The Mid-Atlantic Privacy Compass

This text by Privacy Commissioner Alexander McD White was first published in the Compass Point Blog Series between April and May 2020. Three years on, it is especially topical, and we are republishing it as a paper.

Executive Overview

Privacy & Ethics

- Ethical behaviour should always be an organisation's true north. An organisation's ethics inform their sense of corporate responsibility and must be valued as much as profitability.
- Organisations should develop Deliberate Ethics, a process for considering and formalising ethics within their operations through both an ethical framework and the mechanisms to implement it, such as ethics review processes and advisory boards.
- Particularly, organisations working in advanced technology that move more quickly than laws and regulations must recognize their responsibility to engage in ethics-by-design and demonstrate their accountability.

Privacy & Responsibility

- Organisations must reject the notion that innovation and speed require sacrificing values and embrace the possibility of "Privacy and…" not "Privacy or…."
- Innovative organisations, regulators, and other stakeholders must work together to develop well-defined systems of collaboration to allow innovation in responsible ways that respect rights. Ideas and technology can then be tested in recognized and formalized trials and "Sandboxes" that allow for a controlled environment and due consideration of various factors.
- Restrictions on activities can be challenging, but challenges often inspire greater and more innovative creativity. Acting responsibly means that organisations cannot trample on rights simply to take the easy path.

Privacy & Oversight

- Oversight means more than the actions of regulators. It can happen through courts, economic markets, self-regulatory schemes, and citizen action.
- Organisations should engage with regulators, civil society, and other stakeholders as trusted advisors. No party should hold a confrontational, cat-and-mouse mind-set, but should seek proactive and constructive engagement.
- Rights and privileges can only be protected if all groups work in collaboration. With the goal of providing individuals with understanding and assurance, businesses must embrace the value of oversight groups, and vice versa.

Privacy & Community

- All parties are interconnected. We must exchange ideas and learn from each other. Too often, fear of regulatory action or negative public opinion prevents an organisation from discussing its mistakes or misfortunes.
- Both individuals and oversight groups should recognize that no one is perfect, and organisations must reward that trust by prioritizing community as highly as self-interest.
- We must develop a new Data Protection Social Contract to recognize common interests and ensure we work together effectively, not only in the use or analysis of data for the public good, but also in learning and improving.

Privacy & Individuals

- Use of personal information should keep the individual at its heart, and the organisation's relationship to the individual should guide its decision-making.
- Respecting the rights and preferences of the individual builds trust and deepens the relationship.
- Tandem individual and corporate actions are needed to protect privacy, not an adversarial, oppositional approach.

Privacy & Stewardship

- An organisation, and people in general, should be a steward in all things. This principle extends to communities, the natural environment, and to data.
- When individuals provide personal data to organisations, the entity must take the mind-set that the data is only temporarily in their care and they are acting on the individual's behalf, as a formal agent or otherwise.

Privacy & Incentives

- Incentives should be embraced at every level to ensure that persons, organisations, and economies are structured in an ethical way that encourages win-win achievements with privacy and other, complementary goals.
- Organisations should structure their business goals to encourage employees to seek achievements related to ethical behaviour or building individual trust. Consent-based models which only incentivise getting agreement, not necessarily giving a full disclosure or receiving true buy-in, should be avoided.
- Oversight should create an environment that focuses on the true issue of preventing harm, not punishing noncompliance. A focus on noncompliance may have the perverse effect of rewarding the unscrupulous who save time and effort by not trying to comply. Merely financial penalties make rights abuses a cost of doing business.
- All parties should collaborate to create tools and resources to help all others comply with standards and support individuals' rights, for the sake of a level playing field and to encourage a healthy market. Small enterprises should not be punished for lack of resources to implement complex compliance programs.

Privacy & Interoperability

- Thanks to the emergence of global platforms like the internet, privacy laws around the world have a kinship or descendancy, and have converged to present a consensus on international standards. Whether formally or otherwise, the regulations and guidance in foreign jurisdictions have a persuasive effect.
- Both principles- and risk-based regulation require organisations to conduct a bespoke analysis of their actions and context. While regulatory compliance floors may differ, a focus on a neutral analysis that mitigates the true harms will most benefit individuals.
- Organisations should focus on Interoperability with legal regimes, technological platforms, and even future developments. They should be encouraged to develop practices that apply regardless of jurisdiction or technology, as long as the goal is to support individuals' rights.

