Old Policy, New Tech:
Reconciling Permissioned Blockchain Systems with Transatlantic Privacy Frameworks

By Remy Hellstern and Victoria Lemieux

Introduction

The world is organized in a centralized manner. We have a central body that governs the rules of society and a central bank that dictates the transfer and flow of money. This centralized system is traditionally how we have organized the world and based much of the legal and regulatory system on. However, these systems are becoming increasingly more problematic for users due to lack of transparency within privacy agreements and limited autonomy over individuals' personal information. Personal information is seen as an asset that can be bought and sold as opposed to the right of an individual to possess, share, and own. In 2008, Satoshi Nakamoto produced the Bitcoin whitepaper which ushered in an era of change for these traditional centralized systems. Through peer-to-peer systems, individuals no longer needed a third-party intermediary to establish trust.

This evolution could not have come at a better time. As a result of the 2008 financial crisis individuals lost trust in financial institutions and government agencies (Uslaner, 2010). At this time, blockchains and decentralized systems had yet to explode in popularity. However, mistrust in institutions accelerated by the financial crisis laid the groundwork for individuals to have interest in alternatives to these centralized systems. While this mistrust was growing, so was social media. The year 2008 was also the year Myspace surpassed one million users per month, ushering in the era of social media dominance (Ortiz-Orpina, 2019). However, with the proliferation of these firms, it became increasingly more difficult to regulate the tech industry (Raval, 2019). Individuals were left to manage their own privacy, and even the most technically savvy people were unable to stay informed on the data use, collection, and storage policies of these companies (Obar, 2019). This put policy makers in a bind as they were trying to be friendly to innovation while limiting the over-collection and unauthorized use of individuals' information (Furman et al., 2019). In many ways, regulation addressing these challenges was incredibly slow to come out, thus allowing the mass collection of personal information for years. As a result, a game of cat and mouse ensued where new regulations would come into place and firms would make small adjustments to be allowed to legally operate. While all of this was happening, decentralized and distributed systems were gaining popularity with the creation of systems like Ethereum and Hyperledger in 2015. Individuals started to realize they did not have to be married to the traditional centralized systems.

Distributed ledger and blockchain-based technologies are advantageous to firms with the rise of data breaches and need to store personally identifiable information. However, there are trade-offs associated with running and maintaining these systems, like start-up cost and energy cost associated with running servers. Regulators and policymakers should not be naive about the importance of this technology, the exponential growth we have seen, and the expected growth noted by those in the industry. The regulatory environment for global privacy standards is ever evolving and often lacks the nuance needed to incorporate all forms of new

technologies, much like decentralized systems. Companies are not aware of the specific requirements needed to comply with regulation, especially when there are a variety of policies at different levels of government. This makes it difficult for firms to design solutions to address problems created by traditional centralized systems, for example the bundling and selling of personally identifiable information.

This paper will explore the global conversation and consensus around data privacy regulation, with specific attention to the European Union and Canada. It will work to understand how blockchain-based firms situate themselves amid this regulation in relation to the storage of personally identifiable information by looking at relevant policy decisions, legal cases, and commentary from regulatory bodies and commissions. This paper will contribute to the larger academic realm by examining the current global state of data privacy policies, easing the communication gap between the public and private sectors, and providing policy recommendations for future work in this space. With increased communication and collaborations between private industry and governing bodies, the future of regulation can protect the rights of individuals and their data while simultaneously fostering innovation.

Understanding Network Structures

Approaching systems from this binary perspective lacks a nuanced approach to highly sophisticated technologies. Truthfully, these are complex systems that often need to be examined on a case-by-case basis to assess their architectures and associated strengths and vulnerabilities. Specific solutions can borrow aspects from centralized, decentralized, and distributed architectures. Many of these architectures share similar attributes, however, they also often deviate in significant ways. Understanding the differences among these systems will allow regulators to approach issues that arise and with the language needed to design regulation. Regulation should work to find a balance between supporting innovation in this emerging technology space while simultaneously supporting the rights of citizens and figuring out how these rights operate in an online environment.

The following section will provide a high-level overview of *centralized, decentralized, and distributed* (see Figure 1).

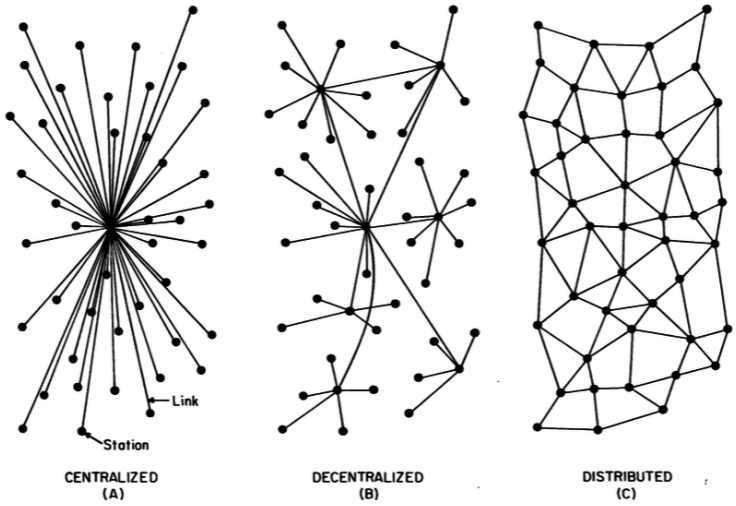

Figure 1: This illustration shows three different types of networks.
Source: *On Distributed Communications Networks* by Paul Baran

Centralized Systems

Centralized systems are the most common organization and system structures we encounter on a day-to-day basis. Any legacy system, government institution, and most private firms still rely on centralized systems to collect, process, and store information. A centralized system has one data controller and one location where all the information is kept. These systems tend to be characterized as being low maintenance, low in scalability, unstable, and having a single point of failure (Truong et. al, 2016). They are generally considered to be very low maintenance and easy to implement. However, they can be difficult to scale because there are challenges with long-term high volume storage. Also, these systems can be unstable because they have a single point of failure. Single point of failure refers to a system that relies upon the functioning of a single part, which, if it fails, causes the entire system to go down (Andriole, 2021). This leaves centralized systems vulnerable to attacks as bad actors only need to target one aspect or component of the system to put it at risk. However, there are benefits to using centralized systems, especially for non-sensitive information (e.g., as already mentioned, low cost to establish and quick to develop and implement).

Decentralized Systems

Decentralized systems deviate from centralized models as no one node controls the system. Instead, different nodes store information and operate independently of a centralized controller. Often decentralized networks distribute power equally among the nodes and there is no formal control over the system (Lemieux, 2017). These systems tend to be characterized as requiring moderate maintenance, moderate scalability, are fairly stable, and have finite points of failure (Truong et. al, 2016). Such systems need moderate maintenance because it is possible that some of the servers may go down. In a decentralized system not all nodes are connected with one another so it is possible if one server goes down, part of the system will

require maintenance (Berty, 2019). However, the system itself will continue to run as long as one server is functioning, making it a fairly stable network. These systems are relatively scalable because you can add new nodes to the network at any time but there are trade-offs with running a large, decentralized network. Lastly, because of the number of servers on the network, there are finite points of failure on the system making it resilient to attacks. However, they can be expensive to operate and require dedicated resources.

Distributed Systems

Distributed systems arose from the limitations of centralized and decentralized systems. While these systems share a similar structure to decentralized systems, they offer no centralization whatsoever while ensuring all nodes on the system have equal power. These systems tend to be characterized as requiring a high level of maintenance, unlimited scalability, are very stable, and have infinite points of failure (Truong et. al, 2016). Distributed systems are considered to be high maintenance because they are difficult to deploy due to the complex nature of these networks and have a high start-up cost. With these systems, there is unlimited scalability because once the network is established nodes can be added at will. This in turn makes the system very stable because as more nodes are added, the system becomes more robust and more reliable (Shah et. al., 2019). Lastly, this system has infinite points of failure because all nodes share ownership of data. Depending on the architecture of the system, specifically in private systems, some nodes may have more authority over others and are able to add or delete members. However, central to the core of the system is the idea that all nodes are equal players in the system.

