GDPR AND THE PRIVACY SHAKE-UP

Time to Abandon Zero-Sum Models and Shift to Positive-Sum Thinking

April 2018

GLOBAL PRIVACY AND SECURITY BY DESIGN

DATA Catalyst

Shift to Positive-Sum (Not Zero-Sum) Thinking

With the due-date for implementation of the GDPR fast approaching, it is clear that this new European privacy regulation has been shaking up businesses world-wide, not to mention putting a spotlight on outdated privacy laws in other jurisdictions. This paper will recommend considering the benefits of Privacy by Design's approach to privacy -- addressing multiple interests in addition to privacy, which inevitably leads to improved privacy governance.

GDPR and the Privacy Shake-up: Time to Abandon Zero-Sum Models and Shift to Positive-Sum Thinking

Ann Cavoukian, Ph.D., LL.D. (Hon.), M.S.M.
Creator of Global Privacy and Security by Design
Distinguished Expert-in-Residence, Privacy and Data Analytics
Privacy by Design Centre of Excellence, Ryerson University, Ontario, Canada
Email: ann.cavoukian@ryerson.ca

Acknowledgements: The author wishes to acknowledge the contributions of Michelle Chibba, Ryerson University and Jake Ward, Data Catalyst, for their input and feedback on various drafts of this paper.

The Perfect Storm

The implementation of the European Union's General Data Protection Regulation (GDPR) in May of 2018 introduces new obligations for any organisation that handles data about EU citizens, whether or not that organisation is located in the EU. The new pan-European privacy framework is ambitious, and at times, complex and strict. The impetus of the European efforts and the domino effect cascading on other jurisdictions with outdated privacy laws, creates the need for, and an opportunity to create innovative, effective privacy frameworks that are sustainable and positive sum – win/win!

This regulatory action is a result of the last two decades over which the Internet entered has into a new phase. It is no longer just a communications network, but rather, a platform for computing -- a vast, interconnected, virtual supercomputer. This new digital ecosystem presents complex security and privacy challenges. Legitimate data transactions raise privacy concerns, particularly as geo-location data becomes more personally identifiable with the increased use of mobile devices. In this era of ubiquitous mobile, social and cloud computing, we are producing unprecedented data points, and in turn, losing control over our personal information. Questions are being raised -- What will privacy mean, and how will privacy survive, let alone thrive, as a viable human right, operational value, and critical enabling trust factor, in a world where the individual is less and less directly present in the midst of data-rich transactions? Privacy equals control – personal control over the uses of one's personal information.

Against this backdrop of radical technological advances, and the Snowden revelations unearthing massive surveillance, you have the unraveling of a privacy regime that was considered adequate to support cross-border flows of personal data from Europe to the U.S. In 2015, the European Court of Justice invalidated the Safe Harbor Agreement, declaring Safe Harbor inadequate; the EU-US Privacy Shield was then established in 2016, in an effort to replace Safe Harbor (which has yet to be determined).

Here in Canada, there are no fewer discussions or questions about the readiness of companies to meet these challenges in time for May of 2018. Likewise, questions about the adequacy of Canadian privacy regimes to the new European reality are being raised. Indeed, in a recent talk, Canada's Privacy Commissioner, Daniel Therrien warned that, "Canada could face European adequacy issues in light of the new regulation" and indicated that he has been urging the Canadian Federal government to upgrade our privacy laws,[1] recommending that Privacy by Design be included. He noted: "Organizations must also be more transparent and accountable for their privacy practices. Because they know their business best, it is only right that we expect them to find effective ways, within their own specific context, to protect the privacy of their clients, notably by integrating approaches such as Privacy by Design."[2] Other privacy experts and stakeholders have also weighed in on the impact of the GDPR to Canada's privacy laws, including implications for small and medium-sized businesses.[3] [4]

[1] https://iapp.org/news/a/canadian-privacy-commissioner-announces-proactive-approach-to-enforcement/

[2] https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1

[3] http://www.colinbennett.ca/data-protection/is-canada-still-adequate-under-the-new-general-data-protection-regulation/

[4] https://www.itworldcanada.com/article/canadas-privacy-laws-need-to-be-be-updated-but-dont-look-to-europe-or-the-us-for-guidance-canadian-experts-say/385134

So many events over the last two decades have strongly pointed to the need to improve privacy policy, and data-driven policy overall. The importance of privacy cannot be overstated. In an increasingly interconnected world, both government and industry have a shared responsibility to guard against overreach.