Introduction: Mid-Atlantic Privacy. The Middle Way

Bermuda sits at the crossroads of the Atlantic physically, culturally, and economically. This has long been to the island's benefit, claiming the best of multiple worlds to create a prosperous and successful community.

From a data protection standpoint, there are two schools of thought on each side of the Atlantic Ocean, or so the stereotypes go. Europe calls for respect for individual rights to privacy, while the United States encourages a free-market, business-friendly approach. Many organisations and even countries now appear to find themselves in the position that Bermuda has been in, so often throughout its history, of being forced to choose a side.

But Bermuda has shown that this is a false dichotomy. As has happened so often before, instead of choosing a side we must look to forge a new path, taking the best of both worlds. This may mean embracing flexibility and, at times, a certain sense of uncertainty as we work through novel issues. Following a different way, the middle way, has the potential to succeed in the spirit of both ideologies. This is the goal of Mid-Atlantic Privacy, a guiding philosophy that I have been developing since my earliest days as Privacy Commissioner.

We are often confronted with questions asking which is more important: Business or privacy? Innovation or individuals? Prosperity or rights? We must reject the narrative of "or" and seek win-win solutions. Instead of zero-sum games, we must focus on "Privacy and…." We must find a way to give the highest respect to individual rights to privacy—but do so in a business-friendly way, that shows the work's value to both individuals and organisations.

Why should we choose between business success and rights? Particularly in the field of data protection, the two are intimately linked, with many organisations seeing the harvest of personal data as a way to make a quick buck (or euro). But in addition to the moral imperative of implementing a privacy program, for most if not all organisations, doing so will help the business become more efficient and mature in how it operates. Its data stores will become more organised and more lean, narrowly tailored to the goals they wish to achieve, and thereby reducing excess risk of harm to people and to the organisation's solvency.

Standing between the competing—though converging—privacy ideologies on both sides of the Atlantic, there is still a wide swath of common ground. How can businesses identify practices that are universally useful for compliance and the true goal of reducing risk? By focusing on this common ground, organisations can rest assured that the time and effort they invest will serve them in good stead no matter which regulator may come inquiring. They can reduce their compliance costs by not duplicating efforts, even if it means going beyond what is legally required by the more lax of the regulations. By focusing on the commonalities and the true risks involved, we cut to the heart of the matter: protecting the rights and respecting the preferences of individuals.

As a regulator and in society more broadly, we must ask what may be the best methods to promote good, responsible behaviour in organisations that are stewards of data. In what ways should we challenge them to continue their useful and socially-beneficial innovation while respecting privacy? Despite everyone's natural resistance to limitations, challenges are in fact the best tool for creativity: nothing is more daunting than the "blank page," but place a speck on it and an artist can craft an entire world. Our brains are built to respond to puzzles and challenges, so how can we structure incentives and other mechanisms to trigger that genius?

Privacy is critical to the success of our modern societies, but we must remember that in and of itself, privacy is not necessarily the goal. Privacy helps our democracies to function by protecting freedoms of assembly and secret ballots. It enables our economies by helping us trust one another in online or other marketplaces where we do not know the other party. And as we all get shown more and more "personalized content" or advertisements, we may be getting completely different information than other people. Privacy supports the very integrity of our minds and decision-making.

These are complicated matters. As we keep learning in the world of data protection, there is not, and could never be, a manual for every situation and context. And we cannot simply act as a balloon and blow wherever the wind may take us. Instead we should build a sail that can harness those winds, and turn to a compass to help us navigate them.

Ethics are Your True North

North has always had a point of primacy on the compass rose, and there's no better concept to place in this honoured spot than Ethics. Ethical behaviour should always be an organisation's true north, the central focus from which all other ideas radiate. Many of the privacy decisions that an organisation makes are ultimately a matter of ethics, as they consider what may be the right thing to do, how to meet promises they have made, and what the expectations may be of the individual subject of the data.

We are starting to see more organisations, management bodies, and industry groups recognise that we have created an imbalanced society by placing quarterly returns and shareholder profits above all other considerations. Short-term mind-sets lead to irresponsible exploitation of individuals or common property. If organisations are to be more than merely financially successful, are to become socially successful forces for good in our communities, they must place a higher value upon ethical behaviour.