Use Cases

The prior section highlighted an array of systems including centralized, decentralized, and distributed. This section will explore two use cases that leverage decentralized and distributed networks. When it comes to regulating new and innovative systems, policymakers struggle to establish a "one size fits all" approach. By using the concepts of centralization, decentralization and distribution to consider the similarities and differences of the following use cases, policymakers can create regulatory frameworks that are supportive novel technologies.

Private Blockchains and Distributed Ledger Technology

Blockchains have become a hot topic of discussion for cryptocurrency enthusiasts and individuals alike. However, when we look beyond the technology's ability to transfer cryptocurrency, these systems become a fascinating use case for recordkeeping and storage of information. The *International Organization for Standardization* (ISO) defines blockchains as "a distributed ledger with confirmed blocks organized in an append-only sequential chain using cryptographic links" (ISO, 2020, s. 3.6). Blockchains consist of a series of blocks that are chained, or grouped together, through hashes. Hash values are a result of cryptographic hash functions, essentially assigning a fixed string of numbers to data as a means to identify that information. As noted in the definition, this technology is a distributed ledger which the ISO defines as, "ledger that is shared across a set of [distributed ledger technology (DLT)] nodes and synchronized between the DLT nodes using a consensus mechanism' (Ibid, s. 3.22). To add new

information, or a block, to this ledger, it must go through a process called consensus. This is where nodes on the system will accept or reject the new block. As more blocks are added to the chain, the longer it gets, which makes the system more resilient. Blockchain and distributed ledger systems are unique because of cryptographic hashing, tamper-proofness, and consensus mechanisms (Tatar, Gokce, Nussbaum, 2020).

There are different types of blockchains: public, private, and hybrid. Depending on what type of blockchain you are using, the architecture and access of the system will be different (Walters, 2019). Public, permissionless blockchains are open to anyone with the ability to join the network. Often in public systems, all nodes have equal decision-making power. Ethereum and Bitcoin are two of the most prominent examples of public blockchains. Blockchain technology itself has a wide array of real world applications outside of cryptocurrency, including storing personally identifiable information. Permissioned blockchains are normally closed to a small group and require permission to join. Depending on the system design, it is possible that some nodes have more authority over others. Hyperledger, a protocol created by Etherum, is an example of a permissioned blockchain. Hybrid systems will be a mix between the two. It is possible that such systems are open to everyone to join; however, you still need permission to login to gain access to such systems. All blockchain systems are different based on design choices, but some similarities exist across systems such as an append-only ledger, verification process of records, and, generally speaking, allowing every node to have access to a full or partial replica of the ledger (Sharma, 2019).

Self-Sovereign Identity Systems

Self-Sovereign Identity Systems (SSI) differ from the standard blockchain and distributed ledger technology because inherently, “individuals have sole ownership and custody of their data and control how it is used” (Lemieux, et. al., 2021). The Sovrin Foundation articulates that the three main aspects of SSI are security, controllability, and portability (Tobin & Reed, 2016). The first aspect centers around the security of an individual’s personally identifiable information and focuses on protection of identity information, persistence in the up-to-date record keeping, and minimization of superfluous data. The second aspect, controllability, returns the power back to the users on the system and prioritizes their absolute control over who can see and access their information. Lastly, portability requires that individuals can easily move their SSI across platforms in a transparent and accessible manner. In *Path Towards Self-Sovereign Systems*, Christopher Allen outlines the steps that need to be taken to foster and grow SSI. Allen argues that on the path to SSI, there are four main phases: *centralized authority, federated identity, user-centric identity,* and *self-sovereign identity*. According to Allen, we are currently in the user-centric phase, where companies are recognizing the need to allow individuals to have some control over their online identity. User-centric models tend to focus on user-consent, often in the form of terms and conditions, and interoperability among large tech platforms. However, proponents of SSI like Allen posit that this still does not go far enough to protect individual’s right to privacy as well as right to identification. Within an SSI model, the most effective and meaningful way to store an individual's personally identifiable information is with the individual themselves. Tech platforms are ultimately a business first, thus prioritizing profit over protection.

In SSI systems, individuals' data is used to create a decentralized identity, which is solely owned and operated by the individual. Individuals can then use their decentralized identities, which are often represented in the form of verifiable credentials, to prove who they are for purposes of authenticating to systems in a very privacy-preserving manner. This is fundamentally different from centralized networks which require individuals to input usernames and passwords, and which can create the kind of “digital trails'' that leak private information about individuals. Moreover, because SSI systems do not capture and store information about individuals in order to authenticate to a system or use systems’ services, they do not rely on one data controller to maintain and keep safe personal data. In SSI, individuals are the creator, issuer, and verifier of their identification. In such systems, there is no need for a third party intermediary (ie. government agencies) to provide identification for individuals, instead this system reimagines how citizens can access and use their personal information. In this wider view, individuals would no longer need a centralized authority, like a government agency or organization, to create, issue, and verify identification. This will be challenging to reconcile in most current systems, in which government groups are the sole provider for forms of identification like driver’s licenses and personal health cards. As these systems begin to gain more popularity, regulators are going to have to address the long-term implications of SSI through policy recommendations (Hori, 2021). This includes whether or not governments will accept and work alongside decentralized identifiers and personal credentials issues on SSI systems.

While the world of decentralized and distributed technologies is vast, the remainder of this paper will focus on permissioned blockchains systems and best practices for compliance with current regulations in Canada and the European Union (EU).

Regulatory Models of Privacy Policy

As of 2021, according to the UN Conference on Trade and Development 137 out of 198 countries have data protection and privacy regulations in place (UNCTD, 2021). The global flow of data is becoming more relevant as the internet is expanding to more audiences than ever before, countries are being challenged with creating legislation to protect the privacy of their citizens. As countries are tasked with this, globally there are trends arising within these regulations. Danielle Olofsson identified four major regulatory models around the world including: *comprehensive, sectoral, self-regulatory,* and *co-regulatory* (Olofsson, 2021).

Comprehensive governance models focus on applying one regulation that applies to everyone and all sectors (IAPP, 2021a). These types of regulations tend to be long, inclusive documents that highlight key guidelines companies and institutions must follow to be compliant. Examples of this type of regulation include Canada’s *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the EU’s *General Data Protection Regulation* (GDPR).

Sector governance models take a more nuanced approach to regulation and deal with specific industries separately (IAPP, 2021c). This privacy model is most common in the United States as

different states have unique regulations regarding privacy, with many states lacking regulation entirely. This piecemeal approach means there are a range of policies at the state and federal level that at times can conflict with one another. This challenges corporations to be aware of the jurisdiction they are operating in. For example, in 2018 the *California Consumer Privacy Act* was passed thus protecting the privacy and consumer protection for individuals living in California. This regulation applies solely to the state and preempts federal regulation. However, for sensitive information like healthcare, federal regulations do apply.

Self-Regulatory governance models tend to focus on companies and institutions that fall outside of the purview of federal regulation (IAPP, 2021d). This often takes the form of regulation within the company itself and is then enforced by government agencies. Commonly referred to as fair trade practices, companies decide what works best for them, self-regulatory standards are approved by a federal agency which then enforces those rules. An example of this model would be Japan's *Act on the Protection of Personal Information* which establishes a third-party entity to enforce self-regulation of firms (Ishiara, 2019).

Co-regulatory governance models are similar to the self-regulatory governance model, except it accounts for group consensus (IAPP, 2021b). Instead of company specific privacy regulation, co-regulatory models encourage the industry itself to determine what the standards should be and then are enforced by an external body which regulates those standards. Co-regulatory models can exist within comprehensive and sectoral systems because they establish industry wide standards. An example of this would be Australia's *Communications and Media Authority* which establishes and shapes policy for the media sector in the country.

