IIC Webinar

Privacy and pandemic: Data protection considerations for the telecoms, media and technology sector

Wednesday 29 July 2020

Panel:

Paul Canessa, CEO, Gibraltar Regulatory Authority (Moderator)

Simon McDougall, Executive Director, Information Commissioner's Office, UK

Gregory Smolynec, Deputy Commissioner, Office of the Privacy Commissioner of Canada

Richard Benjamins, Chief AI and Data Strategist, Telefonica SA

Bojana Bellamy, President, Centre for Information Policy and Leadership

Introduction

Technology has played a key role in the global effort to combat Covid-19. This role has depended heavily on data – its use, storage and transmission. It poses new questions in a long-standing debate: what is the balance of interests between the right of the state to use data for the common good, and the individual right to privacy? How should this be decided, applied and regulated, and what can we learn from the experience of dealing with these issues since Covid-19 struck? The webinar was the second of two debates designed to reflect on issues of privacy in the time of pandemic. You can view details here on the first debate, IIC Thailand Chapter Webinar: Data Privacy in the Time of COVID-19 held on 22 July 2020.

Simon McDougall

Simon McDougall began by explaining that, from an ICO perspective, operational performance had been good. A new office structure had been adopted rapidly. Non-Covid activities, such as adtech, were de-prioritised and the challenges over use of data were identified. This presented in a variety of different scenarios. Over 500 individual cases of Covid-19 and data protection were encountered, including innovations in the use of technology, tracing apps and temperature testing. There were also issues over the sharing of health data between government authorities about, for example, vulnerable people.

Approaches to data use and privacy

The organisation had created two specialist teams. The first dealt with case management, while a second looked several months ahead to envisage the 'new normal'. A two stage approach was

adopted. The first was legalistic: was there a lawful basis? In this respect GDPR had – surprisingly – stood up well, and ways had been found to continue the fight against Covid-19 while remaining GDPR compliant. The second approach involved issues of necessity and proportionality. This was more nuanced and recognised that some uses were needed temporarily, but would not necessarily be acceptable permanently.

Creative necessity

A positive outcome from the pandemic is the way in which barriers to data-sharing have been broken down. The sense of urgency has enabled issues that have been problematic for a long time to be solved through creativity and innovation. This is the first crisis in which apps have been able to provide significant help and support. Contact tracing apps have worked in concert with manual tracing, and the decentralised approach has much to commend it. There have been many benefits from the involvement of the private sector, and huge advantages in being able to use a company like Amazon. However governments need to be wary of their reliance on a small number of very large tech companies that could already be 'too big to fail'. Corporate Social Responsibility issues have become an important part of the response, with companies and employees keen to be seen to make the right contribution in a time of crisis.

Now the initial crisis has been dealt with, the dynamics of the second wave have to be contemplated. The key is public trust, and the continued building towards good practice. One effect of the pandemic is that data protection impact assessments (DPIAs), once a marginal part of the digital infrastructure, have become central, and the public have begun to engage with the data protection issue.

Public trust

The issue for the future is how to get back to proportionate responses. There is a risk that behaviours that were voluntary become mandatory. Privacy is not an absolute right and the challenge is to get back to normal life in a way that maintains trust.

A feature of the 'new world' is that we can look around the world, to learn from and work with other Data Protection Authorities. This work is challenging but rewarding. It's critical to establish good governance and communicate openly to the public. Without trust in institutions and technology the fight against Covid will be unsuccessful.

Bojana Bellamy

Bojana Bellamy described how Covid has brought home the need for an acceleration of the digital transition. There is no going back from this – every company is a data company. The initial need was for business continuity, but new processes and approaches have raised other implications, particularly for security. The pandemic has resulted in some new businesses emerging, for example start-ups in immunity passports, but also in a massive need of 'data for social good' supported by company management and leadership as well as employees. Uber has been transporting medicines and offering free rides to health staff, and Amazon is now essential infrastructure. This appetite for data sharing and data frameworks will remain, and need to be managed, especially in light of the new cyber risks. Governments are the spenders, not the solution providers, and need to appropriately regulate the public/private partnerships. The way in which existing companies have new business lines in health and data complicates the procurement task of governments.

Positive responses of regulators

Regulators have also changed and the ICO has set a good example in pausing non-urgent work to focus on data use, not just in terms of compliance, but in enabling sharing in accordance with the law.

There have been visible shifts in strategic plans. Regulators have anticipated changes, recognising that people are prepared to give away some of their privacy rights. There has been useful guidance in interpreting GDPR. Amid extensive reticence risk and fear of 'doing wrong', regulators must continue to be bold to ensure the proper interpretation of GDPR. . Although the initial response was a national one, the creation of the Global Privacy Assembly[1], and the Covid task force, was acknowledgement that regulators need to work together in areas such as accountability, innovation, public/private sector data sharing and the role of data review boards.

Data sharing and privacy must both be achieved – one cannot be at the price of the other. CIPL has produced advice on the lifecycle of data use, involving 'twelve accountability steps'. [2]

Limitations on data

Although it is important to enable data usage, the benefits must be clearly justified. Is personal data needed, or can the ends be achieved with anonymised and aggregated data? There is a challenge to ensure transparency, but there need not be limits to the use of data, especially the additional uses of data, provided risks are managed and it is used responsibly. Agreements may exist on paper, but there has to be audit and assessment in the process, possibly including external validation as well as internal oversight. They must recognise the benefits of what is being designed, balanced against the privacy issues.

