“The Marco Civil and Beyond: Privacy Governance for the Future”
By Martin Abrams

21 September 2014

Preamble

In 2014, Brazil adopted the Brazilian Civil Rights Framework for the Internet, Law Number 12.965 (which we will refer to as “Marco Civil”), that contained privacy provisions. Those provisions are intended to give Brazilians control over their data when online. This paper is not intended to be a review of those provisions but, rather, a broader discussion into what constitutes effective, practical and balanced privacy governance. In drafting the paper, I looked at legal provisions in Europe, the Americas and the Asia pacific region as well as the current global debate on effective privacy governance. The paper reflects my views and is not necessarily reflective of the Information Accountability Foundation, a research and educational organisation I lead, or the Foundation’s funders.

Introduction

We humans have evolved as a social species. We travel in packs and congregate in families. We are very curious about our neighbours yet protect ourselves from their view because we are also a private species. We, at times, crave seclusion, and we maintain secrets within our social groups.

We are also a species with a sense of history. Beginning with cave drawings, we have always built reflections of our thoughts and descriptions of major events. As we have evolved, our technologies for recording histories have evolved with us. Century after century, the new technologies have shaken the balance between the social us and the private us. Probably, the first major eruption was the development of writing in ancient Sumer. The printing press followed four thousand years later, and another four hundred years to the brownie camera that sparked Brandeis and Warren’s law review article on privacy\(^1\). Radio and TV followed.

Then, the computer and communications revolution really took off. The Internet became a consumer media in the mid-1990s, and the iPhone was released in 2007 expanding massive observation beyond the PC. Big data began in the first decade of this century when scientists developed techniques that facilitated the processing of unstructured data such as digital images

as part of advanced analytics. The technologies have broadened the nature of groups – social networks making ad-hoc new associations possible at a distance, the sharing of insights and the linkages among the past, present and predictions of the future.

Visitors to Brazil for the 2014 World Cup posted millions of pictures on social networks using their own personal surveillance device also known as the smart phone. Police maintained order in part through CCTV. Fans celebrated wins and mourned loses with friends oblivious to the observation by others, and then shared their sadness and joy with confidants in pictures and posting where the metadata about that expression passed through thousands of hands.

Authorities throughout Brazil planned for any and all natural and man-made events that might cause risk by using big data analysis. That analysis will be further updated to prepare for the 2016 Olympics.

This is the environment in which we both implement the new Macro Civil and contemplate a new privacy regime.

**Data Drives a Modern Economy**

Knowledge is the new capital in a modern economy and society, and knowledge is built on data. Neil Richards and Jonathon King have referred to the new technology mix as the great metadata computer and the rules that will govern that giant mixture of data as privacy. They see privacy as the rulebook that governs the fair origination and management of information that pertains to all of us. I use the word “pertains” intentionally. Much of the data that is stored about us does not come directly from us. This will be discussed more in a latter section on data taxonomies. Nevertheless, someone else’s impressions of me are not my property but theirs. I may have an interest in how it might be used and require protections against its misuse. However, I cannot claim ownership of that data.

The purpose of this paper is to explore the application of the rulebook in a modern data-driven society and its applicability both in Marco Civil and any new privacy law that might follow. Specifically, the paper will:

- Define privacy and data protection;
- Provide a brief privacy law history;
- Suggest a data taxonomy based on data origin and link it to effective policy;
- Discuss processing governance based on establishing legal basis;
- Describe accountability based privacy protections; and
- Provide a number of practical suggestions.

---

Key Concept Definitions – Privacy and Data Protection

Countries with a civil law tradition typically have data protection laws while those with common law tradition have privacy laws. Are they the same? The Article 29 Working Party (WP29)³, which is comprised of all the European data protection authorities, released a paper in the spring of 2014 that provided guidance on balancing the interests of companies with those of individuals when processing data. The paper argued that data protection is a much broader concept than privacy. This distinction was further elaborated in a paper by Peter Hustinx, European Data Protection Supervisor, entitled “EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation”⁴. Hustinx traces the concept of privacy from the UN Universal Declaration of Human Rights and The European Convention on Human Rights. These documents defined privacy as the right to respect for his private and family life, his home or correspondence. According to Hustinx, The Council of Europe found the concept of privacy too limited and proposed the broader concept of data protection which prohibits the inappropriate processing of information. Both the WP29 and Hustinx would argue that beyond privacy data protection facilitates rights affected by information such as employment, family freedom of expression and economic participation. They would argue the more limited term privacy relates to respect for those interests closest to the individual such as family and home.

