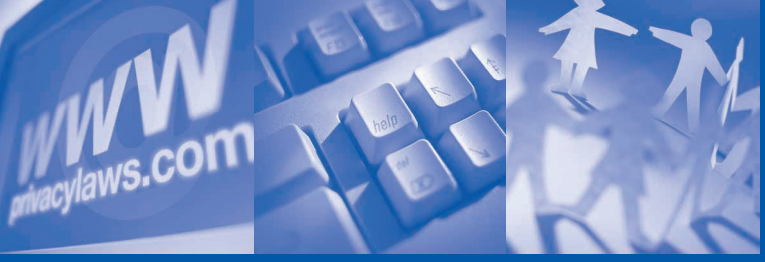

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Now 157 countries: 12 data privacy laws in 2021/22

Sri Lanka, Oman and the United Arab Emirates have adopted new data protection laws in 2022. **Graham Greenleaf** reports on recent developments.

Despite the Covid pandemic, countries across the globe have continued to enact data privacy laws. At the start of 2021, 145 countries had done so,[1] but in the year since then a further 12 countries have enacted such laws, giving a total of 157 by mid-March 2022. As has become familiar, most of these laws are influenced substantially by the EU's GDPR, but with many variations in such implementations. The

Continued on p.3

Apple AirTag debacle shows we need to diversify privacy

Diversifying privacy means more than diversifying product development and privacy teams. We need to broaden the aperture and centre marginalized voices. By **Abigail Dubiniecki**, Privacy lawyer and consultant.

"Apple's website states that 'privacy is a fundamental human right,' but one of its new products apparently didn't get the memo."[1]

Apple has long made privacy a key brand differentiator, with cutting-edge privacy engineering baked into its offering. Yet the PR fallout from privacy risks that surfaced soon

Continued on p.9

Partner with PL&B on Sponsored Events

***PL&B* would like to hear about your ideas for webinars and podcasts (topics, speakers).**

Multiple opportunities for sponsorship deals to build brand awareness with a globally recognised and trusted partner.

Email info@privacylaws.com

Issue 176 **APRIL 2022**

PL&B Services: Conferences • Roundtables • Content Writing
Recruitment • Consulting • Training • Compliance Audits • Research • Reports

INTERNATIONAL report

ISSUE NO 176 APRIL 2022

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Katharina A. Weimer
Fieldfisher, Germany

Nicole Wolters Ruckert and Tim Sweerts
Allen & Overy, Netherlands

Elizabeth Canter and Natalie Dugan
Covington & Burling, US

Abigail Dubiniecki
Independent privacy lawyer and consultant, Canada

Gabriela Kennedy and Joshua T. K. Woo
Mayer Brown, Hong Kong

Nada Ihab
Access Partnership, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2022 Privacy Laws & Business

comment

The many faces of AI

Recently, Italy's Data Protection Authority imposed a fine of €20 million on Clearview, and banned any further processing of citizens' facial biometrics (p.11).

Clearview has also been the target of regulatory action in the UK, France, Australia and Canada. The UK ICO conducted a thorough investigation into Clearview's processing of personal data in cooperation with the Office of the Australian Information Commissioner culminating in ordering the company to stop processing data. In France, the DPA has taken similar action.

Although the company has been heavily criticised for not having an adequate legal basis for its processing, now in Ukraine this facial recognition technology has been used to identify Russian soldiers that have died in Ukraine. While the power of AI can be advantageous in reuniting refugee families or identifying the dead, what happens if the database falls into the wrong hands?

I would be interested in hearing how your company is reacting to the war in terms of data transfers to and from Russia, and processing operations in both countries. Please let me know if you can share your experience with *PL&B* readers.

There is now positive news regarding the EU-US data transfer situation – the parties have announced that they have agreed, in principle, a new framework (p.31). The teams of the US Government and the European Commission will now continue their cooperation with a view to translate this outline arrangement into legal documents that will need to be adopted on both sides to put in place this new Trans-Atlantic Data Privacy Framework. For that purpose, these US commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision, the EU says. Both sides want to avoid a *Schrems III* banning judgement from the Court of Justice of the European Union.