Adequacy Status

This paper will focus on exploring the impact of comprehensive governance models, specifically European and Canadian regulation, and on the development of blockchain-based firms developing solutions for storing personally identifiable information. Data sharing is a lucrative business. Estimates suggest that an individual's data is worth upwards of $500 per month to groups like Google and Facebook (Lazarus, 2020). This is just at the national level. When we account for buying and selling data across international jurisdictions for thousands of individuals, this becomes a multi-billion dollar industry.

This has caused lawmakers to pay attention to this rising industry and work to regulate the buying and selling of citizen's data across jurisdictions. As a way to ensure the privacy of citizens across international boundaries, the EU established an adequacy status (EU Commission, 2021). This status recognizes that while all countries will have different approaches to regulation, the EU is able to determine if non-EU countries have regulations with adequate data protection. This in turn, enables the EU to trade data with other countries around the globe. In 2001, Canada received adequate status for PIPEDA under the *Data Protection Directive* in the EU, which was later reaffirmed in 2006 (EUR-LEX, 2016a). However, with the creation of GDPR, some argue that PIPEDA is no longer on par with the EU's regulatory framework and therefore at risk of losing its status. After the creation of GDPR in 2018, Canada was given 4 years to

create regulations either on par or stricter than the EU's regulation to maintain their status. Canada provides semi-regular updates to the EU regarding their progress with the last report being in December 2019 (Government of Canada, 2019). In 2022, the EU is set to decide whether Canada will maintain its adequacy status. Hence the movement in Canada to update their privacy framework with provincial bills like Quebec's *An Act to modernize legislative provisions as regards the protection of personal information* (Bill 64), federal regulation like the *Digital Charter Implementation Act* (2020) and *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make related and consequential amendments to other Acts* (Bill C-11).

Understanding the General Data Protection Regulation

First introduced in 2016, the EU's GDPR replaced the *1995 Data Protection Directive*, ushering in an era of renewed interest in global privacy regulation (European Union, 2018). GDPR outlines guidelines for companies, institutions, and organizations for how to handle information and data of EU citizens. The articles range in topics from understanding the rights of a data subject to international data sharing to fines and penalties associated with data breaches. Many scholars have surveyed the articles of GDPR and potential impact these sections have on decentralized technologies (Rose 2019, Berberich & Steiner 2016). Some argue that distributed ledger systems are potentially irreconcilable with GDPR (McMahon, 2019) while others suggest innovative solutions can be found to ensure compliance (Walters, 2019, Zyskind et. al, 2015). The following section takes neither approach, and instead highlights key regulatory provisions firms should be aware of while designing their decentralized use case.

Defining the Terms

Article 4 of GDPR defines relevant terms found throughout the regulation. This section works to counter any misconceptions about terminology and phrasing used as well as offers clarity to firms looking to remain compliant. Key terms in this section that are relevant to firms in the decentralized space are personal data, pseudonymisation, and controller.

Personal data is defined as, "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Under this definition hash codes, public keys, private keys, metadata, and static and dynamic IP addresses are considered to be personal data. Many of these, specifically has codes as well as private and public keys, are relevant to decentralized storage solutions. All these pieces of information can provide linkability to a natural person thus making it personal data. For example by combining public and private keys to decrypt encrypted information there is a possibility these two sources could reveal an individual's identity. Therefore, even if the information is encrypted, it is not fully anonymized because it is possible to access the data with the correct keys. Regarding static and dynamic IP addresses, regulators worry that through

social network analysis, it is possible to identify individuals via their connections and communications with other individuals. According to the Privacy Office of Canada, social network analysis "involves creating a graph of the human network around any specific individual- analysts can identify everyone who is one or two degrees of separation from the individual of interest" (Office of the Privacy Commissioner of Canada, 2014, page 7). For example, in the *Breyer vs. Germany* ruling, the court found that if a dynamic IP-address is held by a known third party, it is considered personal information because it is possible to re-identify the individual (EUR-LEX, 2016b). However, if the data is, "rendered anonymous in such a way that the data subject is no longer identifiable, the GDPR would not apply" (Berberich & Steiner, 2016). This is relevant for firms to keep in mind as they are designing their systems. Private blockchains offer some protection as the ledgers are not publicly available. However, firms will need to assess the safeguards they are putting into place to protect the information in order to be compliant with the regulation.

Pseudonymisation is defined as, "…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (Article 4(5)). The idea is for companies to replace any possible identifiers with pseudonyms to guard against re-identification, which is becoming easier because of big data analytics techniques, and to protect the identity of an individual's information contained in a dataset. Under GDPR, the threshold of anonymity is very high. This was done purposefully, to ensure the protection and privacy of individuals and their data. If there is any chance that the information can be traced back to an individual identifiable person, the data has not been adequately pseudonymized.

Controller is defined as, "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (Article 4(7)). Under GDPR, there must be a clear, defined data controller that individuals, or data subjects, are able to identify. The data controller of a system determines the logistics of handling personal data processing. They are ultimately responsible for the system, overseeing the data processing, use, and collection. Under GDPR, it is possible to have joint controllers of a system. Article 26 defines joint controllers as, "when two or more controllers jointly determine the purposes and means of processing" this must be transparent with clearly defined roles and responsibilities. However, there is flexibility within the definition of controllership, whether there are single or joint controllers present in the system. In the 2014 Google vs. Spain court case, the ruling noted, "there is a need to adopt a broad definition of controllership to ensure the effective and complete protection of data subjects" (EUR-LEX, 2014). This decision suggests there is an ambiguous definition of data controller, which gives firms leeway in deciding how best to approach this article (Edwards et al., 2019). In the Solutions section of this paper, there will be an exploration of designating the company itself as the data controller. The issue of determining data controllers is often a difficult one in the

context of decentralized systems, because data controllers is a concept that has arisen out of the centralized systems (i.e., centralized storage, processing and management of data), whereas blockchains are usually decentralized and thus might have many organizations or individuals who participate in processing.

Understanding the Parameters of Personal Data

Article 5 focuses on the specifics of using personal data, highlighting some of the constraints, limitations, and boundaries of what can be collected. Under this article, personal data that is collected must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed" (Article 5(1)(c)). Personal data also must be "accurate and kept up to date" (Article 5(1)(d)). This is important for firms to be aware of as they are designing their systems. Essentially firms need to keep the data they are collecting to a minimum and maintain the data as accurately as possible. Ideas from this article allude to purpose specification, similarly found within Canada's PIPEDA, which requires the data collector and processor to identify which data they will be using, how they plan on using it, and subsequently only use the data in that manner (Nissenbaum, 2016). However, this principle can be difficult to maintain with a blockchain-based system due to the characteristics and specifications of these systems. This specifically refers to the append-only nature of most blockchain systems as the database grows with time and it is difficult to remove data once it has been added to the chain. Researchers have suggested that there may be workarounds to this which will be further discussed in the Solutions section of this paper. It is also difficult to define the purpose of the data processing because in a blockchain-based system the data goes through multiple processes including associating a public key with the data, storing the data on the blockchain, and having the nodes reach a consensus when new blocks are added. This article reinforces the idea that firms need to have data minimization in mind while designing their systems.

Transparent communications

Article 12 outlines the rights of individuals, or data subjects, to request information about the data firms are holding regarding them. It highlights the responsibilities of data controllers to provide this information in a "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12(1)). Firms need to be cognizant of these requirements while storing personal data. Conversely firms do have the right to charge or deny access to some data if the request is "unfounded or excessive… the controller may either 1) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or 2) refuse to act on the request" (Article 12(5)). The onus is on the firm to prove that these requests are "unfounded or excessive".