Hundreds of definitions of privacy exist. I would argue that privacy under Canadian law has a very broad interpretation more like data protection. For the purpose of this paper, it would be useful for the reader to have a sense of the author’s definition of privacy and how that relates to data protection.

First, by privacy, I mean informational privacy. There is also physical privacy that relates to when others can see and hear us. For example, a camera that watches you when you change your clothing is an abuse of physical privacy. It is watching you when you do not expect to be watched. However, when the images captured by the camera are digitised and stored for further processing, that is a matter of information privacy. The observation of your physical person—when unexpected—is an abuse of physical privacy, while the processing of information (the digital image) is informational privacy. The domain for this paper is informational privacy. When I use the term privacy, I mean informational privacy.

³ Article 29 of the Directive 95/46 of the European Parliament and the Council of Europe created a committee called Working Party 29 comprised of all the national data protection authorities to encourage harmonization of the national laws pursuant to the Directive. The committee provides market guidance via opinions. WP 29 has no actual regulatory authority.
Second, by privacy, I mean the absence of the inappropriate processing of information that pertains to an identifiable person. Appropriate may be defined by laws, regulations, agreements, contracts and even well-established expectations. For example, using my health information to discriminate against me in terms of employment would be a privacy violation, because law prohibits that information from being used for that purpose. I do not limit privacy to the individual’s ability to maintain control over data or the right to be left alone. Those are among the privacy definitions that are more constrained.

Data protection is the system of rules that prevent the inappropriate processing. For example, European data protection law requires organisations to have a legal basis to do any processing of data. It further establishes six legal basis for such processing. It is the responsibility of the data controller to establish the legal basis for such processing.

The broad concept of privacy I describe is very similar to data protection. Functionally, one finds few differences between well-established privacy law in countries like New Zealand and Canada that follow a common law model and data protection law in civil law societies. In fact, one sees a blending between the effects-based approach of privacy law and the procedurally based nature of data protection law.

**Privacy Law History**

Informational privacy law dates to research in the 1960s on the risks to individuals from the broad use of mainframe computers. The most impactful research was conducted by Dr. Alan Westin, a Columbia University professor. His 1967 book “Privacy and Freedom” established the basis for the laws that began to emerge in the 1970s.

By 1978, there was enough interest in privacy, particularly as it might affect the free flow of data across borders, to foster the creation by the OECD of a privacy task force chaired by Australian judge Michael Kirby. The Kirby group developed a privacy framework that was adopted by the OECD in 1980. The OECD Privacy Guidelines are the basis for most privacy laws that followed. The privacy guidelines were developed at a time when early PCs were only for the early adapters, most data was provided in a hardcopy paper form, business were in the early transition to database technologies and a consumer Internet was not even a dream.

The OECD Guidelines\(^5\) contained eight principles for the fair processing of data:

1. **Collection Limitation Principle**
   
   There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data Quality Principle**

---

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 (the third principle, above) except:

   a) with the consent of the data subject; or

   b) by the authority of law.

5. Security Safeguards Principle
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

6. Openness Principle
There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle
An individual should have the right:

   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

   b) to have communicated to him, data relating to him:
      i) within a reasonable time;
      ii) at a charge, if any, that is not excessive;
      iii) in a reasonable manner; and
      iv) in a form that is readily intelligible to him;

   c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and

   d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

Collectively, those eight principles are known as the Fair Information Practice Principles, or “FIPS”. While there are other FIPS versions, they all track to the OECD Guidelines.

