CASTLEBRIDGE

Changing how people think about information

Thoughts on Paradigms for Data Protection and Data Privacy in a US Federal Law

Dr. Katherine O'Keefe, Daragh O Brien, Kate Doherty-Nicolaou, Joshua Hovsha

Foreword

This paper began life, as many of our research strands to, as a brain dump by Daragh O Brien and Dr Katherine O'Keefe in preparation for a meeting in Dublin in November 2019. The brain dump was written up (hastily) as a first draft working paper to distribute at that meeting.

Kate Doherty-Nicolaou and Joshua Hoshva, ESR researchers with the PROTECT project in Trinity College, who have recently joined the Castlebridge team, reviewed document further and added additional input and insight (including poking holes in things) to bring about the version that is published here.

Introduction

The introduction of a vigorous model of data governance was undertaken by the EU in the form of the General Data Protection Regulation (GDPR). This model is worthy of reflection for other states including the US, since it is home to many of the largest data-processing companies in the world. Currently, no federal consensus for data regulation exists. Instead, data governance laws remain in the hands of states where inconsistent requirements place onerous burdens on companies seeking to comply with legal obligations. This Whitepaper explores perspectives on the creation of a federal data privacy regime in the US.

We begin with a practical discussion of whether data can be understood as a form of property right. The notion of data as a property right is often used as a mechanism to construct protections around personal information. While, this model is tempting it is ultimately unhelpful in understanding data and effectively protecting individuals. Instead we place personal data within the framework of privacy as a fundamental right. Specific attention is given to the US Constitutional order and its conception of privacy. Thereafter we provide key architectural principles to be considered in framing a federal law. The benefits to organisations trying to protect privacy rights and better utilise their own data will be explored. Finally, recommended next steps will be listed.

Data as Property

The understanding of data as a form of property is a flawed notion. The “asset” that is information (whether personal or not) is fungible and does not fit the model of a tradeable commodity for several reasons. If we are going to take a property asset class view of personal data, then we should first ensure that organisations and accounting bodies formally recognise and account for the value of that information on their balance sheets.

Today, the understanding of data as a type of property is there by proxy because it is a category of asset that helps to deliver services or produce inflows of value. However, it is measured and reflected in other things such as staff, or actual

tangible assets, so the idea that we can "assetize" data in this way is often bunkum. One can still *monetise* data– by putting it to work, using it to gain insight etc. Data in this way is akin to the role which nitrates serve in soil – they promote growth, but Farmer Brown does not go out and buy a plot of good nitrates, she buys a few acres of land that has nitrates in it. If she does not tend the land properly with effective stewardship, that land becomes exhausted and useless. Moreover, if Farmer Brown does not incur costs to defend and clearly demarcate her physical property, she will encounter squatters, theft, or competing claims to the property.

Similarly, it is a mistake to map an intellectual property model onto personal data. Personal data is not the "copyright of the self" rather it is data about an individual. It is data which describes an individual and can be used to make decisions or take actions that affect or impact an individual. While it is intellectually attractive to draw parallels with the seemingly fungible nature of intellectual property rights, the reality is that those rights are effectively meaningless unless an entity is willing to incur expense to defend them. Such a model places the burden on the rights holder to defend their claim or lose their right.

More significantly, the problem with a property rights perspective for personal data is that it is a flawed analogy. We can understand this when we consider that data which identifies people either directly or indirectly in effect represents the digital essence of the individual and is a manifestation of the person in a different form. When we consider this from an ethical perspective, many of the analogies start to break down very quickly.

As a form of tangible property rights, the idea that one can "sell" a person, or that organisations can "buy" the use of a person is at worst analogous to the idea of slavery and at best comparable to indentured serfdom. Indeed, Daragh O Brien coined the term "Quantified Serf" a number of years ago to describe the concept of people who are toiling in the "data fields" of organisations.[1] These organisations may provide benefits, may be benign, but this is not a guaranteed or consistent aspect of the relationship.