Enter Privacy by Design

Privacy by Design (PbD) is a set of seven foundational principles that serves as an overarching framework for proactively embedding privacy and data protection measures into the design of one's operations, right from the outset. By adding such measures effectively and credibly into information technologies, organizational processes, networked architectures and, indeed, entire systems of governance and oversight, much greater protections will be afforded. There are multiple goals that will be realized: ensuring greater user control, enhancing transparency, and creating greater confidence and trust. The 7 Foundational Principles that form Privacy by Design (see Figure 3) express not only the universal principles of Fair Information Practices (FIPs) but also incorporate a design-thinking approach. Integrally linked, the principles address the need for robust data protection and an organization's desire to unlock the potential of data driven innovation. Just as with the GDPR, the concept of Privacy by Design first started to take shape in the late-1990s. As the author of PbD, the need to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems was clear.

The future of privacy could not be assured solely by compliance with regulatory frameworks that dealt with privacy breaches after the fact; rather, proactive privacy assurance had to ideally become an organization's default mode of operation.

Over the years, a zero-sum paradigm has prevailed, in which one value, such as privacy, competed with another value, such as security, in a zero-sum "win-lose" equation: The thinking went somewhat along the lines of — in order to have adequate security and protect ourselves against the threat of terrorism, we must forfeit our privacy. This notion, however, is based on completely flawed logic and a false dichotomy — that privacy and security must be considered as mutually opposing, which is simply not the case! Privacy can and must co-exist alongside other critical requirements: security, functionality, operational efficiency, organizational control, business processes, and usability in a "positive-sum" or doubly enabling "win/win" manner. By doing so, I believe that Privacy by Design will assist in creating a more desirable culture of privacy which I have been advocating for many years. This culture of privacy emerges when organizations view privacy not as a compliance issue, but as a business issue. It is what takes hold when the leadership of an organization comes to see that the implementation of positive privacy controls creates—rather than constrains—business opportunities.

In short, it is a culture of “win-win” or positive-sum. This is not to suggest that Privacy by Design should be applied in a vacuum. It is a critical part— but only a part—of a suite of privacy protections that includes regulatory instruments, consumer awareness and education, accountability and transparency, audit and control, and market forces.

Approaching privacy from the level of code is a significant shift from traditional ways of thinking about data protection. Just as PbD represents a shift in the way that organizations must think about privacy – moving from a reactive mode to a proactive one – enshrining PbD into regulatory instruments, voluntary codes, and best practices, requires a shift in how law and policy makers approach rule-making in this area. PbD represents the next generation of privacy protection – it invites the development of innovative approaches to promoting and enshrining privacy in various instruments. The goal of laws related to their application should be sustainability, and a lack of unintended consequences, incorporating flexible, forward-thinking approaches like PbD. This requires a paradigm shift in thinking of privacy as a business issue, not simply relating to it as a matter of regulatory compliance.

Incorporating PbD into a country’s legislative body is not without its challenges. Not only must a country explore what kinds of instruments are appropriate, but also how to interpret PbD. The principles of Privacy by Design can inform both the end state (e.g. privacy as the default), and the process for arriving at the end state (e.g. end-to-end, full lifecycle protection). In the process, governments should always consider that PbD provides a baseline for embedding privacy considerations into legislation, and that PbD’s as we presence throughout the business world is becoming more and more the norm.

As we in Canada look to the future, we want to shape our strategies for privacy and data governance, and given that the GDPR also includes Privacy by Design (Data Protection by Design), and Privacy as the Default, there are key features of the Privacy by Design framework that we may consider as we move forward.

Figure 3: 7 Foundational Principles of Privacy by Design

1. Use proactive rather than reactive measures, anticipate and prevent privacy invasive events before they happen (Proactive not Reactive; Preventative not Remedial).

2. Personal data must be automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact (Privacy as the Default).

3. Privacy must be embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. (Privacy Embedded into Design).

4. All legitimate interests and objectives are accommodated. (Full Functionality — Positive-Sum, not Zero-Sum).

5. Security is applied throughout the entire lifecycle of the data involved. (End-to-End Security — Full Lifecycle Protection).

6. For accountability, all stakeholders are assured that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. (Visibility and Transparency — Keep it Open).

7. Architects and operators must keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options (Respect for User Privacy — Keep it User-Centric).