Many organisations support corporate responsibility efforts, which can fall under many headings. It could be charitable giving of time or money, responsible treatment of natural resources and the environment, or consideration of how data and technology can be used for the public good. I applaud these efforts but maintain that our support for ethics must go further: we must consider maintaining ethical standards to be at least as important as making a profit.

Ethical behaviour will not happen by accident or in an ad hoc manner, which is why I am proposing the idea of Deliberate Ethics. If you'll pardon the wordplay, organisations must be deliberate in choosing to embrace ethics, and they must deliberate carefully on the goals and mechanisms they choose. The manner in which Deliberate Ethics is executed may vary from organisation to organisation, but what should be consistent is the presence of an identified process for thinking through and weighing these issues.

As with other organisational policies and procedures, ethics must be formalised and documented so that expectations are clear and the ethics process may be examined. Ethical review processes and advisory boards are two mechanisms that forward-thinking organisations have implemented recently. Whatever the mechanism an organisation chooses, it must be empowered with a voice and authority to effect change. The privacy principle of Accountability provides considerations for documenting and demonstrating due diligence in this regard, among others.

Organisations working in advanced technology or using data or technology in innovative ways must recognise that they have a special responsibility. They will often be moving more quickly than the laws which regulate their behaviour, so ensuring Deliberate Ethics is especially important. With the glory of blazing a new trail comes the responsibility for personal and societal impacts.

By putting into effect ethics-by-design processes, ensuring their ability to demonstrate accountability, and documenting the steps they took to behave properly, organisations can maintain the trust of the public and stakeholder groups - and never lose sight of their true north.

Responsibility, Collaboration, and Creativity + Bermuda's Pink Sandbox

For the purposes of the Compass, Responsibility is found where Ethics and Oversight meet - where knowing the right thing to do meets knowing that you will be held to account. Organisations must take ownership over their actions and reject the notion that innovation and speed of operations require sacrificing values.

Often, privacy is framed in the context of counterbalances, as we have been told we must choose between privacy or technological advances, or national security, or any number of other laudable goals. As I've written in the Mid-Atlantic Privacy introduction, this is a false dichotomy. Privacy is essential to the functioning of our societies, so solutions by their very nature must embrace privacy as an essential element. The solution is not to choose "privacy or" something else but to develop a strategy for "privacy and ..."

To continue our nautical metaphors, privacy is not an anchor but is more like ballast - an essential component that improves the stability and functioning of the ship. If we omit it for the perceived sake of expediency, we only create problems that will arise when the seas get choppy.

Responsibility does not solely fall on organisations. Oversight bodies and stakeholder groups have a responsibility to participate constructively in the process. All of these participants are needed to develop well-defined systems of collaboration so that technological and data processes are formed in responsible ways that respect the rights of the individuals. The burden cannot be placed only on the organisations - everyone must share the load.

Regulators around the world have developed "sandboxes," or structures where innovative organisations can test and experiment in a controlled environment and in close coordination with oversight expertise.

Of course, we know something about sand here in Bermuda, which is famous for its pink-tinted beaches. With that and the Compass Point of Responsibility in mind, I am delighted to announce just such a local program to assist organisations through direct input from my office: the Privacy Innovation and Knowledge-sharing (or, "Pink") Sandbox. I will be announcing more details in due course, but if your organisation might like to participate, please contact me to express interest. By the nature of our community, we are a collaborative space where interactions between participants are convenient. I am sure you will find Bermuda to be an ideal testing ground.

Some organisations resist these types of programs as limitations or restrictions. Again, I make the argument that restrictions are a critical component of any creative process and can inspire greater success. Recall the story of the NASA engineers helping Apollo 13 return home, forced to build an air filter using only the spare parts already on the spacecraft. Or pianist Keith Jarrett, who in a live jazz concert in Cologne played perhaps his greatest performance, in part because the piano he was using had poor playing keys that he was forced to avoid. Challenges can help us become more innovative, making different connections in our brains to solve puzzles in new ways.

Responsibility means learning to operate in challenging circumstances. It means that organisations cannot simply take the easy way. They must consider their ethical responsibilities and individuals' rights, and become more inspired for it.