Right to Access

Article 15 outlines the rights data subjects have to access their information, specifically whether or not their data is being processed and how. Section 1 highlights areas in which an individual

has the right to ask or seek confirmation about the usage, storage, and processing of their data. Article 15(1)(d) ensures that individuals have the right to know how long their data will be processed and stored. This can create difficulties for firms as blockchain-based systems can store their data indefinitely. If this is something the individual is aware of, there is a lesser likelihood of compliance issues, however the individuals' rights on the system must be communicated in a clear and transparent manner.

Article 15(2) entitles individuals to know when their data is being transferred or processed in different countries or other international organizations. This section tried to establish jurisdictional boundaries to data processing. When an individual's data is processed in a third country or by an international organization, the data subject has a right to know the safeguards in place to protect their information. Article 46 explores the safeguards companies must follow when participating in data transfers across jurisdictional boundaries. This creates some challenges for firms as they would need to be aware of the location of all the nodes on their blockchain system. Each node contains a copy (or partial copy) of the distributed ledger and therefore could be deemed a data processor that is potentially outside of the geographical location of the firm.

Article 15(3) gives individuals the right to obtain copies of their personal data while it is being processed. Given that data is cryptographically encoded on a blockchain and intentionally pseudonymized it can be difficult, or even impossible, to collect all information associated with one individual. This can be a time intensive process, especially if more than one individual is requesting copies of their personal information. Currently, it is unclear how this article will impact the operation of data centers by cloud service providers and permissioned blockchains. Presumably they would know of all their data centers which would allow them to track down the information needed to be compliant with this article. With a permissioned blockchain, nodes would have identities attached to their data since they must be authenticated to the network allowing the firm to access the necessary information. However, this would be difficult for a permissionless blockchain where nodes can come and go in a fairly anonymous manner.

Right to Modification

Article 16 gives individuals the right to request their information to be changed or updated. Firms have an obligation to rectify the information in a timely manner as a response to the request. This is a point of contention for firms operating in the blockchain space because traditionally blockchain is associated with immutability. This limits the ability of the firm to correct or modify data. However, this is oftentimes dealt with by recording an updated transaction that links back to the previous, outdated transaction as an update. This, along with the usage of chameleon chains, will be explored in the Solutions section. Ultimately, there are no clear parameters established around "the rectification of inaccurate personal data" leaving best practices around modification ambiguous (Article 16(1)).

Right to Erasure and Right to be Forgotten

Article 17 aims to discuss an individual's right to delete or erase personal information held by firms without delay for several reasons including but not limited to lack of necessity, withdrawal of consent, unlawful processing, etc. Article 17(1) and Recital 66 outline all the reasons for erasure according to GDPR. This article and recital have been of particular interest for scholars regarding practical implementation on blockchain-systems. Many have argued that this article is irreconcilable on private blockchain systems, unless there are structural changes or additions to the network (Jurdak et al., 2019). However due to the lack of concrete definitions surrounding erasure and forgetting, there are possible solutions pertaining to Article 17. Article 17(2) focuses on what it means to delete or erase personal information that has been made public. This article requires controllers to research all available technologies and the associated cost of deleting personal information upon the request of data subjects. However, erasure is never clearly defined under GDPR. Therefore, it is subject to interpretation and could mean something other than absolute deletion or complete erasure. At the time of writing of this paper, there has been only one major court ruling regarding the right to be forgotten by the French authority, *National Commission on Informatics and Liberty* (CNIL) (Kelion, 2019). In a case against Google, CNIL ruled to comply with Article 17 that right to delete does not necessarily mean absolute, permanent erasure (Samonte, 2020). Scholars have suggested that for private, permissioned blockchains destroying the private key in a controlled setting would allow system operators to achieve the equivalent of deletion of data because that information would no longer be accessible; in other words, it affords a de facto right to delete (Daoui et al., 2019).

Protection by Design and Default

Article 25 requires firms to "design to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." Privacy by design makes it essential for firms to center the protection of individual's personal data in the design of their system. Prior to this regulation, there were no strong privacy constraints on the design of systems. This article works to guarantee that the privacy of an individual's data is of the utmost priority for a firm when designing new systems.

Understanding the Personal Information Protection and Electronic Documents Act (PIPEDA)

Canadian regulators have been aware of the importance of data privacy regulation for years. When first introduced in 1983, Canada's Privacy Act was seen as progressive legislation (Office of the Privacy Commissioner of Canada, 1983). Predating the rise of Google and Facebook, this regulation worked to balance the needs of the general public and private firms (Geist, 2018). However, despite the strong start, Canada lagged in updating the regulation for years. In 2000, Canada updated their privacy framework introducing the PIPEDA. This regulation established ten fair information principles for firms and organizations to adhere to while processing data. These principles are: *accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and*

compliance. At the time of its passage, PIPEDA was one of the boldest data privacy frameworks that existed. In some ways we can see how the OECD modeled their privacy principles after that of PIPEDA. This section will examine the ten major principles of PIPEDA and subsequently explore how it is expected to impact the future of Canadian regulation within this sector.

Accountability

The accountability principle requires organizations to be "responsible for personal information under its control [and] appoint someone to be accountable for its compliance with these fair information principles." The focus of this principle is to appoint an individual at the firm to control and oversee the processing of data. By assigning an entity to control the data, the idea is that if there is a data breach an individual or group can be held accountable. This principle falls in line with the GDPR Article 4(7), or the role of data controller. Principles and articles like the one aforementioned allude to the challenge governments are facing when it comes to trying to regulate the control, flow, and processing of data within private firms. Ultimately this traditional approach assumes that individuals are not in control of nor accountable for their personal information on corporate systems, which has been the case in the world of traditional centralized systems. However, with decentralized and, in particular, SSI systems there is a possibility for the users to control their own information thus giving the power of data sharing to the individual as opposed to the firm.

Identifying Purposes

The identifying purposes principle requires that firms "identify and document [their] purposes for collecting personal information.. [and] why your organization needs their personal information before or at the time of collection… [and] obtain [data subject's] consent again should you identify a new purpose". Similar to ideas of purpose specification, found in Article 5(1)(c) and (d) of GDPR, firms must identify the reason they are collecting data, how long they will be holding that data, and what they plan on using that data for. This principle works to create more transparency between the data subject and the firm. If firms wish to use data for a purpose outside of what was originally agreed upon, often through terms and conditions, they must reobtain consent from the data subjects. Regulators have come to realize the danger of firms collecting massive amounts of data points on individuals and the need to regulate these industries. One of the most notable events which shed light and renewed interest on this issue was the 2015 Cambridge Analytica and Facebook scandal (Confessore, 2018). Facebook was found to be collecting, bundling, and selling the data of individuals on their platform (Chaykowski, 2018). This resulted in hours of testimony to the US Congress, the ushering in of regulations like the California Consumer Privacy Act, and global interest in the repercussions, or lack thereof, Facebook would face.

Consent

The consent principle outlines what meaningful consent is and how "people must understand what they are consenting to… [and that] customers will understand the nature, purpose and

consequences of the collection, use or disclosure of their personal information". Consent must be free, informed, and retractable at any time throughout the collection, processing, and use. There are few exceptions in which disclosures of information can be given without consent, however most reasons pertain to active investigations or criminal proceedings. Article 7 and Recital 32 of GDPR provide the conditions needed to obtain consent. Firstly, both regulations allow for individuals to withdraw consent at any time and firms must respond in a timely manner. This means firms must be aware of what they need to do in the case of consent being revoked. Secondly, both regulations require terms and conditions of services as well as use, processing, and collection of data to be explained to the data subjects in a clear manner. Lastly, for both regulations, it is important to note that conditions for consent change for children and when handling healthcare data.

Limiting Collection

The limiting collection principle establishes that firms must be honest about the information collected and to "collect personal information by fair and lawful means.. [and] collect only the personal information [the] organization needs to fulfill a legitimate identified purpose". Data collection has a ubiquitous presence in our day to day lives with firms massively benefitting from gaining all of this information. Oftentimes, individuals unwillingly give away their information, whether that be via clickthrough agreements or cookies tracking your browser history. The limiting collection principle tries to protect the privacy of our personal information and requires firms to make a cognizant effort to explain what information is being collected and the identified purpose for that collection.