Privacy by Design Essentials: The 3 C's (Consultation, Cooperation, Collaboration)

The main features that make Privacy by Design especially relevant as we prepare privacy regimes to meet the needs of the 21st century, are as follows:

i) Taking a proactive, problem-solving approach lies at the heart of PbD (Principle 1). PbD makes privacy a foundational requirement, anticipating and preventing privacy-invasive events before they happen -- it's a model of prevention. A critical success factor in this approach is that the regulator must also be adaptive. In fact, Canada's privacy commissioner signalled last year that his office plans to initiate a 'consumer-focused', 'proactive approach' where the Office would find a way to work with companies to identify gaps that can be addressed before any serious problems occur.[5] Frameworks created without the benefit of input from industry, particularly small businesses, deny themselves a uniquely valuable perspective, readily available and increasingly essential.

ii) The principle of full functionality requires going beyond making privacy declarations and data protection commitments, to demonstrating how all data processing and other objectives have been, and are being, satisfied (Principle 4). When embedding privacy and data protection into a given information technology, process, system, or architecture, it should be done in such a way that full functionality is not impaired, and that all legitimate interests relating to both privacy and security are accommodated, and requirements optimized.

Privacy and data protection are often positioned in a zero-sum manner; that is, as having to compete with other legitimate interests, design objectives, and technical capabilities in a given domain. Privacy by Design rejects taking such an approach – it embraces legitimate additional objectives and accommodates them in an innovative positive-sum manner. All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and unnecessary trade-offs or unintended consequences rejected, in favour of finding a solution that enables multi-functionality, multiple stakeholder interests.

[5] https://iapp.org/news/a/canadian-privacy-commissioner-announces-proactive-approach-to-enforcement/

These are the benefits that make Privacy by Design stand out as a global privacy framework -- the principle of being proactive about privacy and the principle of inclusiveness regarding objectives and interests (positive-sum) are essential and should be carried out with three key words in mind: consultation, co-operation, and collaboration (3 C's). Consultation keeps the lines of communication open. Cooperation is emphasized over confrontation to resolve possible differences. Collaboration is sought proactively by seeking partnerships to find joint solutions to emerging privacy and security issues. The development of a shared understanding assists in facilitating a focus on the privacy rights of the individual and the achievement of innovative, user-centric results. As always, the aim is to understand and be responsive to all the perspectives involved, by adopting this methodology.

Use Positive-Sum not Zero-Sum Models

Additional recognition is garnered for creativity and innovation in achieving all objectives and functionalities in an integrative, positive-sum (win/win) manner. Entities that succeed in overcoming outmoded zero-sum (either/or, win/lose) choices are demonstrating global privacy leadership. Privacy by Design challenges policymakers, executives, technologists, and designers, to find ways to achieve better privacy and data protection in a given technology, system, or domain than is currently the case,, and to be able to document and demonstrate achievements so that others may learn from them, making them ultimately become best practices. Why couldn't this be applied to privacy regulatory schemes?

The privacy landscape continues to evolve. So, like the technologies that shape and reshape the world in which we live, the privacy conversation must continually renew and sharpen its focus. These days, the stakes are high; perhaps higher than they've ever been before. Privacy will continue to come under increasing pressure from many different forces including online social networks, an explosion in social media, governments and businesses providing services that are highly individualized and information-dependent.

The flawed view that privacy, in and of itself, stifles innovation is simply a myth. It consists of a false dichotomy, built upon unnecessary trade-offs. The opposite is true: prioritizing privacy drives innovation! It forces innovators to think creatively to find solutions that serve multiple interests and functionalities.

But how will privacy survive, as the foundation of our freedoms, driver of prosperity, operational value and critical enabling trust factor in a world where the individual is rarely present to assert control over their personal information, in the midst of such data-rich transactions? The future of digital privacy may well depend upon changing the current online paradigm.

For some time, I have said that a new "playbook" is needed. We need to abandon zero-sum (win/lose) thinking and adopt a positive-sum (win/win) paradigm where both innovation AND privacy may be achieved. Adopting Privacy by Design is a powerful and effective way to embed privacy into the "DNA" of an organization in order to establish a solid foundation for data analytics that support innovation, without compromising privacy. I have referred to this as the "Privacy Payoff" – protecting customer privacy yields big returns – from increased consumer confidence and enhanced customer trust, to gaining a competitive advantage. This is where privacy acts as a significant differentiator. I consider the need for this new playbook to be so vital, that I recently formed a new Council -- The International Council of Global Privacy and Security, by Design.