Constructive Oversight

Oversight is critical to the healthy functioning of a community's sense of social responsibility. Power and privilege must always be held to account for their actions and the consequences.

Traditionally, oversight is seen to come from regulatory offices, like this one. In fact it may come from many sources, as courts and the judicial system investigate legal duties, as each of those mythical "rational" persons exerts pressure based on their purchasing power and decisions, as the business community polices itself through self-regulatory commitments and legally binding agreements, and through collective citizen action. In many ways, data protection authorities such as the Office of

Privacy Commissioner for Bermuda are merely a subset of that last category, the holders of delegated power from the citizens - via our government - in order to protect their rights.

Unfortunately, the relationships between oversight groups and the organisations they supervise often sour into forms of confrontation, with one side seeing its role as playing a game of "Gotcha" and the other seeing its own role as grabbing everything it can until it gets caught. These mind-sets result in distorting behaviour on both sides and reducing the effectiveness of regulatory efforts.

Oversight bodies, particularly regulators, should keep in mind that their role is to protect and mediate, and create Incentives to focus on the true issue of preventing harm, not punishing noncompliance. They should seek proactive and constructive engagement to help organisations learn the merits of protecting privacy rights. The goal should be to show businesses how maturing their privacy processes can lead to both more trustworthy and efficient operations

Rights may only be successfully protected through good faith efforts by all parties to create a healthy ecosystem that can withstand the occasional bad actor. Businesses need the trust of their customers or else no one would provide their personal data, and they also need to ask individuals to behave in certain ways to express privacy preferences or protect data from breach. Oversight bodies can form the bridge of trust between those two groups, lending authority to each side to help the community as a whole develop good data hygiene. By inviting oversight's involvement, organisations can ensure that their responsibilities, and the limits of those responsibilities, are understood in the community.

But the ask - for organisations to go out of their comfort zone to invite in oversight - cannot be only one-way. Oversight bodies, being government or nonprofit entities, can often be conservative in their own risk-taking, but we must also be brave. Just as the data processing organisations must earn the trust of individuals, oversight must earn trust to maintain our place in the process. We should reach out to and reward organisations who make good faith efforts.

The exact form of these outstretched hands may vary by the body's form or powers, but as my office picks up steam in its regulatory efforts, we will engage in practices such as statements of grace or regulatory comfort for those who engage in our Pink Sandbox or seek advice. We will create or identify bespoke guidance on how to implement practices under the Personal Information Protection Act, as well as persuasive guidance that may be found in other jurisdictions. We will explore ideas seen in other places, such as trust marks, seals, awards, and other recognition. Oversight should not be solely about punishment of the negative, but spotlighting the positive.

As we know in the privacy world, philosophers and psychologists have long argued that the act of being observed changes behaviour. For those organisations with responsibilities to the community, oversight of their behaviour is a necessary counterpart of that responsibility. The work of oversight is to ensure that organisations meet their responsibilities - but also are credited for their hard work.

Our Community Needs a Data Protection Social Contract

Organisations should be driven by a sense of Community. Collectively, we may achieve more than is possible on our own, and that includes successfully protecting rights. We must seek to share our knowledge and experience so that the community can benefit from the sum total of it all.

Our current incentives often reward hiding mistakes or misfortunes from the community, for fear of inviting regulatory actions or public criticism. Mistakes are the best teacher, especially when we can learn from others. We must encourage and incentivise the sharing of lessons learned and hard-won knowledge about cybersecurity and data usage.

We too often try to isolate or compartmentalize responsibility and blame. Many of the mechanisms to do so derive from long legal or business tradition, or even philosophies of individual responsibility. Lawsuits or regulatory punishments may seek to assign fault on one side or the other.

But data protection blends the categories and contributions. When data is misappropriated or misused, the organisation may be a victim alongside the individual, albeit with a different spectrum of harms. Mistakes may have occurred or harms accrued despite their due diligence, and rushing to point fingers will do nothing but obscure the true lessons to be learned.

Protection of a community's data can only succeed collaboratively, with society investing in the necessary security infrastructure, with organisations accepting responsibility for the data they collect, with each individual taking steps to protect their own data, and with oversight bodies working to provide expertise on best practices.