The early privacy thinkers saw privacy as best practiced if there was a control chain in place. The individual begins having control of data about themselves and selectively yields to others for particular defined purposes. One sees this in the OECD guidelines beginning with the collection principle that specifies data should be collected where possible with the consent of the individual. This control concept is continued with the purpose and use principles as well. The concept of express consent in Marco Civil tracks directly to these early thoughts about privacy controls but goes a step further. Appropriate consent may flow directly from a transaction. For example, when one buys furniture and asks that the furniture be delivered to a particular address, the individual is implying that he or she is providing consent for the address to be shared with the delivery service. The requirement for expressed consent brought by the Marco Civil may be understood as calling for an explicit consent for all such actions. This creates a process that is both burdensome for all parties and dilutes the effect of explicit consent in those instances when it is fit to provide protection.

As mentioned earlier, not all data that pertains to us comes directly from us. We are a very curious species. We observe others, and those observations become impressions. When we memorialise those impressions, they become data that pertains to others but are not under their control. These observations have always existed in the form of notes and even ledger books, as they were when the OECD Guidelines were adopted. Over time, the impressions have become a larger portion of total data and have become digital data. Today, observations no longer require the eyes, ears and nose of an individual, thanks to technologies such as cookies or beacons, devices such as sensors, or systems such as CCTV.

So, technological evolution has originated a tension between the concept of the individual as the controller of the file and the nature of how data is originated that will be explored in the next section.

Data Taxonomy

A plain reading of Marco Civil would suggest the law is most applicable to data readily provided by the individual or observed by the Internet server. To understand the differences between these two types of data in addition to data not explicitly covered by the legislation, a data taxonomy would be useful.

Informational privacy law is essentially the regulation of the processing of data that pertains to individuals in a fashion that may be linked to those same individuals. The term for that data that is the domain for privacy law enforcement is personal data. Data about animals, vegetation and materials are not the domain for privacy law. Data about human individuals by name, address or other identifiers are clearly within the domain of privacy law. Data that may be knitted together to link to a unique individual might be the domain for privacy law. This last
category, data that might be knitted together, has been expanded exponentially by the emergence of new information and communications technology.

The need to govern effectively these new technologies has created a demand for new data taxonomies. The OECD held a workshop in March 2014 to look at their privacy framework and challenges that might arise from big data. The Information Accountability Foundation prepared a new taxonomy based on how data originates\(^6\). The section that follows is taken directly from that work and helps illustrate the challenges that new technologies create for systems, even more so if the governance systems only contemplate express consent.

Background

In looking at data processing’s evolution, the Foundation was able to isolate four classifications of data based on their origin. This background charts the development of the four classifications: Provided, Observed, Derived and Inferred.

Provided

In 1967, when “Privacy and Freedom” was published, the vast majority of data processed by computers that pertained to individuals came directly from the individual’s conscious and voluntary actions.\(^7\) The individual would apply for a loan, register a deed, open an account, apply for a license, pay a bill or graduate from a school. All of these discrete actions would create a record that truly involved the individual. Within this setting, the actions were matched by a collection of data in which the individual participated. So, collection and origin were one in the same.

Observed

At the time, there were small observational data sets, but most were not computerised. Physicians created notes about their patients in paper-based medical charts, small merchants made notes about their best customers and early direct marketers noted similarities about their best customers. These mostly manual data sets—created without the involvement of the individual—were, for the most part, not significant enough to affect a governance model that was generally based on individual autonomy. This taxonomy will classify this category of data as observed.

Derived

As long as there has been data that pertains to an individual, there have been others that have looked for similarities in the data. Merchants have been classifying their customers based on common attributes for as long as there have been buyers and sellers. In 19\(^{th}\)-century North

---


\(^7\) Some of the earliest modern computers were used in World War II to target artillery and develop weapons. Computers were then used for scientific research. Using computers to process data pertaining to people, such as payroll data, came later.
America, merchants created co-ops to share information about credit worthiness with classifications derived from shared data. The direct marketing industry began with the simple process of using transactional data to derive market segments based on look-a-likes. Furthermore, once analysts began looking for similarities, they began to conduct simple arithmetic calculations to enhance comparisons. For example, would ratios of mortgage debt to consumer debt demonstrate something interesting? The products of these simple calculations are data derived from underlying data. The insurance industry has for hundreds of years looked at birth, death, occupations, location and lifestyle and derived actuarial tables that are still used for life insurance underwriting. While the classification builds on data that comes from interactions and transactions that involve the individual, the individual is not involved in the creation of the new data. The taxonomy will classify this data as derived.