This is welcome progress as it is expected that the final agreement will be ready this Spring. In the meantime, another three US states, Colorado (p.13),Virginia and Utah (p.15) have adopted data privacy laws (the California Consumer Privacy Act was adopted in 2018).

Internationally, Professor Graham Greenleaf reports (p.1) on 12 new data privacy laws in 2021/22, including the more recent ones in Oman, Sri Lanka and the United Arab Emirates.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Survey... from p.1

table below provides a summary, followed by a brief analysis of key features and sources for each law. Trends which may be emerging from these new laws are noted.

Twelve new national laws

The 12 new laws come from most regions of the globe: Central Asia, Latin America, the Caribbean, Africa, Asia and the Mid-East, plus the last state in Europe. Brief details follow of the laws, and where more details can be found.

Ecuador now has the 13th law in the 22 **Latin American** countries.

Ecuador – Organic Law on Protection of Personal Data 2021 (Latin America): In May 2021 Ecuador's *Organic Law on Protection of Personal Data* was enacted by its National Assembly, and after receiving no objection from the President, was gazetted and became law. The law established an independent Superintendency of Protection of Personal Data, to enforce the law and maintain a national registry of data controllers. The law has strong GDPR similarities:[2] data subject rights including data portability, the "right to be forgotten" and controls on automated processing; extra-territorial scope similar to the GDPR ("white list" and "appropriate safeguard" provisions, but not a local representation requirement); and requirements for many organisations to have a DPO. Administrative penalties for breaches can range from 3% to 17% of the previous year's revenue of an organisation. One trigger for the law was a 2019 data breach affecting nearly all Ecuadorians, where considerable amounts of personal data were stored outside Ecuador without the authorization of data subjects.[3]

El Salvador's Assembly also passed a *Law on the Protection of Personal Data and Habeas Data* in April 2021, but it was vetoed on 7 May 2021 by the President on the grounds of deficiencies in its consistency with other aspects of El Salvador's laws, and lack of expertise in the proposed data protection authority.

Two more jurisdictions in the **Caribbean** have enacted new laws, bringing the total to 16 of the 29 Caribbean states.

British Virgin Islands – Data Protection Act 2021 (Caribbean): The British Virgin Islands (BVI) are a

TABLE OF NEW COUNTRIES WITH DATA PRIVACY LAWS 2021-22

Country	Title of law	Data protection authority	Region
Rwanda	Law Relating to the Protection of Personal Data and Privacy 2021	National Cybersecurity Authority	Africa
Zimbabwe	Data Protection Act 2021	Postal and Telecommunications Regulatory Authority	Africa
Zambia	Data Protection Act 2021	Data Protection Commissioner	Africa
Sri Lanka	Personal Data Protection Act 2022	Data Protection Authority of Sri Lanka	Asia
British Virgin Islands	Data Protection Act 2021	Information Commissioner	Caribbean
Belize	Data Protection Act 2021	Data Protection Commissioner	Caribbean
Mongolia	Law on Protection of Personal Information 2021	National Human Rights Commission & Communications and Information Technology Authority	Central Asia
Belarus	Law on Personal Data Protection 2021	National Personal Data Protection Center	Europe
Ecuador	Organic Law on Protection of Personal Data 2021	Superintendency of Protection of Personal Data	Latin Am
Saudi Arabia	Personal Data Protection Law 2021	Data & Artificial Intelligence Authority	Mid-East
United Arab Emirates (Federal)	Law regarding personal data protection 2022	UAE Data Office	Mid-East
Oman	Personal Data Protection Law 2022	Ministry of Transport, Communications and Information Technology	Mid-East