The need for all these different groups to work together implies the need for a new guiding philosophy, a Data Protection Social Contract. I don't mean this term in the sense that we should identify who has the "divine right" to use personal data. Rather, it is to redress the fact that with all of us operating separately, with organisations amassing data for their own interests and individuals largely unable to monitor or control what happens, we find ourselves in a state of anarchy.

Instead of allowing rules or norms to develop ad hoc, we should make conscious decisions about what community we want to build, what responsibilities should fall on each of the various stakeholders, and how they should interact and collaborate to meet their obligations.

In addition to learning from others' lessons, organisations should keep front of mind their sense of community when making decisions about how we choose to operate, asking how data or experience can be used for the public good. The decisions we make should focus on creating a better village, both global and local, for us all.

Individuals and Trust at the Forefront

Use of personal information should keep the individual at its heart, and the organisation's relationship to the individual should guide its decision-making.

Respecting the rights and preferences of the individual builds trust and deepens the relationship. Tandem individual and corporate actions are needed to protect privacy, not an adversarial, oppositional approach.

Much ink and many photons have been spilled extolling the need to keep individuals at the forefront of privacy activities, so while I am more brief here, know that it is not for lack of importance.

If an organisation were to keep the individual front of mind, they could likely intuit their way to a successful privacy program. What does this individual expect of me? How am I keeping the promises I make to them? What could happen to them if the data is misused? Communications, like privacy notices, should be written to individuals, not to judges or the Internet. Privacy breaches harm a specific person, and it is for *that person's* sake that we work to prevent them.

The relationship between an organisation and individual is often considered in the context of receiving the person's consent to process their personal data - and unfortunately, for many organisations that is the sole focus of the relationship. This leads them to communicate details and receive consent, not in the best way for the individual to understand, but in the simplest way to get the signature. Bewildering legalese and long terms of service discourage individuals until they give up and check the box marked "I Consent".

Organisations should think of their relationship to the individual in terms of trust. An individual must trust a business to purchase something online, or they won't risk sharing their financial data or address. Customers reward such efforts to build trust with their loyalty, so it is in organisations' interest to ensure that individuals understand their practices, accept them, and are satisfied with the access, correction, or deletion services that are provided.

Organisations should be encouraged to, and rewarded for, working with individuals to help them understand what is happening with their data. We can only unlock data's potential, while respecting rights, through communal action. We must ensure that all stakeholders play their part in data protection, and individuals are key stakeholders.

Stewardship in All Things

As we travel on our various journeys - through time, space, or life itself - we are transitory. In business or otherwise, we have the opportunity to make use of the resources in front of us, but must always act responsibly, conserving common goods for the benefit of the community now and in the future.

These sorts of arguments are often used for natural resources: in various philosophies, and even Biblically, humans are considered to be the caretakers of the world, not necessarily its owners. This form of thinking shifts the balance away from a sense of entitlement. We should be stewards in all things.

As with other resources, framing the discussion around personal data as one of stewardship, as opposed to ownership, changes the way we intuitively understand its exploitation or protection. An owner is free to sell or consume a resource, but a steward has a duty of care to preserve it. A steward acts on behalf of the individual, in their best interest, ensuring that the data retains its value while also bringing a benefit to the data subject.

An organisation that uses personal data must take the mind-set that the data is not theirs, but only temporarily in their care. Ideas around agency can be very useful in this regard: the organisation should not consider themselves an outside third-party who has triumphed in a negotiation to win data rights - this mind-set is oppositional, winner-take-all. When using personal data, in fact they are carrying out the instructions of the data subject, and should consider the duties of care and otherwise that such a role implies.

Individuals provide data to organisations so that it may be used in ways they prefer, for a benefit they decide is worthwhile. The organisation must consider themselves a steward - or even an agent - of the individual, acting on their behalf and seeking to preserve the resource.

It is common in business parlance to use the word "owner" as the ultimate expression of responsibility, implying that people will surely treat their own property with the highest care and reasonableness. I would argue that is not the case: I am free to use my own property frivolously if I want, if I deem the goal worthwhile.

On the contrary, the highest duty of care arises when one is a steward, charged with protecting property on behalf of someone who has placed a great deal of trust in them. There is a certain amount of humility to this mind-set, but humility is needed from organisations charged with protecting individuals' rights - in other words, any organisation using personal data.