Inferred

An early application of computerised statistics against large personal data sets was the bankruptcy scores developed by MDS and Fair Issacs in the 1980s. The scores made use of computerised credit reports to predict the likelihood that an individual would go bankrupt over the next five years. The MDS credit score was not just a matching of attributes of those individuals that went bankrupt but, rather, a statistically-based prediction that was validated using historic data. The resulting credit score is a piece of data based on the probability of a future event taking place that is linked to an individual. While the underlying data came from interactions with the individual, the individual had no involvement in the creation of the score. The classification for this data is inferred.

Data has expanded rapidly since the invention of modern computers during World War II. Rapid change in information and communications technologies led to the expansion of data sets in the late 1980s and the 1990s. The most significant trigger for data expansion was the literal explosion of observational data that was sparked by the Internet in the 1990s. The 21st century has led to sensor technologies that make granular observation possible in the physical as well as virtual world. The combination of online and physical observation has facilitated the massive expansion of observational data. While this data begins with the actions of individuals, the individuals are not active partners in the origination itself. During the past decade, scientists have learned how to use unstructured data in analytic models that predict future behaviour. This significantly expanded the amount of data that could be used for research, since data no longer had to be formatted in traditional fields. Informatics is increasingly able to rank order individuals based on probability, which has led to a rapid expansion of inferred data.

Taxonomy Based on Origin

Our taxonomy based on origin has established four classifications for data based on how the data originates:

1. Provided
Provided data originates via direct actions taken by the individual in which he or she is fully aware of actions that led to the data origination. Provided data includes registrations, surveys, applications, and any instances when the individual provides data with a full awareness that he or she is doing so.

2. Observed
Observed data is simply what is observed and recorded. The emergence of the Internet as an interactive consumer medium has made it possible to observe and digitise data in a more robust manner. On the Internet, one may observe where the individual came from, what he or she looks at, how often he or she looks at it, and even the length of pauses. Facial recognition and the Internet of things are making observation in a digital manner possible in the physical world.

3. Derived
Derived data is data that is simply derived in a fairly mechanical fashion from other data and becomes a new data element related to the individual. For example, simple ratios calculated from other data is derived. Marketing clusters are also an example of derived data.

4. Inferred
Inferred data is the product of a probability-based analytic process. Credit and identity scores are examples, as are many of the inferences that come from big data analysis.

The following table lays out data classifications in greater detail. Column 1 lists the major classifications based on how the data originates. Column 2 contains sub-classifications, which help to make the analysis more granular. For example, some levels of observation are anticipated, the active sub-classification, while others are oblivious to the individual, such as the passive sub-category. Column 3 includes examples to assist the reader in relating the categories to the data world. Column 4 provides a simple ranking based on how aware the typical individual might be based on the distance and manner of data origination. Legacy data governance, most laws based on the OECD Guidance and the EU Directive, is very dependent on individual awareness to both exercise consent as well as data review (access rights) and correction.
<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>Example</th>
<th>Level of Individual Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provided</td>
<td>Initiated</td>
<td>- Applications&lt;br&gt;- Registrations&lt;br&gt;- Public records such as licenses&lt;br&gt;- Credit card purchases&lt;br&gt;- Medical history as provided by individual</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Transactional</td>
<td>- Bills paid&lt;br&gt;- Inquiries responded to&lt;br&gt;- Blood pressure or weight as recorded in clinical care setting&lt;br&gt;- Public records such as court proceedings</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Posted</td>
<td>- Speeches in public settings&lt;br&gt;- Social network postings&lt;br&gt;- Photo services&lt;br&gt;- Video sites</td>
<td>High</td>
</tr>
<tr>
<td>Observed</td>
<td>Engaged</td>
<td>- Cookies on a website&lt;br&gt;- Loyalty card&lt;br&gt;- Enabled location sensors on personal devices&lt;br&gt;- Fitness tracking using wearable device</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Not Anticipated</td>
<td>- Data from sensor technology on my car&lt;br&gt;- Time paused over a pixel on the screen of a tablet</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Passive</td>
<td>- Facial images from CCTV&lt;br&gt;- Obscured web technologies&lt;br&gt;- Wi-Fi readers in buildings that establish location</td>
<td>Low</td>
</tr>
<tr>
<td>Derived</td>
<td>Computational</td>
<td>- Credit ratios&lt;br&gt;- Average purchase per visit&lt;br&gt;- Risk of developing a disease based on a single genetic variation</td>
<td>Medium to Low</td>
</tr>
<tr>
<td></td>
<td>Notational</td>
<td>- Classification based on common attributes of buyers&lt;br&gt;- Medical condition based on diagnostic tests</td>
<td>Medium to Low</td>
</tr>
<tr>
<td>Inferred</td>
<td>Statistical</td>
<td>- Credit score&lt;br&gt;- Response score&lt;br&gt;- Fraud scores&lt;br&gt;- Life expectancy</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Advanced Analytical</td>
<td>- Risk of developing a disease based multi-factor analysis&lt;br&gt;- College success score based on multi-variable big data analysis at age 9</td>
<td>Low</td>
</tr>
</tbody>
</table>
Taxonomy Analysis