[1] See https://www.irishexaminer.com/lifestyle/features/how-to-take-back-your-online-privacy-383609.html

Similarly, the analogy of personal data as an intellectual property right also falls apart when we start to consider how that relates to the defence of image rights by celebrities and others. These individuals have chosen to market their image or likeness in a professional context as opposed to individuals who are simply trying to interact with businesses, government, or other categories of organisation in order to, quite simply, live their lives and engage in private activities.

This conceptual difference goes to the heart of the right to privacy as set out by Warren and Brandeis in 1890.[2] They explicitly made clear that personal information about oneself is not to be conceived of as a proprietary right. Rather, the concept of privacy is to be understood as a right that enables people to create the space in which they can formulate, develop and exercise their personal thoughts, ideas, and beliefs which they might not otherwise wish to be made public.

An interesting perspective on this aspect of personal data privacy and data protection rights as a form of intellectual property right can also be found in a recent case between the UK's Revenue and Custom's and the Inland Revenue Service and a television presenter. The presenter successfully argued that a tax bill levied against her was incorrect because she was not employed by the TV station as a person but rather, she was hired by them as a performer to play the role of a "chatty TV personality."[3] She was, therefore, self-employed and entitled to a different tax treatment of her earnings in that role.

Therefore, despite being an initially attractive proposition the adoption of a property rights model for data privacy is likely to have many unintended consequences. In the context of algorithmic processing and analytics, the creation of a regulatory environment where data describes and defines the essence of an individual who is subject to being bought, sold, and bartered effectively leads to a form of digital slavery or serfdom. It is at this point that the individual is at the mercy of the market. This risk arises irrespective of the potential for rights of

[2] "The Right to Privacy," S. Warren and L. Brandeis, 4 Harvard Law Rev. 193 (1890)
[3] See https://www.bbc.com/news/entertainment-arts-47648053

action to be introduced for individuals to sue to protect their rights. Such rights will inevitably be expensive to exercise and will inevitably pit individuals against organisations in an unequally matched contest.

Michelle Dennedy posits an analogy that maps data to currency as an asset class because of its dual state.[4] At rest, data has many of the characteristics of a tangible property asset. It can be counted, its quality can be measured, its security needs to be protected/defended, and to an extent value can be derived from the sale of the asset as an 'inert' thing (i.e. not in motion or use, just as it is stored). When data is 'in motion' and is being put to use, it has many of the characteristics of an intellectual property right as there is an exchange of value that is essentially based on a 'license' that is granted to an organisation by an individual to use their data for a particular purpose.

Dennedy identifies the overlap between these two states of data as being akin to currency, where the "conversation" between the parties is a transaction, and the careful curation and measurement of those transactions is the key to developing and delivering value. This then lends itself to a discussion of how the "value" inherent in an exchange is defined, described, and measured and how trust in the nature of the exchange can be established and maintained. However, currency still needs to be defended and protected thereby raising the security aspects of data once again.

This conceptual model is an improvement on a pure property rights perspective as it more correctly defines the nature of data being exchanged as a measure of value and worth in an exchange. However, it is incomplete until one considers how to define the context of the exchange in which value can be defined and what the externalities would be in any 'market' that would help set the balance on the

[4] Testimony of Ms. Michelle Dennedy, Chief Executive Officer, DrumWave Inc. For Hearing on "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation" Before the United States Senate Committee on Banking, Housing, and Urban Affairs Thursday, October 24, 2019.
Available at: https://www.banking.senate.gov/hearings/data-ownership-exploring-implications-for-data-privacy-rights-and-data-valuation

supply and demand curve. The conceptual model of ‘data as currency’ also introduces obligations and constraints into the assessment of the utility of the exchange of data (as defined from both the perspective of the individual and the perspective of the organisation) and the level of invasiveness of that data into the private sphere of the individual.