Nota bene: If you'll indulge me, a few additional thoughts for clarity:
When speaking about data and ownership, discussions can go down many, complex roads. If an individual is an owner, does that mean they can sell or lease their data, even for a poor deal? Should we evaluate these agreements for unconscionability? What would be the fair compensation for a perpetual license to process data to make judgments about an individual's preferences for targeted advertising? How could the many, online, micro-transactions possibly equate to matters of rights and principles?

For such reasons I am not yet convinced by arguments regarding data-as-personal-property. Yet, as we have been told so many times in recent news, data has a value and can be exploited. In many ways it is analogous to common areas or natural resources, matters that could profit those who would exploit them, with consequences to be borne by the community. The unfortunate result of this type of structure is the tragedy of the commons, with our privacy the spoilt resource.

On the contrary, I would argue that the inherent harms to rights and freedoms that may come from unchecked data use place an extra responsibility on those who would collect it to act in the best interests of the subject.

Certainly, the organisation may still create something of value for themselves as part of the process of providing a service to the individual, but by shifting the mind-set to the context of stewardship, their duties to the individual become more clear.

They are not to exploit the resource, but to engage in careful management of it for the benefit of the individual. Their duty is not solely to make a profit, but must be balanced against the duties of care or otherwise that they would owe as an agent or caretaker. This shift in perspective provides an important focus, orienting the organisation towards the individual and counterbalancing other incentives. It would be anathema for a steward to exploit data to the point that it harms their charge. It would be violating their duties.

Incentives that Operationalise our Ethics

One of the failings of our modern society is that we have incentivised behaviours that are antisocial. Aside from debating morality, it is a simple fact that people will often gain a material advantage from acting in a way that may be detrimental to others or society as a whole. To use the economic parlance, they are only being "rational" in this course of action, acting according to a logic.

We often see this in personal data-heavy companies, who utilise surveillance capitalism techniques to harvest data from individuals or build profiles for sales and marketing. Online platforms and other businesses have a lot to gain from acting in this way.

However, incentives can be changed, and such changes in environment result in behavioural changes by individual or organisational actors. All social stakeholders should examine the incentives in place and the behaviours that they encourage to ensure they meet the collective goals of valuing data protection and the right to privacy.

At an organisational level, entities should examine how their policies and procedures encourage employees to act. They should ask how their very business goals influence behaviour. For example, if an employee is rewarded with a bonus for sales volume, they will prioritise sales and may choose to improperly utilise personal information to make a sale - even if corporate policies state how much the organisation values privacy. Organisations should find ways to achieve and reward goals related to ethical behaviour or building individual trust.

Similarly, stakeholders should re-evaluate the mechanisms involved in the collection of personal information, particularly gathering of individuals' consent. Utilising a consent-based model will create incentives for the organisations and individuals. Namely, when consent is the key to unlocking the business relationship, then the true goal and incentive is merely to complete the agreement. Or, tick the box. Or - worse still - not *un*tick the box.

We must work to incentivise organisations to give a full disclosure of their practices, in a way individuals can truly understand, in order to receive the data subject's buy-in. This can be hard, much harder than to have a one-off legalese form that whithers and wherefores its way to the length of *Hamlet*, and lulls the reader into consenting merely to move on. We need to develop different kinds of relationships than legalistic or oppositional.

Oversight bodies should examine the environment that we are creating as well. If we choose to focus punishment on technicalities of noncompliance, we create an environment that could miss the true focus of preventing harm to individuals. Organisations would become incentivised to create the long, legalistic statements I just described, instead of engaging in a dialogue with data subjects. We should incentivise the spirit of our goals as much as technical compliance.

A focus on noncompliance may also have the perverse effect of rewarding the unscrupulous - if an organisation will be punished, and potentially heavily punished, for technical noncompliance, even despite best efforts, that entity will be in a worse position than those who did not make the attempt. The latter will have saved time, money, and effort by not even trying to comply, hoping to dodge detection.

The same can be true of the nature of the penalties that are distributed. Merely financial penalties make matters of privacy rights and abuses into an equation, a cost of doing business. Instead of focusing on the financial, my office will develop orders and other remedies to reach the heart of protecting individual rights.