Marco Civil uses express consent as the means of governing data that originates via the Internet. The initial question one should ask is whether consent is a viable means for privacy governance on the Internet. The second question is whether it is the best mechanism. While the third question would relate to privacy in Brazil beyond the Internet.

Much of that Internet personal data is provided directly by the individual through registrations, postings and interactions with the browser that are clearly participatory. Additional data originates through the observation of the individual’s actions while online. For example, the length of time a consumer pauses over a pixel may be a data point, but it is more observed rather than provided. Still, further data is inferred via the modelling of the provided and observed data. Some of the inferred data is used for marketing, for billing purposes, or to determine which part of a website is being used or not, while other inferences are used to protect servers and the network as well.

Consent is a viable means of governance on the Internet since there are opportunities for individuals to read a notice and provide consent based on the notice. But, just how effective is that consent when one goes beyond provided data to observed data? Will the individual transfer the knowledge gained from the notice to an awareness of the passive collection that takes place through observation?

Some would argue that expressed consent, as provided for in the law, enhances the protections. However, expressed consent is only as robust as the individual’s understanding of the underlying purpose specification notice. As uses get more complex, it is probable that understanding diminish. Furthermore, as uses become more complex, expressed consent would require more consents from individuals. Consent fatigue becomes a problem, and consents are soon bundled. At that point, they become less meaningful. Malcolm Crompton, the former Australian Privacy Commissioner, has argued that consent then becomes a transfer of risk from the corporation using data to the individual who is assuming risk by providing a consent.

As one moves away from the interactive nature of the Internet to the world at large, the challenges for consent get even greater. When one considers the 3000 sensors in a new car monitoring its performance as well as the performance of the driver, one can begin to see the challenge to governance by way of consent. And the automobile is just one example of a fully networked world where sensors are embedded in the products we use on an everyday basis. One adds the CCTV cameras used to protect public safety, and one can see even more challenges.

The comments above are not intended to understate the value and purpose of consent. Where consent is effective, it should be the primary mechanism for governance. Consent works well
when the individual is the active provider of the data. However, even in the circumstances where consent works, consent is not a safeguard in itself. Privacy protection is dependent on data stewardship the further one moves from the process where individuals are the providers of data and are therefore actually in control.

**Legal Basis to Process**

Some legacy data protection laws make provisions for instances where consent is not effective in protecting individuals. The European Data Protection Directive (Directive 95/46)\(^8\) bases governance on an organisation’s legal basis to process personal data. Consent, while the preferred method contained in the Directive, it is one of six legal basis. Article 7 reads:

> Member states shall provide that personal data may be processed only if:
> (a) The data subject has unambiguously given his consent;
> (b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
> (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or
> (d) Processing is necessary in order to protect the vital interests of the data subject; or
> (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
> (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject, which require protection under Article 1(1.) (which covers the objectives of the Directive).