In this regard, the conceptual model of ‘data as currency’ in which data has a value needs to be disambiguated from a model where ‘data is barter’ and is exchanged in a form of asset swap transaction. In Dennedy’s ‘data as currency’ framing, data is a means of measuring the value of the transaction, considering any requirements to curate and protect the data. ‘Data as currency’ framing also takes into consideration the granularity, depth, and breadth of the data being requested from an individual (or being obtained about them from a third-party) in exchange for a service, product, or other benefit.

Data and Fundamental Rights

Dennedy's view is closely aligned with the fundamental rights basis of EU data protection law as it highlights the need for the 'value' of data to be considered and for there to be defined constraints introduced into the concept of the exchange of value. It also highlights the need for the opportunity cost of a transaction to be considered when assessing the fairness of the exchange and the 'transaction'.

This is expressed through the requirement to consider the impact on other rights and freedoms of the individual arising from the use, misuse, or abuse of the data or from any decisions or actions which may be taken on foot of any processing of the data. Consideration must be given to the curation and management of the information beyond the immediate instance of the transaction; this includes consideration of externalities and risks to both the individual and the organisation which might not be immediately apparent. At the risk of creating a property rights analogy, this is akin to a realtor being required to disclose any known issues or defects with a property which might lead to hidden future costs for a purchaser.

In the European model, which is often held up as a benchmark, there is a clear grounding in fundamental rights. This underpinning of the EU's data protection and data privacy framework is often overlooked in other jurisdictions who copy the model of the legislative form without addressing the principles-based foundations of the model. However, even where the foundations might not have clear and direct constitutional groundings, there is a broad agreement on the Fair Information Processing Principles (one of the US's great contributions to the field) which have found restatement in the core principles of the GDPR and its predecessor legislation.

The Fair Information Processing Principles provide a basis for the curation of the transactions in Dennedy's 'currency' model. This is achieved through the enumeration of key considerations and constraints in the supply/demand curve of the market at which the value can be set for the transaction being undertaken. The principles create a basis by which the individual's bargaining power in respect of any service or benefit they are seeking to acquire is strengthened. Working

within these principles becomes the price of entry into a market for a service provider, and the approach to complying with these principles and meeting obligations within the legislative framework becomes the hallmark of quality that an individual can look to when deciding who to allow access to their data.

However, this requires an anchoring point in fundamental principles, a 'gold standard' against which the 'value' of the currency in Michelle Dennedy's conceptual model can be pegged.

Data Privacy and Constitutional Rights in the US

Several states recognize the concept of privacy as a fundamental or inalienable right, recognizing, as the Constitution of the State of Montana states, that "[t]he right of individual privacy is essential to the well-being of a free society."[5] These protections have varied according to state legislation, but the number of newer measures towards protection of privacy show increasing specific attention to privacy as a fundamental right and a need for greater protections around data privacy specifically.

At a federal level privacy and data protection are fundamental to US Democracy despite not being explicitly listed in the US Constitution. In Griswold v. Connecticut[6] the Supreme Court found that the right to privacy is implicit in the First, Third, Fourth, Fifth, and Ninth Amendments, while Justice Harlan's concurrence highlighted the Fourteenth Amendment. [7] However, a narrow construction of the constitutional protection of the right to privacy, as recognized in American case law, may not fully recognize how privacy is not simply one of the unenumerated rights protected by the Ninth Amendment.

---

[5] The Constitution of the State of Montana as Adopted by The Constitutional Convention March 22, 1972, And As Ratified By The People, June 6, 1972, Referendum No. 68 https://leg.mt.gov/bills/mca_toc/CONSTITUTION.htm

[6] *Griswold v. Connecticut,* 381 U.S. 479 (1965)

[7] *Ibid.* at 500

Rather the rights to privacy and data protection are fundamentally integral in underpinning the enumerated inalienable rights of the US Constitutional order.