Limiting Use, Disclosures, and Retention

The limiting use, disclosures, and retention principle determines that "unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected… [and] must only be kept as long as required to serve those purposes". This principle corresponds with Article 5 of GDPR, specifically around the idea of data minimization and ensuring the information remains confidential. This principle and Article 5 of GDPR require firms to actively engage with data throughout its entire lifecycle at the organization and be responsible for how the information is being managed. In limiting the use, disclosures, and retention of data, PIPEDA is focused on minimizing the amount of time firms hold on to data and who they are sharing that information with. Specifically in regards to sharing that information, according to the consent principle, it needs to be clearly outlined how this information is being used, how long it will be used, and who will have access to it. This limitation principle gets to the planning phase of projects. Groups need to meticulously think through the ways this information will be used because those are the only parameters the individual is consenting to. It is better for firms to take more time in the planning phase to think about all the requirements they will need to clean, process, and analyze information in a timely manner as well as what happens to the data when they are finished.

Accuracy

The accuracy principle encourages firms to "minimize the possibility of using incorrect information when making a decision about an individual or when disclosing information to third parties". This principle focuses on ensuring all information maintained and stored about individuals is as correct as possible. This requires due diligence on the side of the firm and that it quickly responds to calls for correction. This principle coincides with Article 16 of GDPR, which guarantees the right to modification in a timely and accurate manner. Individuals have a right to change their information to reflect current correct information. Essentially this principle and article guarantees the accuracy and integrity of the records being stored within the systems at the firm.

Safeguards

The safeguard principle requires that firms "protect personal information in a way that is appropriate to how sensitive it is… [and] against loss, theft, or any unauthorized access, disclosure, copying, use or modification". This principle works to build confidence among individuals that their personal information is being kept in a secure and sensitive manner. Individuals put a lot of trust in companies and organizations that they share their data with. Often this can be transactional data linking to a credit card or sensitive information like passport numbers. Firms often struggle with ensuring the safety of this information. In IBM's *Cost of a Data Breach Report 2021*, 44% of all data breaches were of customer's personally identifiable information with firms paying an average of $180 USD per lost or stolen record (IBM, 2021a). Findings also suggest that the cost of a data breach in Canada has gone up by almost one million CAD from $4.5 million CAD in 2020 to $5.4 million CAD in 2021. While there are no specific requirements in PIPEDA on how to safeguard an individual's personal information, firms should be aware of the importance of keeping their systems secure and up to date. This is both a moral imperative, to maintain the trust of customers, as well as good business practice due to the cost associated with addressing data breaches.

Openness

The openness principle works to guarantee firms "inform customers and employees that you have policies and practices for managing personal information…[in a manner] easily understandable and easily available". This principle focuses on the need for transparency when firms address and share information with individuals. Information provided by the firm needs to be clear and easily digestible. This principle gets to the nature of the knowledge gap between most firms and the individuals using their platform or product. The company or organization holds all the knowledge and individual users are only privy to some of the information. This openness principle corresponds with Article 12 of GDPR, in the sense that, under both regulations, firms have a responsibility to provide transparent communication to their customers. A key aspect of this under PIPEDA, is having easily accessible names and titles of people working in the company as well as who to contact for what information. This allows individuals to have ease of access if they have questions or concerns about the practices of the firm.

Individual Access

The individual access principle informs firms that "individuals have a right to access the personal information that an organization holds about them. They also have the right to challenge the accuracy and completeness of the information, and have that information amended as appropriate". This principle is closely related to the openness principle because it requires firms to have a clear plan of how to address individuals' questions about obtaining, accessing, and requesting their personal information. It is beneficial and advisable for firms to have this information readily available for individuals interested. This information needs to be clear and understandable. This means that plain language must be used, and it is recommended to avoid unexplained acronyms and abbreviations. These requests for information should also be addressed within 30 days unless there are unforeseen obstacles or outside consultation is needed (Fraser, 2022).

Challenging Compliance

The challenging compliance principle allows "an individual must be able to challenge [the] organization's compliance with the fair information principles''. This principle gives individuals the right to file a complaint against firms if they believe the firm is not fulfilling their obligations under the fair information principles. This principle encourages firms to establish investigation and complaint handling processes. All complaints filed against firms must be taken seriously and properly investigated in a timely manner. The firm is responsible to inform the individual of their own procedure for handling complaints as well as procedures from regulatory agencies and the Office of the Privacy Commissioner of Canada. All complaints must be addressed by the individual accountable for the firm's compliance with PIPEDA, often this is the Chief Privacy Officer. Upon completion of the investigation into the complaint, the firm has an obligation to inform the individual regarding the outcome. While this is the federal precedent, provinces with their own privacy regulation, including British Columbia, Alberta, and Quebec, have their own procedure for handling complaints at the provincial level. In Canada, the federal and provincial regulation work together, in which provincial regulation supersedes federal regulation (Ibid). While these regulations may differ, largely they are similar to federal policy.

Potential Challenges and Solutions

Upon examining the foundational requirements of GDPR and PIPEDA, five major challenges arise from the regulations for those operating in the decentralized and distributed space. While these challenges can create some obstacles for firms during the design phase, it is good to keep these in mind. The major challenges identified are *right to forget, erase, and modify; role of data controller; privacy by design; anonymization; and jurisdictional constraints*. Because these challenges arise in both GDPR and PIPEDA, there is a strong indication that we will see the development of these aspects of the regulation with time. When firms consider if these challenges apply to their solution and how they will address these challenges, their product or

platform will ultimately be stronger for it. In the following section, we will briefly re-introduce the topic and offer some solutions for private blockchains and distributed ledgers.

Right to Forget, Erase and Modify

This section of regulation gets to the heart of the idea that individuals may want to change the information being stored about them. They can choose to do this in multiple ways under GDPR and PIPEDA which include erasure and/or modification. This can be difficult on blockchain-based systems due to the immutability of the network. However, fundamentally these two are not irreconcilable because regulations have left the definitions or parameters of deletion and modification vague. In turn, this does give firms some options and leeway regarding how best to go about addressing these challenges. So far, there are three potential solutions to addressing these challenges on blockchain-based systems including: modification via chameleon chain, modification via updating information through additional blocks, and erasure via destruction of private key.

First, modification via chameleon chain offers an editable, redactable blockchain architecture (Tatar et al., 2020). By having an editable blockchain, individuals would be able to keep their personal information up-to-date and remove any data they no longer want the firm to hold. This addresses some of the concerns regulators have with the immutability component to blockchain and distributed ledger systems. At the 2017 *IEEE European Symposium on Security and Privacy*, researchers posited that the creation of a chameleon chain was possible by targeting the collision resistance property of blockchain systems. The researchers found:

> "All blockchain designs rely on a hash chain that connects each block to the previous one, to create an immutable sequence. The immutability comes from the collision resistance property of the hash function. The best way to grasp the concept of a redactable blockchain is to think of adding a lock to each link of the hash chain… Without the lock key it is hard to find collisions and the chain remains immutable but given the lock key it is possible to efficiently find collisions and thus replace the content of any block in the chain. With the knowledge of the key, any redaction is then possible: deletion, modification, and insertion of any number of blocks. Note that if the lock key is lost or destroyed, then a redactable blockchain reverts to an immutable one." (Ateniese et al., 2017, Page 112)

This system does trade-off security to achieve erasability because it is possible that a bad actor finds the correct collisions on the system and in turn incorrectly modifies the chain. However, this solution also offers some work around regarding one of the major challenges firms are facing when trying to implement decentralized systems.

