GPA
Global Privacy Assembly

Digital Citizen and Consumer Working Group

Intersections with Privacy Survey
Summary report

Contents

Introduction

The Digital Citizen and Consumer Working Group (DCCWG) became a permanent working group of the Global Privacy Assembly (GPA) in 2021. The DCCWG's work has focused on considering the intersections of, and promoting regulatory cooperation between, the privacy, consumer protection and competition/anti-trust regulatory spheres. Pursuant to its mandated actions under Pillar #2 of the GPA Strategic Plan 2021-23, the DCCWG has undertaken extensive work to explore the relationships between these regulatory spheres.

As technologies rapidly evolve, the challenges and opportunities in the digital landscape continue to defy traditional regulatory frameworks. In 2022-23, we saw increased data breaches, novel forms of artificial intelligence technologies, along with a variety of enforcement and policy responses to resultant harms. Accordingly, the working group sought to identify areas of emerging regulatory intersection with privacy in the digital society and economy. This work is intended to inform the future direction of the DCCWG and support its goal of promoting regulatory co-operation and collaboration on cross-cutting issues and activities in the regulation of digital platforms.

To do so, the DCCWG surveyed GPA members in 2023 to ascertain their experiences with regulatory intersections and collaboration. The survey posed eight questions which aim to understand which regulatory areas members are currently experiencing, or foresee, intersecting with privacy within their jurisdictions (other than consumer protection and competition/anti-trust). The report seeks to identify members' views on the risks, opportunities and potential impacts that these intersections may have on the digital society and economy, and which areas of emerging intersection are of the greatest potential significance.

This report sets out the finding from that survey, supplemented with additional information from the ongoing work the DCCWG conducts in monitoring and mapping international activities that demonstrate the intersections between regulatory regimes. The intention of this report is to provide a high-level snapshot of the types of regulatory spheres that privacy and other regulators should be aware of and explore further in their own jurisdictions, as they work to develop solutions to complex regulatory challenges in the digital economy.

The five main trends that emerged from the survey are cyber security, online safety, financial services, artificial intelligence and telecommunications. These issue are increasingly of relevance to, and intersect with, privacy regimes of the members that responded. It was evident that authorities wish to see greater collaboration in regulation to combat emerging issues. As the digital economy evolves, joined-up regulatory collaboration on policy initiatives, as well as regulatory action, has clear benefits to both regulators and broader society.

These are of course, not the only regulatory challenges in the digital environment. We anticipate that as jurisdictions grapple with how to regulate other issues, such as disinformation, misinformation and online gambling, we will see these continue to grow in prominence as other areas that intersect with privacy regimes.

We recommend that the DCCWG continues to focus on strengthening capacity of GPA members to identify intersections and develop domestic collaboration strategies and forums. Throughout the 2022-23 year, the group has witnessed an increased interest in other members' experiences, ranging from informal collaboration to more established collaboration initiatives such as the UK's Digital Regulation Cooperation Forum, Australia's Digital Platform Regulators Forum (DP-REG) and Canada's Digital Regulators Forum.

Survey responses

12 GPA members responded to the survey, covering five continents: Africa (8%), Asia (25%), Europe (33%), North America (16%) and South America (16%).

The following GPA members provided responses:

1. Office of the Privacy Commissioner of Canada ("**OPC Canada**")
2. Instituto De Transparencia, Acceso A La Información Pública Y Protección De Datos Personales Del Estado De México Y Municipios ("**INFOEM**")
3. National Privacy Commission (NPC) Philippines ("**Philippines**")
4. Superintendence of Industry and Commerce – Republic of Colombia ("**Colombia**")
5. Gibraltar Regulatory Authority ("**Gibraltar**")
6. Catalan Data Protection Authority ("**Catalonia**")
7. Access to Public Information Agency – Argentina ("**Argentina**")
8. Office of The Privacy Commissioner For Personal Data (PCPD), Hong Kong, China (**"Hong Kong")**
9. Commission Nationale Pour La Protection Des Données (CNPD) – Luxembourg DPA (**"Luxembourg"**)
10. Norwegian Consumer Authority ("**Norway**")
11. Burkina Faso Data Protection Authority ("**Burkina Faso**")
12. Personal Information Protection Commission Japan ("**Japan**")

