Creating a climate for change: the privacy conundrum

By Annelies Moens CMgr FIML and Chris O'Connor

We recently read an illuminating article by Jeff Kluger, editor at large for *Time*. At its core, it asserts that from a behavioural standpoint, we humans are going to find it very difficult to take action on climate change – until it's too late. As he put it, "when it comes to the loss of the entire planet, well, we ought to take action. And yet we don't; we never do."

Why the widespread inaction?

Kluger rationalises that climate change falls into an 'ignore-the-problem' box as it doesn't fulfil the criteria we need to be motivated to act. The same can be seen in how privacy issues are often treated – organisations are sometimes good at predicting future outcomes and identifying risk but fail to understand the relative potential of the risk and ultimately, do nothing about it.

When it comes to taking steps to manage fundamental human and economic rights, such as privacy, many organisations fail to appreciate its significance. Privacy is a building block that leads to the protection of other rights taken for granted in many parts of the world such as autonomy and freedom of expression (no chilling effect). The protection of people's privacy is fundamental to democracy. Yet it is easily whittled away to the point that individuals no longer have control over their own personal information.

The common folly

The over-collection and misuse of personal information, as well as the ubiquitous number of data breaches, bear a heavy cost on society and business. Think of Facebook's market capitalisation that dropped US$119 billion after announcing that growth had slowed since the Cambridge Analytica scandal. Equifax and Target's well-publicised data breaches cost the companies approximately US$300 million each, not including all the indirect costs such as customer churn, loss of trust, identity theft and the illegal sale of personal information.

Despite this, many organisations fail to adopt basic precautions, such as two-factor authentication or minimising collection of unnecessary data points, such as date of birth or deleting data they no longer need for their organisation's purposes.

Each quarter, the Office of the Australian Information Commissioner (OAIC) reports on the causes of data breaches by regulated entities. The majority of data breaches are due to human

factors such as falling for phishing attacks, which can be thwarted if secure forms of two-factor or multi-factor authentication are in place. Indeed, half of cyber incidents as the OAIC reported in its most recent quarterly reports were due to phishing attacks.

Despite climate change, data and cyber issues being in the top five likely to occur risks, privacy, like climate change, can be seen as a far-off issue, one that takes a back seat to more immediate and pressing issues. This is a mistake.

To motivate action our knowledge and beliefs must align

What do privacy and climate change lack in fulfilling the required criteria to motivate people to act? Here are some reasons:

1. **They lack the "me" component.** As David Ropeik, an international consultant on risk perception and communication, said in the *Time* article, "Nobody wakes up in the morning and looks at the long-term climate forecast. They ask what the weather is today, where I live, and how it's going to affect me."In terms of privacy, the lacklustre response of senior leaders and directors to privacy issues show the failure of leaders to put themselves into the shoes of their customers. They prioritise shareholder primacy and profits over customer privacy (consider Facebook's response to the privacy scandals) or give primacy to politics (consider the privacy problems surrounding the rollout of the e-health record in Australia).

   It is growing increasingly clear that customer and community values need to be accounted for. It's not good enough to focus solely on maximising shareholder value, if long-term sustainability is a goal for shareholders (see "Innovate before it's too late" by Mariana Mazzucato in *Company Director* pp.12-13, Dec 2018/Jan 2019).

2. **The consequences seem far in the future, so we discount the risk.** Paul Slovic (University of Oregon psychologist and the President of Decision Research) said in the *Time* article, "When it comes to acting on problems, the lure of our current comforts and conveniences will often cause us to act contrary to our values." When it comes to valuing privacy, numerous studies show that whilst people highly value their privacy, they often don't take steps to trade it off for other considerations such as convenience. This is known as the Privacy Paradox.
3. **It can be hard to envisage how climate change or a breach of privacy will affect us – personally.** What will our lives be like if there are two or three degrees of warming or if our identity is stolen? Ropeik says "if you ask even the most devout climate change believers how they think it's going to affect them, they often can't quite describe it". If you can't put yourself in the picture, it'll be easy to ignore.