Second, and less technically sophisticated than the previous option, is to modify the chain with updated information in new blocks. Ideally, the block to be modified would be the latest one on the chain making the rectification of that block clear in the subsequent block afterwards. Firms stray away from completely removing the block with incorrect information because that would

'break the chain' thus breaking its integrity and weakening the system (Jurdak et al., 2019). However, if an individual requested that their information be corrected, adding a new block on the chain would address the incorrect information (Riva, 2020). While this would not totally erase the old information on the blockchain, individuals would be able to see that new information was added, thus addressing past blocks. This solution should be further explored with legal counsel to determine whether it meets the standards within the jurisdiction the firm is operating in.

Lastly, and most experimental, is destruction of an individual's private key as means of erasure. Also referred to as crypto-shredding, this new technique posits that since all personal records are encrypted with a private key, if an individual were to destroy that key, their records would be inaccessible and thus rendering them erased (Robinson, 2020). This would also include back-ups of the individual's records, which is often one of the most difficult aspects of deletion for firms. Recently the software company, Thoughtworks, recommended this solution to Technology Radar as a means to address the right to be forgotten (Thoughtworks, 2019). This is a new solution that hasn't been explicitly addressed by any regulatory body, at the time this paper was written. However, it does offer a promising solution to the right to erasure. Again, due to the newness of this technique, it is recommended that firms seek the help of legal counsel before wholly committing to this solution as an answer to the right to be forgotten and right to erasure.

Role of Data Controller

By establishing an individual or organization as a data controller, regulators are trying to create accountability within the handling of information and personally identifiable data. The mishandling of data is a major problem in the tech industry and policymakers' approach is to establish an entity to be legally responsible over the data to encourage and ensure firms compliance with current regulation. Traditionally this role is filled by the Chief Privacy Officer of the company, however, for decentralized and distributed systems where there is limited to no centralized authority this approach can be challenging.

In these systems there is not necessarily a single authority figure (given the system design) who controls all the data and information; instead, there are many nodes on the systems. Some groups like the CNIL and the UK's Information Commissioner's Office (ICO) have suggested that the role of data controller can be defined more loosely than originally thought. In November 2018, the CNIL issued a report looking at possible solutions to reconcile blockchain-based technologies and GDPR. Of particular interest was the note that, "in many cases, the participant (i.e. the person deciding to register data on a blockchain) can be considered as a data controller given that the participant determines the purpose and means of data processing" (CNIL, 2018). Depending on the system architecture, nodes in decentralized and distributed systems can have control over what data is stored in the network. Some have argued, including CNIL, that these individuals are both the processor and the controller of their data. However, this decision is not universally recognized throughout Europe. Also in 2018, the UK's ICO issued guidance on data controllers and processors under their *Data Protection Act*. In their findings, they suggest that

entities must be either the controller or the processor of a system and there is no room for crossover (ICO, 2018). However, they also suggest it is possible to designate the firm or company itself as the data controller of the system. This is because a data controller can be a legal agency, according to the definition in Article 4(7) of GDPR. However, this solution will only work for decentralized systems associated with a larger firm, but that is not always the case as some systems run in a truly decentralized manner with no authority.

Privacy by Design

This challenge arises because in GDPR and in PIPEDA, regulation requires firms to center the privacy of individuals in all steps of the design, planning, and implementation phase. This challenge corresponds with the basic ideas of data minimization and purpose specification mentioned in the previous sections. In blockchain-based systems it can be difficult to ensure privacy by design because often these systems collect a plethora of information on individuals and store data indefinitely. This can be extremely difficult to resolve with current regulation, especially on public blockchains where information, potentially personally identifiable information, is available to all nodes on the system. One solution to address this challenge is to store all information off-chain. IBM defines off-chain storage as "any non-transactional data that is too large to be stored in the blockchain efficiently or requires the ability to be changed or deleted" (IBM, 2018). By using off-chain storage solutions, firms benefit from more advanced search functions, faster processing time, and lastly, more privacy because transactions are not visible on the public chain (Pinto, 2019). By offering privacy-preserving options through off-chain storage and having the ability to edit and delete data, firms are able to work within the regulatory framework. When designing a decentralized and/or distributed system, firms should consider using off-chain storage for security and privacy reasons.

Another privacy-preserving approach is to use an SSI system. In SII systems, transactional data that might contain personally identifiable information is never stored on a ledger; instead, communications occur peer-to-peer. The ledger is simply used to set up a cryptographically secured communication channel and for purposes of verifying the integrity and authenticity of information exchanged.

Pseudonymization

A major challenge that arises from comprehensive data governance models is the threshold for anonymization of personally identifiable information. Governing bodies have made a strategic decision to set a very high threshold for anonymization of data, in part, because of the prevalence of data breaches as mentioned in the Safeguards section in this paper. However, there are no clear parameters of when data has been anonymized enough. This can leave firms guessing about whether their solution meets these ambiguous guidelines. One way to deal with this issue is through decentralized identifiers (DIDs). According to Microsoft, DIDs are, "a trust framework in which identifiers, such as usernames, can be replaced with IDs that are self-owned, independent, and enable data exchange using blockchain and distributed ledger technology to protect privacy and secure transactions" (Microsoft Security, 2020). The purpose

of DIDs is to return the power back to the individual making them the issuer and verifier of their own identity. DIDs have risen in popularity as a response to the lack of control individuals have over their personally identifiable information and who is storing it. With this information stored in caches that individuals are often unaware of, such data becomes vulnerable to cyber security attacks.

Consumers have normalized having much of their personal information given away during transactions when often that information is not relevant. For example, if you go to the store to buy alcohol and you show the clerk your driver's license, all they truly need to know is whether you are at or over the age required to buy alcohol. However, they have access to your home address, name, driver's license number, birthday etc. because that information is readily available on your license. In turn, the individual has no control over sharing that information with them. DIDs reduce how much information is shared for any transaction, thus reducing identifying factors that could be traced back to an individual. These identifiers can be completely anonymous, if an individual wants, making them a suitable option for compliance within regulatory frameworks (Goodell & Aste, 2019). Use cases of DIDs include but are not limited to identification, payments, and healthcare records (IBM, 2021b). Firms interested in storing personally identifiable information should consider utilizing DIDs to meet the requirements of anonymization.

Jurisdictional Constraints

Geographical boundaries are relevant when it comes to third party processing of data across international borders. If countries have agreements with one another, much like the adequacy status between Canada and the EU, there is a free flow of information. However, issues arise when the processing of information takes place outside of the country of origin. This in part has to do with consent as individuals only consent to having their data used, collected, and processed in the country in which the firm is located. This challenge will be unique to every use case because of the design of the system. One way to guarantee a firm is compliant with this restriction is to have all processing of information take place in the firm's country of origin, but this approach has obvious limitations for large-scale public permissionless blockchains even if suitable for private, permissioned systems.

Limitations

This study provided an overview of relevant articles, recitals, and principles outlined by Canadian and European privacy governing agencies for firms operating in the decentralized space. The focus of this study was to research the impact these privacy regulations have on private, permissioned blockchain-based systems and present possible solutions to challenges that arise with compliance. As decentralized systems become more prominent and relevant in today's discourse about privacy and data rights, governments need to focus on creating regulation that encourages the development of these systems. Moore's Law suggests that a computer's processing speed doubles every 18 months which ushers in periodic bursts of innovation in system speeds and processing power (Rotman, 2021). According to IBM, demand

for blockchain skills has increased by “almost 2,000% from 2017 to 2020” (IBM, 2020). Similarly, the 2019 Gartner Chief Information Officer (CIO) Agenda Survey noted that “even though they are still uncertain of the impact blockchain will have on their businesses, 60% of CIOs… said that they expected some level of adoption of blockchain technologies in the next three years'' (Rimol, 2019). These reports indicate firms are expecting to see growth in the blockchain-based information processing sector. Technology and innovation grows exponentially, leaving regulators and policy makers constantly playing catch up. As a result, we can see regulation also changing, granted, at a much slower pace. Firms will need to remain aware of the changes happening within the field and the long-term impact that has on regulation within the country in which they are operating.