Key emerging areas of intersection

Respondents were asked for their reflections on what were the key current and emerging areas of intersections with privacy, and their associated risks. The responses provided demonstrated consistent themes from the regulators, including that online safety, cyber security (and national security), financial services, artificial intelligence and telecommunications are increasingly of relevance to, and intersecting with, privacy. Cyber security and online safety were the most frequently mentioned areas of intersection, followed by artificial intelligence, telecommunications and financial regulation.

Online safety

Two thirds of respondents recognised online safety as an emerging intersection. Online safety, in simple terms, refers to the act of staying safe online. It is also known throughout different jurisdictions as internet safety, e-safety or cyber safety. Being safe online means individuals are protected from online harms and risks, such as bullying, image-based abuse and exposure to illegal content such as child sexual abuse material, terrorist messaging or violent images. Ineffective online safety protections may lead to unsafe communications which can affect mental health and wellbeing.[1]

DPAs said that as the collection, processing and disclosure of personal information becomes more ubiquitous, it has become easier for malicious actors to exploit vulnerable populations by disclosing individuals' personal information online. Tensions may arise between privacy and online safety, when considering technologies such as age assurance, end-to-end encrypted services, and the use of biometrics to detect unsafe online content. Respondents also reflected on the growing need for regulators of these regimes to cooperate to address possible regulatory overlaps.

Cyber security

Cyber security and cybercrime are a current significant intersection for 42% of respondents. Increasingly, cyber breaches result in the unauthorised access to, or disclosure of, personal information held by the entity subject to the breach. Enhanced cyber security and more sophisticated measures against cyber threats can positively impact individuals' privacy by reducing the likelihood/risk of data breaches and limiting the level of potential harm. DPAs noted, however, that individuals using cyber security technologies are typically not aware of what they are consenting to which itself contributes to risk. Only one DPA, Norway, noted that their law explicitly mandates collaboration with their domestic cyber security agency.

National security

Recent cyber incidents have demonstrated novel challenges with respect to national security. Four DPAs – Japan, Canada, Luxembourg and Norway – identified national security as an emerging area of intersection with data protection. While not all cyber security breaches will give rise to national security issues, Japan and Luxembourg noted that a lack of cyber security literacy has seen an increase in national security concerns. Where personal information is involved in a cyber security breach this can give rise to national security issues, for example where critical infrastructure or intelligence services are concerned.

[1] UK National Online Safety's definition of online safety. What is Online Safety? | National Online Safety

Financial services

Half of the respondents found that regulation of financial services is a key emerging area of intersection with privacy. For example, frameworks around anti-money laundering, counter-terrorism financing and credit reporting often require the handling of personal information in order to regulate effectively. Additionally, as an increasing array of digital financial services products become available and financial markets become more digitised, the amount of personal information collected and processed by the financial services sector has grown significantly. Respondents raised concerns about the way in which these emerging financial services products may be using personal information. Gibraltar noted that the growth in processing of sensitive financial data carries risks related to profiling and targeted advertising often impacting the most vulnerable groups in society.

Artificial intelligence (AI)

One third of respondents referred to AI as an area of emerging intersection. We use the term 'artificial intelligence' to refer to a cluster of technologies and techniques, which include some forms of automation, machine learning, algorithmic decision making and neural network processing.[2] AI is an area of intersection with privacy because AI models are often trained using personal information, which may or may not be anonymised and/or deidentified, and may in turn be used to further process personal information. The associated privacy risks of AI that DPAs identified are:

1. The origin of training data
2. How data subjects could have consented to their information use and potential storage
3. Challenges with transparency and notification to individuals about the way that their data will be used, and corresponding challenges in seeking explanations and review when decisions have been made about individuals
4. Data may not be effectively anonymised and AI, when provided with multiple data sets, may be able to re-identify individuals
5. AI is trained on anonymised personal information which can, even if anonymised, entrench and exacerbate existing biases and inequalities, such as discriminatory perspectives or limit a segment of the population's access to goods, services and/or opportunities.

