into individuals' privacy [15]. This notion has been extended into the realm of interactions between private individuals. Exceptions are, however, granted, for example, for wire-tapping, but with a court order. Nonetheless, while freedom of speech is explicitly constitutionally enshrined, privacy is only implicitly guaranteed by the Constitution and is seen mainly as a protection from the intrusion of the government and not of other private individuals.

6.3 Legal Structure and Judicial Landscape

6.3.1 Common-Law Systems. One of the complicating factors is the different legal frameworks between both countries, that is the US and France. The US has a common law structure [28]. Common law uses case law as its basis. Judges read the law and apply the law on a case-by-case basis, and in so doing, provide greater detail and explanation of how the law applies. The detailed explanation of a decision is an opinion from such an appellate judiciary, which becomes a precedent. Current judges read the past decisions and base their decisions on precedent, and lawyers read the same decisions of the past and base their arguments on those precedents. If there is no precedent, then the judge's decision becomes precedent. In effect, judges are the ones who determine the meaning of legislation in individual cases; they interpret the law. Consequently, it means the laws are subject to contemporary interpretations. In fact, the ability to change or evolve the law into an ever more just system is the main strength of common law system. Common-law countries, like the US usually elect local judges by the people, which in turn places the onus in the people to elect wise and just jurists.

6.3.2 Civil-Law Systems. In a civil law system, pervasive in Europe and applicable in France, courts of law make decisions based on the codified law, not on previous decisions. Civil law relies heavily on the statutory law or the complication of the rules themselves, rather than an individual judge's interpretation. Hence, there is less precedential value that contributes to a judge's decision. Judges have no power to change or adjust an unjust law based on contemporaneous circumstances that require modification of the law, as would be the case in a common-law structure. In a case requiring modifications to the law, the judge will defer to the legislative body. Civil law is inflexible in the case where there is an immediate need for new legislation. Civil law can and is changed frequently as new regimes assume power and legislate according to the will of their electors. In the US, succeeding administrations have less comparative power to change the judicial landscape in the rapid way changes can be brought about in the civil law system. Judges and precedent usually precede and endure beyond the tenures of successive administrations and rarely depend on the particular disposition of any current administration.

Further, in line with this view, Solove and Citron [27] demonstrated in their work that Courts have ruled inconsistently in lawsuits about data breaches. Most Courts have dismissed lawsuits alleging harms due to data breaches for the failure of the plaintiffs to establish the alleged harm. Since harm is central to the standing of plaintiffs, it is pivotal that plaintiffs be able to sufficiently establish that data breaches create a risk of future injuries, such as creditworthiness, employability, insurability, tenancy, or reputational damage, and that breaches cause them to experience anxiety about these impending risk. The majority of Courts only seem to accept the post-facto establishment of harms. Hence, the context and landscape of promulgation are significantly different and demand organic approaches to implementing imported ideas and legislation [30].

6.4 Historical Context

When it comes to American history, particularly concerning the relationship of the individual to the State, the State (the government) tends to err on the side of refraining from meddling in the affairs of private parties, which tends to ingrain a culture of every man for himself, which, in turn contextually paints the landscape of efforts to address the problem of lopsided power relationships in consumer private information handling. In contrast, Europe's extensive GDPR is a privacy regulation rooted in its history. Its recent history indicates why many European countries have sought to strengthen individual privacy rights far more than has been the case in the United States. Fascist governments and post-War Communist regimes of the recent past have exercised widespread abuse of power in their use of private information, though those were by public/governmental entities [32].

Nonetheless, the recent sentiment of dossiers being compiled is reminiscent of the collection of secret government information files that Fascist regimes used to commit crimes against humanity. This sentiment has translated into a distrust of Corporations collating databases of dossiers, which resulted in many governments of European countries taking action to protect Individuals' private information from potential abuses by private and public entities alike. This is evident in the comprehensive data protection laws enacted after World War II by the French and Germans [31]. However, in order to avoid having to import European values and principles that are inconsistent with American ones, it will be necessary to rely on American industrial actors and legislators who will be able to develop the comprehensive industrial norms and standards consistent with American ideals. It means the solutions and recommendations need to take into account the cleavages of the American polity and legislative landscape in order to have a chance of being successfully enacted.

7 OPPORTUNITIES AND RECOMMENDATIONS

7.1 Legislative Actions

On the legislative front, it appears that having a single unified national body that provides a one-stop-shop with sufficient authority

to enforce the accountability or the infringement of rights of individuals will be more effective than a diffused group of proponents for individual rights.

7.1.1 Proper Authorities through Legislation. There should be law promulgated in line with the GAO recommendation that Congress consider giving FTC civil penalty authority to enforce GLBA's safeguarding provisions. Such a bill will reign in abuses considerably as CRAs will face the clear option of either putting a good faith effort toward securing consumers' personal information or facing strict consequences in the absence of good faith effort. The GAO's recommendation that the CFPB identify additional sources of information on larger CRAs, and prioritize examining how it assesses CRA data security posture is another critical path to empowering consumers in relation to the CRAs [24].