The right to privacy is most often argued for as implicit in the Fourth Amendment right against unreasonable searches and seizures. The Fourth Amendment explicitly describes the "right of people to be secure in their persons, houses, papers and effects" effectively enforcing the right to privacy of home and person. Additionally, privacy as a concept underpins several of the other amendments in the Bill of Rights as well. The Third Amendment protecting citizens against quartering protected the inviolability of the private home and family life. While these conceptualizations of privacy underpinning the Fourth and Third amendments are often described with the concept that "each man's home is his castle", the concept of security in one's person extends far beyond the physical concept of home. Furthermore, the context of data privacy provides a constitutional foundation for the concept of privacy as an inviolable personality right comparable to the understanding of Warren and Brandeis. This can also be likened to the German constitutional concept of Persönlichkeitsrecht, the right to develop one's identity and personality, or as Warren and Brandeis put it, the principle of "an inviolate personality".[8]

The implicit understanding of an inviolate right of personality enforceable against arbitrary interference underpins the rights enumerated in First Amendment protecting freedom of speech, and freedom of association. Warren and Brandeis recognized the importance of privacy to freedom of expression, arguing that "the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[9] This understanding is essential in framing privacy rights around data and communications, as in an information society the physical concept of a "home as castle" can become a very strained metaphor. Free development and expression of the self in relation to, communication with, and transaction with other entities requires the freedom to have the privacy to choose not to speak, and to develop one's thoughts in private so one can choose what to speak. Freedom of association requires the ability to associate without the chilling pressure of surveillance (whether governmental or corporate). The question is less that of the "expectation of privacy", but rather about ensuring

[8] Warren and Brandeis, 205
[9] *Ibid.* 198

that the underpinnings of fundamental rights essential to the well-being of a free society are preserved. Violations of information privacy risk citizens Fifth Amendment rights to due process and protection from self-incrimination. The fair information processing and data protection principles of data minimization and purpose limitation protect against these risks. Similarly, the use of algorithmic decision making in "predictive" policing activities and sentencing support risk violating the Fourteenth Amendment as well as due process rights.

Fair Information Processing Principles underpin the European concept of "Data Protection" as an expansion from privacy rights to cover fundamental rights more generally. "Data Protection" requires that bodies processing information about people must follow these principles in order to ensure that they do not violate their fundamental rights when processing their data, privacy being the first and most likely right to be impacted. This recognizes the mutually supporting nature of the fundamental rights recognized in European and American laws and cultures. In an information society, the rights to privacy and data protection are not simply implicit in the penumbra of the explicitly listed rights. Instead, they are necessary preconditions to enable and uphold enumerated constitutional rights and freedoms.

Rights must be upheld across sectors in order to uphold constitutional rights and freedoms, and the enforcement of privacy rights and Fair Information Processing Principles are integral to the functioning of a free democracy. This is even more crucial in an age where control of and access to data in ways affecting the integrity and freedom of one's person and the functioning of democracy are often impacted by corporate as well as government action.

Data Rights, Rights of Action, and Deming

We note that there has been wide discussion of the right of action for data protection and data privacy breaches. In the GDPR, the EU has in effect broadened that right by making it clear that individuals can recover for non-material loss and creating a quasi class-action mechanism for jurisdictions (such as Ireland) who do not have this concept.

However, to the vast majority of potential plaintiffs, the concept of a right of action as a way of upholding and protecting their rights with respect to data about or relating to them or that identifies them directly or indirectly, is practically and pragmatically meaningless as the majority of individuals will simply not have the means to exercise these rights in practice. Bearing in mind that individuals will often have to exercise these rights against organisations who view losing such cases as an existential threat to their business model and operations. The cost of such actions would be significant for an individual and any victory would likely be pyrrhic as the harm or damage would already have been done or incurred.

In his book *Out of the Crisis,*[10] W. Edward Deming (writing about quality management in US industry) identified rising litigation costs as being one of the "Seven Deadly Diseases" of management, particularly of US management, and specifically US manufacturing management. While Deming's words were written over three decades ago, the fundamental lessons he set out are as relevant to today's information-driven business as they were to the manufacturing business who were Deming's primary audience in the 1980s.