AI is a key emerging technology, traversing many regulatory frameworks, with new privacy implications arising as the technology continues to develop. Accordingly, regulatory collaboration on AI would require cooperation by multiple actors across diverse frameworks.

Telecommunications

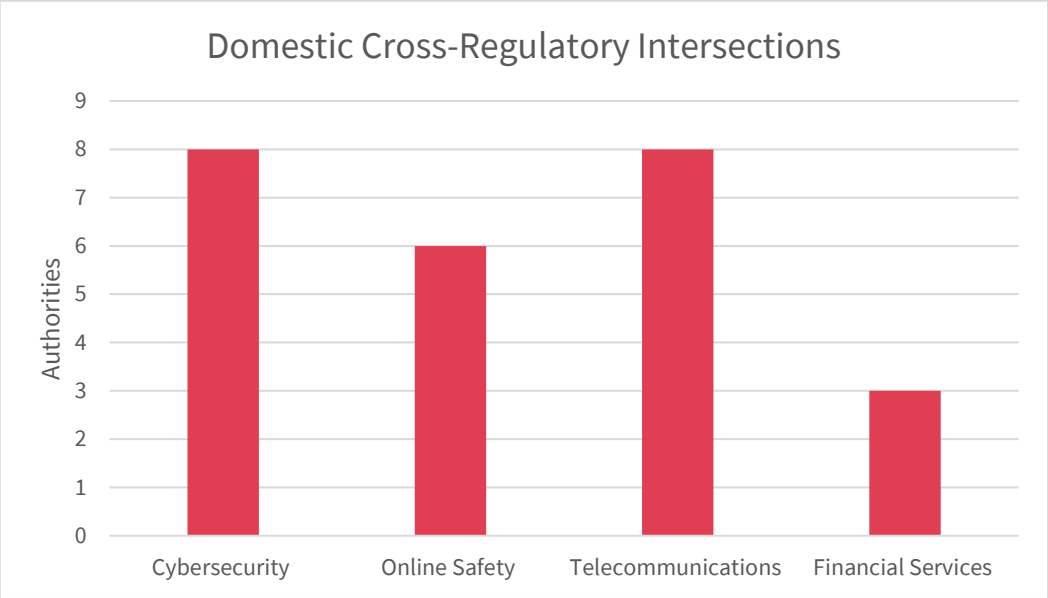
Telecommunications was also raised as a primary emerging issue for a third of respondents. The prominent risk is that telecommunications companies hold granular data on nearly every aspect of an individual's online (and at times offline) activity and risks related to surveillance of individuals and security of personal information arise.

[2] AHRC Human Rights and Technology Final Report 2021.

There is a growing trend among DPAs which sees them entering onto agreements which enable them to cooperate with telecommunications regulators in relation to personal information handling practices.

Recent domestic cross-regulatory intersections

Survey respondents were also asked to identify examples of regulatory issues which have fallen within both their own jurisdiction and that of another domestic regulator. The table below sets out the primary cross-regulatory intersections that respondents identified as necessitating a collaborative approach to address, and the number of authorities that identified each area of intersection.



Cyber security – Two thirds of respondents cited that cyber security and online safety were major regulatory issues that show a need for cross-jurisdictional cooperation.

Online safety – Half of the respondents noted instances that related to online safety which spans children's online safety, cyberbullying and cybercrime.

Telecommunications – Two thirds of respondents recognised telecommunications as a cross-jurisdictional issue which may extend to the placement of cookies and the confidentiality of communications.

Financial services – One quarter of respondents said that financial services are a cross-jurisdictional issue for them, including gambling, money laundering, financial markets, credit reporting and anti-corruption.