Legislation should be enacted that imposes mandatory, strict liability penalties for breaches involving consumer data, beginning with a base penalty higher than the $100 suggested by the Data Breach Prevention and Compensation Act for each consumer who had one piece of personal identifying information (PII) compromised. A correspondingly higher penalty than the $50 should be levied for each additional PII compromised. The consequence should be such that such wanton neglect that results in such a breach could cost so much that the enterprise involved might come close to ceasing to exist due to penalties levied consequent to violations of law that result in breaches or the failure to protect personal information.

7.1.2 Unified Effort through Legislation. When it comes to a single law for strengthening the oversight of CRAs, practically, what is likely to happen is a gradual evolution into a national data protection and data privacy regulation similar to Europe's GDPR, but with some distinct differences, particularly with regard to the monotonous consenting processes by individuals. It would be more practical and effective if promulgated bill would be embody a categorized approach to consent rather than the monotonous approach to consent mandated by the GDPR.

7.1.3 Courts Should Recognize Risk and Anxiety as Harms. The American legal system needs to confront data-breach harms because individual consumers and society bear real costs. Ignoring the costs results in an inefficient deterrence effect on credit reporting corporations' behaviors, which rely on externalizing business-related risks onto individual consumers as part of their business model.

Court rulings have demonstrated that the Courts have had difficulty accepting the argument: that future risks resulting from data breaches cause harm to plaintiffs [27]. Harms from data breaches are manifested when victims experience anxiety about the increased risk of future harm resulting from unauthorized possession of their private data that identity thieves can then use. The anxiety is experienced because victims know that identity thieves can use this personal information to the victim's detriment. Such detriments are instantiated in the future as losses to the victim's creditworthiness (inability to access credit from lenders), employability (pejorative information in the record as a result of someone else's activity, but attributed to the victim, resulting in lost employment opportunities), insurability (health and medical information that would otherwise not be taken into consideration resulting in increased premiums or denial of coverage), tenancy (adverse tenant screenings resulting in lost residential opportunities), and reputational damage (embarrassing or reputation-damaging information otherwise kept private by the victim). Prospective plaintiffs suffer future risks that entail real harm and emotional distresses. Further, these harms may only materialize well after applicable statutes of limitations, which might vary for each victim.

7.1.4 Interactions between Legislators and Industry. And on the technical front, there needs to be better liaising between industry and legislation. Because of rapid technological advancements that often results in a different understanding of where boundaries of privacy lay, as well as unforeseen consequences and issues of privacy that were never expected to be confronted, there need to be the ability to respond to changing landscape and innovate and take intelligent risks. Hence, there needs to be some frequent periodicity for looking at contemporary definitions of privacy in light of emergent technological advancements. For example, big data analytics is now able to reveal private information that once was thought to be anonymous in released datasets. An archaic definition of data will be under serving. Europe's emerging Data Governance Act has a broad and evolving definition of data that takes into account technological advances and how that might affect what is considered attributable data. So, it is important to understand that because technology moves at a rapid pace in some spheres, legislative efforts may need to keep up with some degree of rapidity, otherwise there will be too much room for exploitation in those spaces of time when legislation lags [29].

8 CONCLUSION

The federal government of the United States is lagging in its efforts to reign in the worst impulses of capitalism, particularly with regard to the regulation of financial institutions. Institutions like CRAs have taken advantage of the excessively permissive business environment by shifting business risks and costs onto consumers. There continues to be cybersecurity breaches, including at CRAs, that jeopardize consumers' private information, however, little recompence is being allotted to rectify the cybersecurity postures of these CRAs so that they are more robust to cyber attacks. And even in the event of loss of private information, due tot he negligence of the CRAs, the victims, that is the consumers whose private information is now in unauthorized hands have little options. Efforts around the world to rectify the individual consumers' with relationship with corporations like CRAs have the potential to be effective at curbing abuses. The French government's approach allows for fine-detailed interjections into the workings of these relationships. Several elements of the French approach will work in the United States, however, the elements have to be Americanized before they can be implemented.

ACKNOWLEDGMENTS

Thanks to Professor Joan Feigenbaum; Teaching Fellow: Anat Lior, CPSC 610 –Topics in Computer Science and Law. My gratitude also to Titilayo Ogunyale.

REFERENCES

[1] 106th Congress Public Law 102. 1999. *Gramm–Leach–Bliley Act.* Retrieved May 14, 2021 from https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

[2] 111th Congress Public Law 203. 2010. *Dodd–Frank Wall Street Reform and Consumer Protection Act.* Retrieved May 14, 2021 from https://www.govinfo.gov/content/pkg/PLAW-111publ203/html/PLAW-111publ203.htm

[3] Donald J Boudreaux and Robert B Ekelund Jr. 1992. Cable Television Consumer Protection and Competition Act of 1992: The Triumph of Private over Public Interest. *Ala. L. Rev.* 44 (1992), 355.