Deming countered that the way to address the "Seven Deadly Diseases" was through the adoption of a quality systems approach which, amongst other things, placed the emphasis on *prevention* of defects rather than "scrap and rework" (to fix broken products) and litigation (to defend against claims for harm arising from defects). A key part of Deming's prescription for management was to "adopt the new philosophy" of quality. In the context of data protection and data privacy, that "new philosophy" is, in effect, the adoption of the fundamental

[10] *Out of the Crisis*, W. Edwards Deming, MIT Press, 1986. Reissue available here: https://www.amazon.com/Out-Crisis-Press-Edwards-Deming/dp/0262535947

principles and practices that are increasingly enumerated in the data protection laws of the majority of countries in the world.

In *Ethical Data and Information Management: Concepts, Tools, and Methods*[11], O'Keefe and O Brien explore the relationship between Dr Deming's quality concepts, and the quality systems thinking of other pioneers in that space, to the questions of data ethics and data privacy and we believe this is a valuable contribution to the discussion.

From a practical and pragmatic perspective in business, litigation is often viewed as part of the cost of doing business. Reliance on a right of action approach to regulatory correction of a market will serve to do the following:

It will lead to large class action litigation which will take time to remediate the underlying issues in data processing or in business models or practices which gave rise to the infringement of a data protection/privacy principle.

It will, in practice, divert resources AWAY from staff in organisations who might otherwise be in a position to design "quality" (i.e. privacy/data protection) into the processing activities, product design, and service delivery of an organisation because the legal bills are mounting up.

The scope and application of the law will evolve on a case by case basis. Principles open to interpretation and litigation outcomes hinge on specific causation questions or the specific facts of an individual case.

In effect, to draw a manufacturing analogy, the right of action places litigators in the role of extremely expensive janitors in a production line seeking to sweep up the products that have been made to a poor standard, and assess how they can be fixed *after the fact*, or argue with the customer about how the product was fine, they just used it wrong.

This is essentially the management model that Deming and others railed against in the manufacturing sectors a lifetime ago.

What is required, therefore, is a set of principles (the "new philosophy" to borrow Deming's term) which can be used to guide management, and which will require enforcement mechanisms that can have a more direct effect on the

[11] *Ethical Data and Information Management: Concepts, Tools, and Methods,* K. O'Keefe, D. O Brian, Kogan Page Limited, 2018.

curation of data to ensure that how it is used meets or exceeds the expectations of the individuals that that data describes.

Deming developed his quality management principles in the United States in support of the development of war material in the Second World War. He was then dispatched to Japan to teach his principles to Japanese businesses as part of the rebuilding of Japan after the war. His principles remained largely ignored in the US until their benefit to Asian manufacturers became painfully obvious. The historic irony is not lost on us.

The US made pioneering contributions to the development of the Fair Information Processing Principles (FIPPs). However, it has failed to keep pace with how those principles have been adopted, adapted, and applied globally and, just like US manufacturing in the 1970s and 1980s, the quality revolution is now coming home to roost.

Some Architectural Principles for Legal Frameworks

What are the architectural principles for legal frameworks and how do we put them into practice?

1. **Codify FIPPs, or an updated version of these, into a statutory and regulatory framework.**

The core principles set out in the GDPR provide a reasonably robust generic set of principles in this context. However, they cannot stand alone and require some other architecture to be put around them.

2. **Cease the practice of sectoral regulation and legislation for data privacy.**

A core baseline legislative spine is required against which exceptions can be defined either to create a basis for processing in a particular context, or to define additional or higher standards of safeguards and controls in others.

For example, while Privacy Shield has benefits for many organisations, its scope is limited to FTC-regulated sectors. Having served as Data Protection Officer (DPO) as required by GDPR for a US-based international non-profit, there was *no* specific regulatory basis for that organisation to govern the processing and handling of member data.