There has been more attention placed on the five legal basis beyond consent as Europe has debated the new proposed regulation to replace the Directive. Of particular interest has been legitimate interests, Article 7, Section (f). Legitimate interest has not been heavily used in southern Europe\(^9\). However, the growth of the Internet and the emergence of the Internet of things, the cloud and big data have caused the WP29 to revisit the use of legitimate interests as a legal basis. In Spring 2014, the WP29 issued an opinion on the use of legitimate interest, seeking comments on the draft guidance. The opinion said that the correct legal basis should be

---


\(^9\) Many Latin American data protection laws are based on southern European laws, mostly the Spanish law, but also the Italian law.
used based on the nature of the processing. For example, WP29 found that the appropriate legal basis for processing data to prevent fraud should be legitimate interests and not consent. The requirements for using legitimate interest are very robust. One must conduct a balancing-of-interests analysis. The analysis must take into the consideration the legitimate interests of the controller and all interests of individuals affected by the processing. The controller must then stand ready to demonstrate the process to a data protection commissioner when asked. The capabilities for conducting such an analysis come with having a comprehensive privacy program.

Accountability and Comprehensive Programs

There is a growing awareness that effective privacy protections require data controllers to be responsible stewards of the data they process. That data stewardship needs to be grounded in recognised external criteria such as law, regulations or guidelines. That concept of data stewardship comes directly from the OECD Guidelines. Guidelines when based on industry standards may be referred to as self-regulation. There is a growing consensus that such self-regulation should be binding on organizations through enforceability by regulators. In the United States, many industry codes and even the EU/U.S. Safe Harbor requires an organization to announce its participation so the U.S. Federal Trade Commission can enforce against a lack of compliance as a deceptive act.

The OECD Accountability Principle 8 reads: A data controller should be accountable for complying with measures which give effect to the principles stated above. For most of the thirty-four year history of the OECD Privacy Guidelines, the accountability principle has sat dormant. The Canadian private sector privacy law (PIPEDA) contains a set of principles with the first one accountability. The APEC Privacy Framework contains principle 9 on accountability. As data processing became more complex and more data originates at distance from the individual, there was more discussion about creating guidance to give some direction to accountability. In 2009, the Global Accountability Dialogue was created as a multi-stakeholder collaboration. Year one was in Dublin with the Irish Data Protection Commissioner as the facilitator. The dialogue report for year one contained the essential elements of accountability:

- Organisational commitment to accountability and adoption of internal policies consistent with external criteria;
- Mechanisms to put privacy policies into effect;
- Systems for internal, ongoing oversight and assurance reviews and external verification;
- Transparency and mechanisms for individual participation; and
- Means for remediation and external enforcement.

The essential elements are the outline for a privacy programme that has the capability of driving the responsible use of data pertaining to individuals. Canadian Regulators took this a
step forward by issuing “Getting Accountability Right with a Privacy Management Program”\textsuperscript{10}. The guidance is broken down into two parts. The first part contains the building blocks necessary to build a privacy programme, while part B discusses how to maintain and improve such a programme. The presence of such a programme is enforceable under the Accountability principle contained in the laws.

The Hong Kong privacy commissioner issued similar guidance in 2014. The Hong Kong guidance is a strong suggestion and not enforceable under Hong Kong law.

Accountability concepts and incentives to develop accountability programmes are also present in privacy laws in Colombia and Mexico. Accountability is explicitly part of the EU draft regulation that if enacted will replace the directive.

The United States Federal Trade Commission has also required comprehensive programmes as part of the consent decrees it uses to resolve enforcement.

**Conclusion and Recommendations**

Privacy law is hard to draft and hard to enforce, since we as individuals have conflicting expectations. Our social self wants recognition and is very curious about others, while our private self wants to be shielded from the view of others. For example, we want the personalisation that comes with observation on the Internet, yet we do not want to be watched. Finding an equilibrium between the social us and the private us is very difficult and is often based on the context of the interaction. This is further exacerbated by the pace of change in information and communications technologies. It took four thousand years to go from writing to the printing press, but it took less than sixty years to go from mainframe computers to mobile phones with more computing power than the old mainframes. The nature of data has changed as well. In 1967, when “Privacy and Freedom” was published, most data was provided by the individual in a way the individual truly understood. Today, observational and inferred data dwarfs the data that we provide. This changes the basic governance equation. While governance through individual consent was very effective in 1972 (when the first privacy laws were enacted), consent is much less effective—and sometimes not even feasible—in governing the applications driven by observed and inferred data.