[4] Consumer Financial Protection Bureau. 2010. *The Bureau.* Retrieved May 14, 2021 from https://www.consumerfinance.gov/about-us/the-bureau/

[5] Michael Carlin and Ellen Frick. 2013. Criminal records, collateral consequences, and employment: the FCRA and Title VII in discrimination against persons with criminal records. *Seattle J. Soc. Just.* 12 (2013), 109.

[6] Electronic Privacy Information Center. 2020. *Equifax Data Breach.* Retrieved May 14, 2021 from https://epic.org/privacy/data-breach/equifax/

[7] Young B Choi, Kathleen E Capitan, Joshua S Krause, and Meredith M Streeper. 2006. Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *Journal of medical systems* 30, 1 (2006), 57–64.

[8] European Commission. 2020. *Data Governance Act.* Retrieved May 14, 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767&from=EN

[9] Federal Trade Commission. 2014. *Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission.* Retrieved May 14, 2021 from https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014

[10] Federal Trade Commission. 2020. *Equifax Data Breach Settlement.* Retrieved May 14, 2021 from https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

[11] Federal Trade Commission. 2021. *About the FTC.* Retrieved May 14, 2021 from https://www.ftc.gov/about-ftc

[12] Experian. 2015. *Data Breach T-Mobile Facts.* Retrieved May 14, 2021 from https://www.experian.com/data-breach/t-mobilefacts

[13] RÉPUBLIQUE FRANÇAISE. 1978. *Information Technology, Data Files and Civil Liberty.* Retrieved May 14, 2021 from https://www.cnil.fr/fr/la-loi-informatique-et-libertes

[14] Senate Judiciary. 2019. *Corporate Executive Accountability Act.* Retrieved May 14, 2021 from https://www.congress.gov/bill/116th-congress/senate-bill/1010

[15] Al Katz. 1969. Privacy and Pornography: Stanley v. Georgia. *The Supreme Court Review* 1969 (1969), 203–217.

[16] Oliver J Kim. 1999. The Driver's Privacy Protection Act: On the Fast Track to National Harmony or Commercial Chaos. *Minn. L. Rev.* 84 (1999), 223.

[17] Congress Public Law. 2003. *Fair and Accurate Credit Transactions Act of 2003.* Retrieved May 14, 2021 from https://www.ftc.gov/enforcement/statutes/fair-accurate-credit-transactions-act-2003

[18] Congress Public Law. 2018. *Fair Credit Reporting Act.* Retrieved May 14, 2021 from https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act

[19] Marc Chase McAllister. 2017. Modernizing the Video Privacy Protection Act. *Geo. Mason L. Rev.* 25 (2017), 102.

[20] Agence nationale de la sécurité des systèmes d'information. 2015. *French National Digital Security Strategy.* Retrieved May 14, 2021 from http://www.souverainetenumerique.fr/institute-digital-sovereignty-isn-and-afnic-publish-internet-things-digital-sovereignty-report

[21] The Institute of Digital Sovereignty. 2021. *Internet of Things Digital Sovereignty.* Retrieved May 14, 2021 from http://www.souverainetenumerique.fr/institute-digital-sovereignty-isn-and-afnic-publish-internet-things-digital-sovereignty-report

[22] Congress of the United States. 1791. *First Amendment to the United States Constitution.* Retrieved May 14, 2021 from https://constitution.congress.gov/constitution/amendment-1/

[23] Government Accountability Office. 2018. *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* Retrieved May 14, 2021 from https://www.gao.gov/products/gao-18-559

[24] Government Accountability Office. 2019. *Consumer Data Protection: Actions Needed to Strengthen Oversight of Consumer Reporting Agencies.* Retrieved May 14, 2021 from https://www.gao.gov/products/gao-19-196

[25] European Parliament. 2018. *General Data Protection Regulation.* Retrieved May 14, 2021 from https://gdpr-info.eu/

[26] House Financial Services. 2019. *Data Breach Prevention and Compensation Act of 2019.* Retrieved May 14, 2021 from https://www.congress.gov/bill/116th-congress/house-bill/2545?s=1&r=8

[27] Daniel J Solove and Danielle Keats Citron. 2017. Risk and anxiety: A theory of data-breach harms. *Tex. L. Rev.* 96 (2017), 737.

[28] Harlan F Stone. 1936. The common law in the United States. *Harv. L. Rev.* 50 (1936), 4.

[29] Zhaohao Sun, Kenneth David Strang, and Francisca Pambel. 2020. Privacy and security in the big data paradigm. *Journal of computer information systems* 60, 2 (2020), 146–155.

[30] André Tunc. 1975. Methodology of the Civil Law in France. *Tul. L. Rev.* 50 (1975), 459.

[31] Olivia Waxman. 2018. *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History.* Retrieved May 14, 2021 from https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/

[32] Ernst-Oliver Wilhelm. 2016. A brief history of the General Data Protection Regulation. *Retrieved February* 17 (2016), 2018.