3. **Implement appropriate governance and accountability requirements including:**

- The creation of a Data Protection Officer (DPO) / Chief Privacy Officer (CPO) position is necessary. This role *must* be structured so that it can act as an independent conscience of the organisation where needed and not simply as another officer role which might be compelled to act in the short-term interests of the organisation or an operational unit of the organisation.

- The appointment of the DPO role, and the level of knowledge and skills required, should be considered in the context of the volume, nature, and inherent risk in the data that is being processed. Certain types of business working with certain types of data will require this type of role. Others may not, however it may be advisable.
- At a minimum, the governance and accountability requirements should ensure that there is someone in the organisation who has day to day responsibility for ensuring that there are appropriate controls and governance in place to ***prevent*** misuse or abuse of personal data. This is a broad mandate for data governance in the organisation and consideration should be given to data protection / privacy as the tip of the spear into a wider evolution of management practices in organisation with respect to information management.
- These oversight and accountability functions must operate as part of an integrated data governance framework and culture in the organisation and must be recognised as part of the leadership function in the organisation. This should be done in the same way as other roles with responsibility for critical asset classes such as financial or human resources which are explicitly recognised in the organisation chart.

4. **Implement effective regulatory enforcement and do not rely on individual suits to correct systemic concerns.**

The enforcement powers of regulators in the EU are quite strong and they have a range of non-fine sanctions that are available to them which would be considered an existential threat by Data Controllers. These include ordering the suspension of processing and the deletion of data.

Fines, like litigation, can be discounted by executives as a cost of doing business. Being told to stop doing business *that way or at all* can have a more focussing effect.

5. **It must have a fundamental encompassing scope of application.**

This is, in effect, a restatement of point 2 above. It is preferable to have a common baseline that defines the constraints and structures that will operate to affect the definition of “value” in a transaction involving the “data currency”, with any specific sectoral variation being explicitly addressed through a considered modification of the constraints in the market based on an assessment of what is needed to best balance utility and invasiveness.

Also, the rights and benefits should not be constrained based on citizenship or nationality. The EU model whereby the rights arise by reason of you being in the jurisdiction, and any diminution or constraint of those rights then requiring a clear legal basis, is a key principle.

6. **It should not unduly fetter the free movement of data.**

The objective is establishment of constraint and the encouragement of restraint, not the erection of borders and barriers without cause.

By ensuring commonly applicable principles are codified, enforceable, and acted on, in the context of a broadly comparable right-based framework that encourages (and indeed mandates) the appropriate curation of and governance of data, a better and more predictable platform for cross-border movement of data can be established.

Likewise, the creation of rights that allow the individual to take control of how their data is used and to request its transfer to other service providers if so desired, will further support the concept of data as a means of measuring the value of an exchange. If I do not like the service I receive, I can take my money elsewhere and deprive the organisation of future benefits arising from their continued access to my wallet. I should be able to do the same with my data.

Potential Benefits to Organisations

The potential benefit to organisations of codifying principles at a Federal level with associated federal level enforcement mechanisms go beyond the simple matter of reducing the number of regulatory regimes that need to be considered when engaging in processing of data. However, the difficulty of navigating these regimes should be noted.

New regimes for data protection are growing on a state by state basis creating more barriers for uniform compliance. A notable example is the California Consumer Privacy Act of 2018,[12] which will go into effect on January 1, 2020. Similarly, Illinois' Biometric Information Privacy Act[13] has far reaching implications for all organisations processing the biometric data of state citizens. Categories include DNA, fingerprints, facial patterns and voice prints among others. These two laws require significant planning on the part of organisations in order to ensure compliance. Additionally, the fast-flowing nature of data means that a state line complete with jurisdictional authority is increasingly difficult to define.

The increasing number of state data privacy regimes adds to this complexity. In the 2019 legislative session alone data property laws were debated or introduced in 11 states.[14] As this trend continues the absence of a federal regime on data privacy will continue to create greater obstacles for organisations seeking to comply with legal obligation in this field.