Future Research

Due to Canada’s changing adequacy status with the EU it can be expected that major privacy policy changes will come out in the following one to two years addressing some of the gaps between the regulations. Quebec’s Bill 64 and the tabled federal legislation, the Digital Charter, provide insight into the direction the Canadian regulation is moving. Both of these new regulations mirror the language and tone of GDPR from requirements of firms to potential penalties for not reporting breaches. Canadian privacy regulation has tended to stay general, providing principles to follow instead of firm, set rules. However, in November of 2018, Canada signaled that the government was going to start to put stricter regulations and punitive measures in place, like a maximum fine of $100,000 CAD, for firms that fail to report data breaches (Global News Staff, 2018). As new regulations and amendments come out, it will be helpful for firms to understand the relevant policy changes and possible fines they can receive. Therefore it is recommended to follow-up this report when the new Canadian regulation comes into place and analyze how these changes will impact the development of companies.

Simultaneously, there is a need to analyze specific use cases based on their design, white paper, and functional specification to provide specific recommendations and privacy by design suggestions moving forward. Decentralized systems, specially distributed ledger technologies, are highly sophisticated and have to be examined at the microlevel in order to determine whether or not a particular system is compliant. It is also recommended that firms complete a Privacy Impact Assessment for individual use cases, depending on their location these can differ country to country and province to province. However, it is often when firms rush through these processes that they miss vital information that will help the longevity of the company. This also extends to the requirements of the reporting process, specifically in the Safeguard and Challenging Compliance principle, which highlight the responsibilities firms have while collecting, processing, using, and/or storing personally identifiable information. For example, in 2020, 40% of firms who reported a breach of records did not fulfill the requirements or provide the necessary information to assess the “Real Risk of Significant Harm'' as mandated under PIPEDA (Krebs & Brock, 2020). Ultimately, this lack of communication between regulators and firms harms the individual who is using the system. Hence, taking the time to provide the necessary documentation to do full assessments of the system architecture is vital to the long-

term success of any project. Governments need to clearly outline the steps that firms can take to remain compliant with current regulation.

Conclusion

Distributed ledger and blockchain-based technologies are advantageous to firms with the rise of data breaches and storage of personally identifiable information. There are trade-offs associated with running and maintaining these systems in the long run, like start-up cost and energy cost associated with running servers. Regulators and policymakers should not be naive about the importance of this technology, the exponential growth we have seen, and the expected growth noted by those in the industry. They need to understand how offering blanket regulations for new innovations has significant limitations and could hinder the growth of the industry. Offering concise language about what regulations mean and clear legal definitions will benefit private industry when designing solutions. Current regulation is ambiguous and often does not directly discuss different forms of decentralized technologies making it unclear how firms best situate themselves. More governments need to refer to documents like CNIL's "*Blockchain and the gdpr: Solutions for a responsible use of the blockchain in the context of personal data*" to provide a clear framework for these decentralized firms to operate. These new innovations in technology are not going away and policy makers need to be proactive in their approach to working through some of these challenges.

Ultimately for all firms piloting solutions in the decentralized, distributed, and self-sovereign space, it is important to take a risk-based approach. Be aware of the tools that can be used, like Privacy Impact Assessments and guidance from legal professionals. Much of this regulation is still relatively new and utilizes ambiguous language, which leaves firms in the dark about what they need to do to meet the current industry standards. Noting relevant court cases will help companies and organizations track the direction the industry is moving in and the legal precedent for specific challenges that arise. With increased communication and collaborations between private industry and governing bodies, the future of regulation can protect the rights of individuals and their data while simultaneously fostering innovation.

References

Andriole, S. (2021, July 16). *Too many single points of failure threaten our digital infrastructures - & they're multiplying*. Forbes. https://www.forbes.com/sites/steveandriole/2021/07/16/too-many-single-points-of-failure-threaten-our-digital-infrastructures----theyre-multiplying/.

Ateniese, G., Magri, B., Venturi, D., & Andrade, E. (2017). Redactable blockchain – or – rewriting history in Bitcoin and friends. *2017 IEEE European Symposium on Security and Privacy*. https://doi.org/10.1109/eurosp.2017.37

Baran, P. (1962). On distributed communications networks. *IEEE Transactions on the Professional Technical Group on Communications Systems*, *CS-12*(1). https://doi.org/10.7249/p2626

Berberich, M., & Steiner, M. (2016). Practitioner's corner · Blockchain Technology and the GDPR– How to Reconcile Privacy and Distributed Ledgers? *European Data Protection Law Review*, *2*(3), 422–426. https://doi.org/10.21552/edpl/2016/3/21

Berty. (2019, June 25). *Centralized vs decentralized vs distributed systems*. Medium. https://medium.com/berty-tech/berty-tech-centralized-vs-decentralized-vs-distributed-systems-2e9efd856c2.

Chaykowski, K. (2018, April 12). *Congressional leaders Press Zuckerberg on political bias, data collection at Facebook*. Forbes. https://www.forbes.com/sites/kathleenchaykowski/2018/04/11/congressional-leaders-press-zuckerberg-on-political-bias-data-collection-at-facebook/?sh=52751d971a95.

CNIL. (2018, November 6). *Blockchain and the gdpr: Solutions for a responsible use of the blockchain in the context of personal data*. Commission Nationale de l'Informatique et des Libertés. https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

Confessore, N. (2018, April 4). *Cambridge Analytica and Facebook: The scandal and the fallout so far*. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Daoui, S., Fleinert-Jensen, T., & Lempérière, M. (2019, June 28). *GDPR, blockchain and the French data Protection Authority: Many answers but some remaining Questions*. Stanford Journal of Blockchain Law & Policy. Retrieved from https://stanford-jblp.pubpub.org/pub/gdpr-blockchain-france/release/1.

Edwards, L., Finck, M., Veale, M., & Zingales, N. (2019, June 13). *Data subjects as data controllers: A fashion(able) concept?* Alexander von Humboldt Institute for Internet and Society. https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400.

EU Commission. (2021, June 28). *Adequacy decisions*. European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

EUR-LEX. (2016a, December 17). *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002.

EUR-LEX. (2014, May 13). *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

EUR-LEX. (2016b, October 19). *Patrick Breyer v Bundesrepublik Deutschland*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0582.

Fraser, D. (2022, February). *Canadian privacy law for non-Canadian lawyers*. YouTube. McInnes Cooper Law Firm. https://www.youtube.com/watch?v=727ZnGfBywE.

Geist, M. (2018, March 5). *No longer fit for purpose: Why Canadian privacy law needs an update*. The Globe and Mail. https://www.theglobeandmail.com/report-on-business/rob-commentary/no-longer-fit-for-purpose-why-canadian-privacy-law-needs-an-update/article38214804/.

European Union (2018). *General Data Protection Regulation (GDPR)*. Intersoft Consulting. https://gdpr-info.eu/.

Global News Staff. (2018, November 1). *Failure to Report Canadian privacy breaches could mean big fines after Nov. 1*. Global News. https://globalnews.ca/news/4619728/failure-to-report-canadian-privacy-breaches-could-mean-big-fines-after-nov-1/.

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. *Frontiers in Blockchain*, *2*. https://doi.org/10.3389/fbloc.2019.00017

Government of Canada. (2019). *Report to the European Commission December 2019*. Sixth Update Report on Developments in Data Protection Law in Canada. https://www.ic.gc.ca/eic/site/113.nsf/vwapj/SixthUpdateReportonDevelopmentsinDataProtectionLawinCanada_en.pdf/$file/SixthUpdateReportonDevelopmentsinDataProtectionLawinCanada_en.pdf.

Hori, S. (2021, August 12). *Self-sovereign identity: The future of personal data ownership?* World Economic Forum. https://www.weforum.org/agenda/2021/08/self-sovereign-identity-future-personal-data-ownership/.

IAPP. (2021a). *Comprehensive laws*. Comprehensive Laws. https://iapp.org/resources/article/comprehensive-laws/.