   Similarly, the nexus between a privacy breach, such as a misuse of your identity and the harm could be years apart. For example, you may only realise the impact of the misuse of your personal information when you can't get a loan for the house you want to buy. At some point in the past, someone has misused your identity and has defaulted on a loan in your name, often seen in privacy complaints to the OAIC. The damage, in contrast to a plane falling out of the sky, is not instantaneous. Sometimes, we can't even connect the misuse with the harm that happens down the track.

4. **There is a sense of futility or hopelessness.** The inefficacy factor, whereby people think that individual action has no impact particularly on large problems. Slovic says that "we reason that we can curtail things we want to do – like driving or flying, but if other people aren't going to do it, it's not going to make any difference."

   Consider all the information about us held by third parties or in the public domain or what our friends post about us on social media platforms over which we have no control. So, what does it matter if we hand out our personal information again? For example, what does it matter if I keep on handing over my personal data in insecure environments (such as HTTP rather than HTTPS on websites); or when the data is actually not required by the requestor (like a vendor asking for a date of birth when you are purchasing wine online, when all the vendor really needs to know is that you are over 18). In the latter situation, many customers would simply provide a fake date of birth to complete the transaction anyway.

So, what needs to happen to effect change in such scenarios? Let's restate the conundrum outlined above in the positive:

Seven knowledge and belief statements that must align to get people moving to make changes

1. I **know** this will affect me
2. I can clearly **envisage how** it will affect me
3. I am clear about the **future consequences** of doing nothing
4. I am willing to make the effort today to **make tomorrow better**
5. I feel **confident** that our actions today will achieve the desired outcomes
6. I have the **support, knowledge and tools** to act

The last and most important factor that the *Time* article does not address is:

7. **Leaders must not just say** they are all behind the initiative, **they must reflect** that commitment **in their actions – every day.**

Many people are very good at spotting inauthenticity and if they don't believe their leaders are committed, they won't be either. Accountability for privacy needs to be at senior leadership levels, with an ability to influence culture and practices organisation-wide.

We are entering an era of social climate change when it comes to privacy, as more and more people are becoming aware of the value of their data and what the impacts are of not managing privacy well. We still, however, have a long way to go to building in privacy by design into organisational processes and systems and making privacy core business.

In terms of climate change, the lack of leadership in some countries is concerning. The stakes are high and in today's global political (rather than scientific) climate, we're not even close to getting on the right track to managing our natural resources sustainably.

Is your organisation displaying symptoms of this collective inertia?

The lessons we're learning on a macro scale about motivation, commitment and action are equally applicable within government, business or not-for-profit. You may recognise the

behaviour described above when you consider the last failed initiative within your own organisation. It may have been that people just couldn't or wouldn't support it. That there wasn't the "corporate will" as some call it, to make it happen.

So, for leaders that are starting to realise the significance of making privacy core business and developing privacy management frameworks, we would encourage you to consider the following questions to start assessing your level of privacy maturity:

- Do we have a clear understanding of the data needed as opposed to the data we would like from our customers and prospects? Can we clearly describe how that will benefit both the organisation and individuals for whom we are their data custodians?
- Do we know what the result of doing nothing is? Can we quantify the risks of a privacy breach? Can we clearly articulate this? What would be the risks or impacts for the individual and other stakeholders? How would we respond?
- Is our plan of action credible and can we show that our leadership is united and willing to do the hard yards and realise that data is an asset or a liability depending on how well it is governed or managed?
- Do we have a clear understanding of what resources staff will need to make change happen? Will they know what to do and how to do it? Can they measure success?

If you can say YES to each of these questions, you're off to a good start. But it's not a silver bullet – there are numerous practical issues that will stand in the way (a discussion for another time), however, without commitment and collective action, you have no chance to overcome the inertia.

For more information on introducing privacy management frameworks and privacy maturity models into your organisation, contact Annelies Moens at operations@privcore.com and Chris O'Connor at chris@ock.com.au

---

Annelies Moens is the managing director of Privcore and Chris O'Connor is the director, practice lead innovation & agility at O'Connor Kingsford.

Posted on 11 April 2019