Problems of compliance

Many compliance issues emerged as a result of the additional use of employee data. Some regulators were slow to acknowledge the extent to which companies needed to monitor employees, both for security and data protection when remote working, but also the expanding concerns of well-being and health. It is not helpful to prevent processing of employee data, such as temperature checks, when employees themselves want to go back to work.

In addition, data processing may not just be an issue of consent, but one of vital public interest. A bolder interpretation is needed, balanced by accountability and transparency from companies. Anonymised data is outside data protection law. When the Dutch regulator said that there's 'no such thing' as anonymous data, it makes the sharing of aggregate data impossible. The current GDPR exemption in health data, needs to be expanded to bring in broader applications such as AI.

Richard Benjamins, Telefonica SA

Richard Benjamins began by outlining the way in which 'Big Data' can provide a proxy for human activity. The activity of networks are very important proxy for how people are behaving during the pandemic. European Telecoms companies were asked by the European Commission in March to share data to understand the propagation of the virus, observe the effect of movement restrictions

[1] https://globalprivacyassembly.org/
[2] https://www.informationpolicycentre.com/cipl-blog/covid-19-meets-privacy-a-case-study-for-accountability

and how confinement measures were working. The value of this anonymised and aggregated data was internationally recognised, and the approach was used by many countries across the world.

Examples of the practical use of aggregated data

Telefonica was involved in several cases where the approach proved useful, including:

- Monitoring the reduction in mobility in Spain after lockdown measures were introduced, broken down by province. The data was also able to use 'mobility functional areas' to provide insights into where lifting restrictions would be more likely to enable economic recovery based on mobility flows rather than administrative boundaries.
- Showing that the health systems of Spanish Provinces near the coast were not at risk from large scale movements to second homes
- In France the company was able to map movement against excess deaths with a 90 per cent spatial correlation. It also demonstrated that, where social distancing was put in place, the impact of mobility was reduced.

Preparation and response

Governments acted once the pandemic took hold. None were properly prepared in advance, except China and South Korea. This is partly explained by the difference in privacy regulation in those countries, both of whom have extensive access to data, including personal data, not available to other countries. Most countries, even the EU, acted one month too late, by which time the virus had already propagated widely and drastic measures were required.

There is an important but poorly understood distinction to be made between personal data, used for contact tracing, and anonymised and aggregated data. This came to prominence when, for example, the European Commission made clear that GDPR was flexible in allowing the data anonymization, access and retention in the fight against Covid, while the Dutch DPA claimed that GDPR prevented the sharing of customer data. In some cases, political parties have proposed boycotts of mobility data studies as a result of confusing the two types of data.

Ten privacy Lessons from Covid-19

- *Combat privacy confusion with education of media and politicians (and regulators)*
- *Regulators need to provide guidance on enablement, not just compliance*
- *It's about public good, not just consent. Privacy is not an absolute right*
- *More work is needed to communicate transparency and benefit*
- *It isn't ethical to fail to use data that can solve problems*
- *Short term measures mustn't automatically become permanent*
- *A financially sustainable model is required - governments need to invest and not expect companies to be philanthropic*
- *Data problems should not define all public policy problems*
- *Post-Covid analysis needs to be critical and organisations need to avoid the temptation to 'look good'*
- *Laws should be technology-neutral and principles-based in order to remain relevant*

Gregory Smolynec

Gregory Smolynec described how the pandemic has accelerated the already rapid changes in data environment that have been evolving for some time. It underlines risks to the human right of privacy, as well as the risks to other rights and freedoms for which privacy is necessary.

The pandemic has resulted in the use of personal data in the fight against the virus, and the Office of the Privacy Commissioner (OPC) has employed a philosophy of flexibility and contextuality. Privacy guidance was quickly developed to help the government in implementing new initiatives and applications.

The broad effects of the pandemic will be long-lasting, especially in the acceleration of digitisation. This is an unfolding history in which digital communications technology is central to social change and the place of the individual in society.

The challenge is to understand these changes and articulate them in sufficient detail as part of a broader picture. Marshall McLuhan described the gravitational effect of technology on cognition, and social organisation. Digital technologies, such as smartphones and apps, are detectably affecting the behaviour of individuals as well as social structures and institutions. One impact is the 'de-centering' of government as a source of public health advice. In privacy, people have a right to meaningful consent, free of coercion. The problem is that the recourse to technological fixes, while not inherently bad, can complicate how individuals exercise their rights. It can magnify problems such as security risks, or exclude vulnerable populations. The current context highlights four data protection challenges:

- The enormous pressure on unprepared governments to mount a response to the pandemic resulted, literally, in the downloading a of a core healthcare function to individuals' phones
- Processing is invisible, and poorly understood, as is the solution
- Data-driven public health programmes may flounder in the face of the underlying specifications, APIs and coding being incomprehensible
- Digital solutions may be positive for smartphone users, but what about others?

McLuhan described electronic environments as 'eluding all easy perception'. This may have an effect on the 're-imagined city', where the structures can't be seen. Massive public policy problems may not be adequately addressed by technological solutions. The ends, ways and means need to be in proportion to each other.

Technology can delimit the scope of the problem prematurely. All public policy problems shouldn't be defined by data problems. Issues like effectiveness, accountability, scientific rigour, minimal intrusion, equity and fairness mustn't be overlooked. Technologies can act as accelerants when a society is in crisis, and many democracies were already in crisis when the pandemic struck, with trust depleted.

The current response is highlighting the potential for the public good, as well as effects on individuals and society. To protect the human right of privacy technology needs to be explicable, transparent, effective and distributed. Policy responses need to be fair, reasonable and proportionate. For societies to be free, fair and democratic, privacy is essential.