IAPP. (2021b). *Co-regulatory model*. Co-regulatory Model. https://iapp.org/resources/article/co-regulatory-model/.

IAPP. (2021c). *Sectoral* laws. Sectoral Laws/Model. https://iapp.org/resources/article/sectoral-laws/.

IAPP. (2021d). *Self-Regulation model*. Self-Regulation Model. https://iapp.org/resources/article/self-regulatory-model/.

Information Policy Team, Furman, J., Coyle, D., Fletcher, A., McAuley, D., & Marsden, P., Unlocking digital competition: Report of the Digital Competition Expert Panel (2019). The National Archives. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf.

IBM. (2021a). *Cost of a Data Breach Report 2021*. IBM. https://www.ibm.com/security/data-breach.

IBM. (2021b). *IBM Verify Credentials: transforming digital identity into decentralized identity*. IBM. https://www.ibm.com/blockchain/solutions/identity.

IBM. (2020, April 24). *The future of blockchain*. Blockchain Pulse: IBM Blockchain Blog. https://www.ibm.com/blogs/blockchain/2020/04/the-future-of-blockchain/.

IBM. (2018). *Why new off-chain storage is required for blockchains.* IBM. https://www.ibm.com/downloads/cas/RXOVXAPM.

ICO. (2018). *Data controllers and data processors: what the difference is and what the governance implications are*. Information Commissioners Office. https://ico.org.uk/media/for-orgnisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

Ishiara, T. (2019, October 25). *In a nutshell: data protection, privacy and cybersecurity in Japan*. Lexology. https://www.lexology.com/library/detail.aspx?g=5968d791-b916-42eb-869a-38ae7d902ab3.

ISO. (2020). *Blockchain and distributed ledger technologies — Vocabulary*. International Organization for Standardization. https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en.

Jurdak , R., Dorri , A., & Kanhere , S. (2019, September 16). *Protecting the 'right to be forgotten' in the age of blockchain*. The Conversation. https://theconversation.com/protecting-the-right-to-be-forgotten-in-the-age-of-blockchain-104847.

Kelion, L. (2019, September 24). *Google wins landmark right to be forgotten case*. BBC News. https://www.bbc.com/news/technology-49808208.

Krebs, D., & Brock, E. (2020, October 5). *40% of data breach records insufficient - Canadian Privacy Commissioner Releases findings on data Breach Register inspections*. Lexology. https://www.lexology.com/library/detail.aspx?g=e1ca79b2-beec-4c7d-ad8d-6cb313781b01.

Lazarus, D. (2020, December 1). *Column: This company will pay you to share your data. Is it worth it?* Los Angeles Times. https://www.latimes.com/business/story/2020-12-01/column-privacy-money-for-data-sharing.

V. Lemieux, A. Voskobojnikov and M. Kang, (2021). *Addressing Audit and Accountability Issues in Self-Sovereign Identity Blockchain Systems Using Archival Science Principles*. 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 1210-1216, doi: 10.1109/COMPSAC51774.2021.00167.

Lemieux, V. (2017). Blockchain Recordkeeping: A SWOT Analysis. https://www.bluetoad.com/publication/?i=454085&article_id=2939577&view=articleBrowser.

McMahon, D. (2019, September). *Blockchain and GDPR - what can we learn from the European Parliament's Recent study?* https://www.mccannfitzgerald.com/knowledge/technology-and-innovation/blockchain-and-gdpr-what-can-we-learn-from-the-european-parliaments-recent-study.

Microsoft Security. (2020, January). *Decentralized Identity, Blockchain, and Privacy*. Microsoft. https://www.microsoft.com/en-ca/security/business/identity-access-management/decentralized-identity-blockchain.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf.

Nissenbaum, H. (2016). *Must Privacy Give Way to Use Regulation?* YouTube. https://www.youtube.com/watch?v=2lIpdPPwKs0.

Obar, J. A. (2019). Searching for data Privacy self-management: Individual data control and canada's digital strategy. *Canadian Journal of Communication*, *44*(2). https://doi.org/10.22230/cjc.2019v44n2a3503

Office of the Privacy Commissioner of Canada. (2014, October 30). *Metadata and privacy - a technical and legal overview*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/.

Office of the Privacy Commissioner of Canada. (1983, July). *Privacy Act (R.S.C., 1985, c. P-21)*. Government of Canada. https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html.

Office of the Privacy Commissioner of Canada. (2021, February 11). *The personal Information protection and electronic Documents Act (PIPEDA)*. The Personal Information Protection and Electronic Documents Act (PIPEDA). https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

Olofsson, D. M. (2021). *Privacy and Data Protection in Canada*. YouTube. McGill School of Continuing Studies. https://www.youtube.com/watch?v=WfJ-vSDRRIw.

Ortiz-Ospina, E. (2019, September 18). *The rise of social media*. Our World in Data. https://ourworldindata.org/rise-of-social-media.

Pinto, R. (2019, September). *On-Chain Versus Off-Chain: The Perpetual Blockchain Governance Debate*. https://www.forbes.com/sites/forbestechcouncil/2019/09/06/on-chain-versus-off-chain-the-perpetual-blockchain-governance-debate/?sh=5964424b1f5e

Raval, T. (2019, June 10). *Regulating social media companies*. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/06/10/regulating-social-media-companies/?sh=724dc21762b9.

Rimol, M. (2019, September). *Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years*. Gartner. https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows.

Riva, G. M. (2020). What happens in blockchain stays in blockchain. a legal solution to conflicts between digital ledgers and privacy rights. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00036

Robinson, B. (2020, March 9). *Crypto shredding: How it can solve modern data retention challenges*. Medium. https://medium.com/@brentrobinson5/crypto-shredding-how-it-can-solve-modern-data-retention-challenges-da874b01745b.

Rose, A. (2019). GDPR challenges for blockchain technology. *Interactive Entertainment Law Review*, *2*(1), 35–41. https://doi.org/10.4337/ielr.2019.01.03

Rotman, D. (2021, April 21). *We're not prepared for the end of Moore's law*. MIT Technology Review. https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/.

Samonte, M. (2020, January 27). *Google v. CNIL: The Territorial scope of the right to be forgotten Under EU Law*. European Papers. https://www.europeanpapers.eu/en/europeanforum/google-v-cnil-territorial-scope-of-right-to-be-forgotten-under-eu-law.

Shah, P., Forester, D., Berberick, M., & Raspé, C. (2019). *Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies*. Practical Law. https://www.davispolk.com/sites/default/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf.

Sharma, T. K. (2019, August 7). *Public vs. private blockchain: A comprehensive comparison*. Blockchain Council. https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus Technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*, *38*. https://doi.org/10.1016/j.clsr.2020.105454

Thoughtworks. (2019, April 24). *Crypto shredding*. Technology Rader. https://www.thoughtworks.com/radar/techniques/crypto-shredding.

Tobin, A., & Reed, D. (2016, September 29). *The inevitable rise of self-sovereign identity*. Evernym. https://www.evernym.com/wp-content/uploads/2017/07/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

Truong, N. B., Jayasinghe, U., Um, T.-W., & Lee, G. M. (2016). A Survey on Trust Computation in the Internet of Things. *Information and Communication: Journal of the Korean Telecommunications Society*, *33*(2).

United Nations Conference on Trade and Development. (2021, April). *Data protection and privacy legislation worldwide*. UNCTAD. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Uslaner, E. (2010). Trust and the Economic Crisis of 2008. *Corporate Reputation Review, 13*(2). https://doi.org/DOI:10.1057/crr.2010.8

Walters, N. (2019). Privacy Law Issues in Public Blockchains: An Analysis of Blockchain, PIPEDA, The GDPR, and Proposals for Compliance. *Canadian Journal of Law and Technology*, *17*(2), 1–31.

Zyskind, G., Nathan, O., & Pentland, A. 'S. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*. https://doi.org/10.1109/spw.2015.27