Modern economies are driven by information in the same way economies in the last century were driven by steel and big machines. Privacy policy must work with industrial policy to create a successful environment for people. Privacy risk and reticence risk that prevents good uses of data are both dangerous.

My suggestions are as follows:

(a) Legislators, whether in Brazil or in other jurisdictions, should begin with well-articulated goals for privacy legislation and test to assure the legislation will actually achieve the goals. Furthermore, the legislative process should recognize that privacy is one of a number of individual rights that should be respected. Those rights include broad sharing of the fruits of technology. Privacy and innovation must go together.

(b) Privacy laws should be principles-based and technologically neutral, specify outcomes rather than specifying the details on how those outcomes might be achieved. The mechanisms will change as technology continues to evolve.

(c) Data security should not be assumed. However, the law should require levels of security that are proportional to the risks to individuals. The law should not specify how organizations would meet the specification. Security risk threats change over time, and security becomes a journey. The law cannot anticipate the journey’s path.

(d) Governance should not depend on a single legal basis to process such as consent but rather a full toolkit of legal basis such as assuring an individual’s broad interests in life and happiness and an organization’s interests as well. The balancing parameters should be spelled out in the law, but the mechanisms to do so should be left to a regulatory process. Consent is an important legal basis and should be the governing instrument where it is effective. However, consent is one of many legal basis and should not be forced where it is not effective.

(e) Individuals have a right to understand how data that pertains to them will be used. This interest goes well beyond the knowledge that might come from a purpose specification notice.

   i. Therefore, openness about how data is used and organizations programmes should be a requirement in the law.

   ii. Furthermore, companies should be required to provide individuals access to data that pertains to them subject to reasonable procedures for authentication and shielding data that might be used to commit fraud.

   iii. There is data that should not be subject to access. For example, data that has intentionally had any linkage to the individual removed should not be subject to access, because doing so would remove the protections associated with de-identification. ¹¹

(f) The law should require comprehensive privacy programmes proportional to organisational complexity. There are excellent descriptions of comprehensive programmes in materials supplied by the global accountability project and by enforcement agencies in Canada and Hong Kong. The requirements should be scalable to organisations of all sizes and complexities. To facilitate scalability industry associations should be encouraged to develop best practices programmes that would be reviewed by enforcement agencies and could be adopted by industry

¹¹ De-identification is a methodology that removes the identifiers from a data set and replaces with a key. De-identification is often used in research where data is matched by one party, but the research is conducted by another. The first party, which does the matching, may be able to provide access to data. However, the researchers using the data should not have the means to re-identify. If they had the linkage, they would have means to take action against individuals. Without the linkages, they can discover trends without knowing who the people are. Providing the means to do so would defeat the protections from de-identification.
players. Spanish data protection law allows the enforcement agency to reduce fines if an organisation is able to demonstrate a comprehensive programme. Such incentives should be considered.

(g) The law should give standing to regulatory agencies to ask organisations to demonstrate their programmes, but there should not be a blanket requirement that every company have their programmes approved.

(h) Regulatory agencies should have the resources to monitor the market, develop guidance and create a high level of certainty that non-compliant organisations will be caught.

(i) Data registration has served no purpose so should be avoided in any privacy law. Data registration was originally seen as a means for individuals to discover which companies process data. Now, every company is a processor, and such a list has no value.¹²

One final note, privacy law is driven by human values. Those values have been a constant during recorded history. However, technology does affect the mechanisms that make the values work. Privacy law should recognise the values while leaving room for guidance as the mechanisms change over time.

¹² Data registration was a requirement of many early data protection laws. Data registration requires all controllers to register databases with data protection authorities. In the 1970s, when the requirements first appeared the reasoning was that databases were few, and by looking at the registry, individuals would see the names of the companies with databases. There is no record of individuals actually doing so in decades. The proposed regulation in Europe would eliminate registration.