Domestic non-privacy responsibilities

Respondents were also asked to comment on any potential or recent legislative proposals which would modify their privacy authority's mandate, and whether their current mandate extends to areas of law beyond privacy.

Two thirds of the respondents have recently seen public announcements about changes that would affect the responsibilities of their authority in an area of law or on a regulatory issue other than privacy. For example, DPAs in Catalonia, Luxembourg and Norway noted a change to the responsibilities of their authority in an area of law or regulatory issue other

than privacy as a result of European law reform (including the Digital Markets Act, the Digital Services Act, the Artificial Intelligence Act and the Data Governance Act).

One quarter of respondents noted that they will likely experience new responsibilities regarding telecommunications due to recent legislation or mandate changes. For example, proposed amendments supported by the Canadian DPA would allow that DPA to collaborate with both the domestic telecommunications and competition regulators to investigate inquiries or formal complaints. The Canadian DPA has also proposed that its ability to cooperate with domestic regulators be extended to other regulatory spheres.

Additionally, one third of DPAs noted that their mandates extend to regulatory issues beyond privacy. For example, legislation has come into effect in Hong Kong that extends the DPA's regulatory mandate and empowers its Privacy Commissioner to carry out criminal investigations and institute prosecutions for doxxing and related offences. This includes collaboration with law enforcement. In Hong Kong, criminal doxxing refers to the disclosure of personal data without the data subject's consent, with an intent to cause specified harm (for instance, harassment, bodily harm, psychological harm, etc), or being reckless as to whether any specified harm would be caused, to the data subject or their family members. It covers disclosure on the internet, social media and other open platforms.

Collaboration

Respondents were also asked about their experiences in collaborating with other regulators, including whether there are any requirements to consult or whether they regularly engage with other agencies or regulators.

Only 8% of respondents have specific legislation that requires them to consult or collaborate with another domestic agency or authority in relation to a particular area of intersection. Further, only 17% of respondents have laws that require other domestic agencies/ authorities or regulators to consult or collaborate with the DPAs.

Japan reported that national administrative bodies in areas of healthcare, finance and telecommunications are required to consult the DPA to develop joint guidelines. In particular, legislative provisions in Japan require a number of domestic authorities to consult with the DPA in relation to the collection and inspection of anonymised medical data. Similarly, Canada's anti-spam legislation requires its competition authority, telecommunications authority and the DPA to consult with one another "to the extent that they consider appropriate to ensure effective regulation".

However, 75% of respondents cited that they *do* regularly engage with another domestic agency/authority/regulator with regulatory responsibility for something other than privacy. This collaboration is informal and not mandated by legislation. For example, the Gibraltar DPA has in recent years increased its collaboration with the Financial Services Commission and Financial Intelligence Unit, putting in place Memorandums of Understanding to facilitate cooperation to address risks in the intersection of financial services and privacy. The Norwegian DPA regularly engages with the national telecommunications authority on the issues of cookies, public warnings and confidentiality of communications, as well as with its financial supervisory authority in relation to financial markets, anti-money laundering and anti-corruption.

Of the DPAs that regularly engage with other domestic authorities on an informal basis, 42% engage with law enforcement authorities, a third with financial services authorities and a quarter with telecommunications authorities. The Norwegian DPA also engages with its domestic media authority and national security authority on online safety and cyber security

matters, as well as with health authorities on the use of health services processing personal data.

Throughout its engagement with members and monitoring work, the DCCWG has also witnessed an increase in instances of formal domestic collaboration initiatives and growing recognition of the ways in which matters relating to digital platforms cut across regulatory remits. The DCCWG has seen the creation of new models of interagency coordination that move beyond bilateral relationships to bring together a range of agencies with different remits to address cross-cutting issues, three examples of which are set out below.

United Kingdom

In the United Kingdom, the Digital Regulation Cooperation Forum (DRCF) was formed in 2020 and brings together regulators with responsibilities for digital regulation – the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO) and Ofcom. Individually, these regulators are responsible for privacy, competition and consumer protection, telecommunications and financial services. The DRCF was established to support cooperation and coordination between members and enable coherent, informed and responsive regulation of the digital economy.