Lastly, we must ensure that all parties are incentivised to participate in protecting rights. Small enterprises may feel that they cannot possibly comply. These entities should not be punished solely for lack of resources to implement complex compliance programs. A failure of incentives in this regard runs the risk of creating data monopolies, where only large, established organisations can comply and new entrants are doomed. We must take a multi-stakeholder approach to ensure that appropriate tools and resources are available to help the entire community, for the sake of a level playing field and to encourage a healthy market.

On our Privacy Compass, the Compass Point of Incentives is found between Ethics and Individuals, because incentives are the way we operationalise our ethics, the way we ensure we keep the best interest of the individuals at heart. Only by creating appropriate incentives can we ensure that our markets, and our society, functions in a healthy, beneficial way.

Interoperability, or Why Bermuda is Not an Island

"No man is an island." John Donne wrote these words in 1624, only fifteen years after the *Sea Venture* encountered Bermuda. It's often said that Bermuda's founding shipwreck inspired William Shakespeare's *The Tempest*, and I like to think that Bermuda also inspired Donne. In my short time in Bermuda these past months, I've taken to adapting the phrase with an ironic bent to say that, paradoxically, "Bermuda is not an island."

As true as this philosophy was at the birth of the modern world, thanks to our technological advances the idea has never been more relevant. We are all interconnected. That's how each of us, even those who live on geographical islands, need to think of the world. Everyone is now our neighbour - capable of sending us a message, logging into our system, or observing our behaviour. No one can rely on obscurity as a protection the way they might have before, which can be a jarring notion.

The internet particularly is a global platform, despite recent trends to wall off portions, and its insertion into all aspects of our lives has enabled global uses of data. Over past decades, privacy laws have emerged organically from trade or governmental discussions to develop national and international standards behind what responsibilities any organisation that uses data may have. Hearteningly, there has been a remarkable consensus around the world to the structure of ideas like Privacy Principles.

Most privacy laws are based on these principles, suggesting the conceptual guidelines that an organisation must follow. To understand how these principles apply, each entity must conduct a bespoke analysis of its actions and their context. Since organisations must comply worldwide with laws based largely on the same principles, in many cases the analysis leads to consensus best practices across multiple jurisdictions. This is why, whether formally or otherwise, the regulations and guidance in foreign jurisdictions tend to have a persuasive effect.

A similar pattern emerges when laws, and organisations, focus on risk. As entities work to effectively mitigate risks specific to their organisation, the vast majority of those risks and actions are consistent regardless of their exact location or jurisdiction. They may face different regulatory compliance floors, but a focus on risk results in an inherently neutral analysis that mitigates the true harms.

Organisations should be encouraged to develop practices that apply regardless of jurisdiction - so long as they support the rights of individuals. This interoperable approach makes business sense, because it allows an organisation operating in multiple jurisdictions to develop a single business program instead of multiple regimes. This approach also supports a high standard of privacy protection for individuals: because organisations must still meet varied privacy regulatory requirements, the net result is a rising tide that lifts privacy rights.

As a regulator, my office will support this practice by identifying and endorsing guidance and best practices that allow organisations to meet these goals, and approaching regulatory action with understanding - if due diligence and a spirit of good intentions are present.

Organisations should also be encouraged to develop practices that apply interoperably to varied technologies. Often, businesses attempt to lock customers in to their ecosystem in an attempt to corner the market for their attention. In the long run, this approach will only benefit a business that achieves monopolistic proportions - which itself runs afoul of other public policy goals.

Instead, by incentivising organisations to make their products technologically interoperable, we encourage a healthy marketplace and competitive space, where individuals are in the best position to choose the products that meet their needs and to make informed choices about sharing, retrieving, and moving their data.

Organisations should make their practices interoperable in one other way: with the future. By preparing in advance for technological developments, regulatory trends, and the protection of individual rights, these entities can engage in future-proofing that allows them to remain in a position to succeed even as the global environment changes.

If we only focus on one jurisdiction or one technology, one right or one emerging issue, then we merely create a single patch of fabric. Instead, we need to focus on the entire sail. Weaving universal, interoperable business practices will allow us to better catch the wind and move ever forward. We can progress with a single, intact sheet or with a patchwork - if, like our approach, it is seamless.