[12] AB 375

[13] 740 ILCS 14 et seq. (BIPA)

[14] Testimony of Chad A. Marlow, Senior Advocacy and Policy Counsel, American Civil Liberties Union. For Hearing on "Data Ownership: Exploring Implications for Data Privacy Rights and Data Valuation" Before the United States Senate Committee on Banking, Housing, and Urban Affairs Thursday, October 24, 2019.

Beyond legal compliance costs, attention must be given to the way in which data quality effects organisational costs. The average organisation wastes between 10% and 30% of turnover (or operating budget) through poor quality data and the costs arising from incorrect decisions, or scrap and rework of data to correct those decisions. The data quality principles in data protection laws will require organisations to face up to this hidden cost of doing business and take steps to improve those processes and address those issues. Recent research by American data quality pioneer Dr Tom Redman, carried out in conjunction with University College Cork, has found that less than 3% of organisations have data that is "fit for purpose".[15]

Organisations struggle to develop and sustain the business case for data governance, despite it being a critical business management capability in any data-driven organisation in the 21st century. By creating a mandate for an independent governance structure for data relating to people, a privacy law would have the effect of establishing a mandate for broader data governance practices within the organisation, leading to improvements in organisation efficiency. Castlebridge is already experiencing an upswing in demand from clients who have begun to implement data governance as part of their data protection/GDPR compliance programme but are beginning to see the wider benefits of common methods, standards, approaches, and accountability in other areas of their organisation's data such as property asset management, product management, and physical asset inventory management.

The potential for interoperability across jurisdictions through a mapping and alignment of regulatory principles, and the potential benefits for organisations of the US having a formally established adequacy decision from the European Commission based on a formalised and meaningfully equivalent approaches to the protection of personal data and the protection of fundamental rights which might be impacted by the inappropriate use, or misuse or abuse, of that data cannot be understated. There is a growing consensus internationally on the framework and form of data protection and privacy laws, notwithstanding the

[15] T. Nagle, T.C. Redman, and D. Sammon. Only 3% of Companies' Data Meets Basic Quality Standards. https://hbr.org/2017/09/only-3-of-companies-data-meets-basic-quality-standards Last accessed 10.12.19.

remaining variances that can exist with respect to the functions by which those principles are given effect.

In the context of innovation, it is a misnomer to consider regulation and innovation to be in conflict. Organisations that approach data protection and privacy regulations as a market constraint that must be worked within are increasingly finding opportunities to innovate business models and technologies that are privacy enhancing and privacy respecting. For firms or industries who are resistant to this change, we must simply restate W. Edwards Deming's admonition to American Industry: "You don't have to do these things. Survival is entirely optional".

Conclusion and Next Steps

Notwithstanding the established right to Privacy in the US Constitutional framework and the historic leadership of the United States in the area of Fair Information Processing Principles, it is clear from the debate on the form and scope of a Federal Data Protection statute that a clear and common framework is required around which the specifics of a US law can be developed.

In this context, we note that the European model for data protection and data privacy regulation has much of its modern foundation in the Convention 108 of the Council of Europe, which is in effect the only global legal framework relating to standards for data protection for the purposes of enabling cross border data flows and the protection of individuals.

We believe there is significant merit in the United States considering applying this framework in the framing of its Federal legislation. It is possible for non-member States of the Council of Europe to accede to this international treaty and this may be a future possibility for closer integration and interoperability of US data protection laws and the laws of other countries.

A critical next step however is to recognise data protection and data privacy as issues that have significant potential ramifications for other rights and freedoms of individuals if the underpinning regulatory frameworks are not properly aligned and attuned. The key to this is a recognition of individual data subjects as stakeholders who seek and deserve mechanisms to ensure their rights and interests are balanced in the marketplace. Equally, organisations who seek to strike that balance appropriately need to be considered as stakeholders who deserve to have controls in the market that can highlight untoward, unethical, or improper data handling practices of other organisations and contribute to a more level playing field in which the data subjects are considered as an end in and of themselves, not simply a means to an end.