Australia

In 2022, the Australian Communications and Media Authority (ACMA), the Australian Competition and Consumer Commission (ACCC), the eSafety Commissioner (eSafety) and the Office of the Australian Information Commissioner (OAIC) formed the Digital Platform Regulators Forum (DP-REG). Individually, these regulators have responsibility for communications and media, competition and consumer protection, online safety, and privacy. DP-REG is an initiative of members to share information about, and collaborate on, cross-cutting issues and activities on the regulation of digital platforms.

Canada

In June 2023, Canada announced that the Competition Bureau (Bureau), the Canadian Radio-television and Telecommunications Commission (CRTC) and the Office of the Privacy Commissioner of Canada (OPC) had formed the Canadian Digital Regulators Forum (CDRF). Individually, these regulators have responsibility for competition and consumer protection, telecommunications and privacy. The Forum was created to strengthen information sharing and collaboration between members on matters that relate to digital markets and platforms.

International Network for Digital Regulation Cooperation (INDRC)

In recognition of the value of these domestic digital regulation cooperation forums, in June 2023, the UK DRCF convened an inaugural meeting of the International Network for Digital Regulation Cooperation (INDRC). The objective of this network is to build international relationships with regulators seeking to increase domestic cooperation, foster discussion between regulators on matters across digital regimes and gather insights into effective approaches to regulatory cooperation.

The inaugural meeting was attended by the Australian DP-REG, the UK's DRCF, the Netherlands' Digital Regulation Cooperation Platform (SDT) and the Irish Digital Regulators Group (DRG). A second meeting is intended to take place before the end of 2023.

The DCCWG provides an opportunity to further facilitate connections with this group and socialise insights to GPA members as they continue to explore and expand collaborative efforts in regulating digital platforms.

Conclusion

The findings from this survey provide insights from privacy regulators as to their experiences with emerging areas of intersection with privacy that various jurisdictions are grappling with.

The international privacy landscape is diverse and jurisdictions face distinct challenges. However, it is evident that many DPAs share the same or similar concerns and experiences in relation to cross-regulatory intersections. Our findings indicate that the following areas of intersection are increasingly important for DPAs to consider:

1. Cyber security
2. Online safety
3. Financial services
4. Artificial intelligence
5. Telecommunications

Authorities anticipate that the greatest risk to privacy is the fast-paced development of technology and digitisation of goods and services. This introduces challenges related to user consent, a lack of technical and legal knowledge, and transparency regarding the collection of data. The privacy risks arising from these intersections demonstrate a greater need for domestic and international collaboration.

These findings confirm that the evolving nature of digital environments continues to defy traditional regulatory spheres, highlighting the need for further informal and formal collaboration between regulators. Our findings reflect that such collaboration is necessary to achieving the vision of the GPA and moving towards a higher level of global data protection and privacy in the digital environment. The DCCWG will continue to focus on strengthening capacity of GPA members to identify regulatory spheres intersecting with privacy in their jurisdictions and sensitising the work of the DCCWG to assist members in developing collaboration strategies and forums.

Appendix

Global Privacy Assembly and DCCWG Materials
GPA Strategic Plan 2021-23

Respondents Materials (alphabetically)

Argentina
Law on Audiovisual Communication Services
Law on Information technology and communications
Law on Access to Public Information
Circular Conjunta

OPC Canada
Canada's anti-spam legislation
Memorandum of Understanding
Joint announcement on anti-spam legislation
Joint letters on anti-spam legislation
Personal Information Protection and Electronic Documents Act *(PIPEDA)*

Catalonia
Law on the Protection of Data 32/2010
Catalan Transparency Law
Spanish Organic Law 3/2018

GDPR
Art. 36 GDPR

Hong Kong
Further information on Doxxing

Japan
Telecommunications Business Act
Act on Anonymized Medical Data That Are Meant to Contribute to Research and Development in the Medical Field.

Philippines
Data Privacy Act of 2012