[1] https://iapp.org/news/a/canadian-privacy-commissioner-announces-proactive-approach-to-enforcement/

This international council is all about advancing both Privacy and Security, by Design not just within large enterprises, but to spread the message so that even small and mid-sized organizations not only recognize the value of making privacy and security essential, but can also implement this approach in a proactive manner.[6]

To design practical yet effective privacy and data protection in a given information technology, organization, or networked architecture, privacy architects typically need to take into account multiple legitimate (and, yes, at times competing) interests, and accommodate them in optimal, innovative ways.

[6] Global Privacy and Security by Design. Globe & Mail. January, 24, 2018. https://www.theglobeandmail.com/report-on-business/former-ontario-privacy-commissioner-forms-global-council-seeks-funding-for-research/article37720201/

Global Privacy and Security by Design

So, while we are in the perfect storm and disruption of privacy regimes as we approach implementation of GDPR, I am taking the 3C's approach to reaching a 'win-win' solution to bring particular attention to dispel the commonly held view that organizations must choose between privacy and security, or privacy vs. business interests (i.e., "big data" analytics). The Council's goal, ideally everyone's goal, is to educate stakeholders that public and private-sector organizations can develop policies and technologies where privacy and security, privacy and data analytics, can work together to achieve positive-sum, win-win outcomes. Towards that end, we will also be pursuing the development of leading-edge, technologies of privacy such as SmartData -- technologies of freedom! The International Council on Global Privacy and Security by Design will work with companies, national privacy commissioners and technology professionals, including international NGOs such as Data Catalyst, to educate the public and raise awareness for Privacy by Design. We also acknowledge that small business is big in Canada: Small businesses are the engine of the economy, their success is vital to Canada's prosperity,[7] [8] and their contributions essential to writing effective, well-informed data privacy regulation.

The Council's third goal is to collaborate with policy designers in both government and business, in the hopes of tearing down the traditional "silo" approach to developing privacy strategies.[9] A more integrated approach to solving the challenge of privacy, one that includes stakeholders from conception through execution, will result in more informed, effective, and sustainable national and international privacy rules, to the benefit of all involved.

[7] According to the Business Development Bank of Canada, 98.2% of all businesses have fewer than 100 employees. When you add in medium-sized businesses (100 to 499 employees), the percentage rises to 99.8%. This is also true for other jurisdictions around the world according to a World Bank report: http://www.worldbank.org/en/news/feature/2014/06/03/small-and-medium-enterprises-the-engine-of-an-economy-sustained-by-sound-financial-reporting

[8] The Privacy Toolkit for small and medium-size businesses is a joint initiative between Hewlett Packard Enterprise and Privacy by Design Centre of Excellence at Ryerson University. http://h41111.www4.hpe.com/privacy-toolkit/overview.html

[9] https://www.itworldcanada.com/article/you-dont-have-to-sacrifice-privacy-for-security-says-former-ontario-privacy-commissioner/401517

Conclusion/Recommendations

The implementation of the GDPR in the European Union (and all businesses that do business with Europe) is rapidly approaching. There are many facets of the GDPR that are meaningful and progressive. The inclusion of Privacy by Design (Data Protection by Design) as a central pillar is essential to its success, as well as a lesson to be learned by countries creating their own data privacy framework.

The timing is right for Canada and other jurisdictions that are starting from scratch or reviewing existing privacy regimes, not only to include Privacy by Design, but also to be reminded of the 2010 Resolution advanced by International Privacy and Data Protection Commissioners, which was unanimously passed, that resolved to: "Foster the incorporation of the Privacy by Design Foundational Principles in the formulation of privacy policy and legislation within their respective jurisdictions." Since then, Privacy by Design has been translated into 40 languages, giving it a true global presence!

Privacy protection and data regulation are not an exercise in duality, but rather an essential collaboration between business and government. For governments working toward sustainable solutions to regulating dynamic industries without unintended consequences, now is the time to engage those industries. Start with Privacy by Design as a central tenet, taking a positive-sum, win/win approach by bringing small and mid-sized businesses to the table, along with policymakers, to create an integrated process that welcomes all stakeholders: the end-result will yield a far better outcome, one that reflects a privacy designed governance structure: win/win!