British Overseas Territory located in the Caribbean and part of the West Indies. The total population of BVI is under 40,000, but with a high per capita GDP of over USD 35,000. BVI is a parliamentary democracy with a single elected house. The *Data Protection Act 2021* was enacted, by being gazetted, on 13 April 2021, to come into force on a date or dates to be appointed by the Minister. It applies to government activities, but otherwise only applies to the processing of any personal data in respect of commercial transactions, so non-commercial activities (clubs etc) are exempt. Local experts consider the law to be relatively "light touch", in comparison with other Caribbean laws.[4] It includes modest sets of rights and controller ("user") obligations. The Minister may prescribe that "any other personal data" may be "sensitive personal data". The Act establishes an Information Commissioner, but with no explicit statement of independence. Maximum fines of USD $250,000 are now modest compared with some other Caribbean jurisdictions. A direct right of appeal to the Eastern Caribbean Supreme Court is available for persons aggrieved by decisions of the Commissioner.

Belize – Data Protection Act 2021 (Caribbean): Belize is considered to be a Caribbean country, although it is located on the north-eastern coast of Central America, bordering Mexico to the north, and the Caribbean Sea to the east. It is the only Central American country where English is the official language and is a member of the Commonwealth, and "it is considered a tax haven".[5] With a population of less than 500,000 and a per capita GDP under USD 5,000, Belize is a small fish.

The Belize *Data Protection Act*, No. 45 of 2021 was enacted by its National Assembly and assented to by the Governor-General on 29 November 2021. The Act creates an office of Data Protection Commissioner. It is considered to draw heavily for inspiration on Barbados' Data Protection Act, but without the obligation for data controllers to be registered.[6] Some unusual features of the Act include: the inclusion of financial records as "sensitive information"; the exemption of "small businesses" from compliance with the Act; and the exemption of cloud storage from the data export provisions. Other more usual features include data breach notification and demonstrable accountability requirements.

Since September 2021, three comprehensive data privacy laws have been enacted in the **Middle East**, in Saudi Arabia, the United Arab Emirates and Oman, so that 11 of the 14 states of the region now have such laws. These three countries share land borders, so most of the Arabian Peninsula now has comprehensive data privacy laws.

Saudi Arabia – Personal Data Protection Law 2021 (Mid-East): The *Personal Data Protection Law* was adopted by Royal Decree on 16 September 2021, and took effect on 23 March 2022, with controllers having a year to comply. It is a comprehensive law (public and private sectors). The law is considered to be generally "in line with international data protection laws" and in particular with many aspects of the EU's GDPR.[7] Its full implications will not be clear until Executive Regulations are issued.

The law has GDPR-like provisions concerning purpose limitation, limited exceptions for non-consensual processing, data minimisation, most of the data subject's rights (but not data portability, or limits on automated processing), strict data breach notification requirements; and impact assessments. However, many aspects differ from the GDPR, including limited extra-territoriality benefiting Saudi citizens only; a non-independent data protection authority (initially, the Saudi Data & Artificial Intelligence Authority); registration of controllers; and application to deceased persons. It has a strict approach to data exports, generally limiting them to where standards not less than those in Saudi law will apply, and approval to export is also obtained from the Authority. The Authority may decide to issue a "white list" of countries providing an acceptable level of protection. The Authority may issue fines for breaches of up to USD 2.6 million, or award compensation.

United Arab Emirates – Law regarding personal data protection 2022 (Mid-East): The UAE *Federal Decree Law No. 45 of 2021 regarding personal data protection* was issued on 2 January 2022, but controllers and processors have six months to comply. This federal law will operate alongside but not replace the free trade zone laws of Dubai and Abu Dhabi. Regional experts consider that it "reflects international data protection principles and requirements, particularly [the EU GDPR]".[8] Among the stronger obligations in the law are requirements for Data Protection Officers and data protection impact assessments. Data subject rights include data portability and rights to object to automated decision-making. A separate law (Federal Decree Law No. 44 of 2021) establishes the UAE Data Office to supervise the law, but does not make it independent. Penalties for breaches are not specified in the law – this will occur in regulations.

Oman – Personal Data Protection Law 2022 (Mid-East): The Sultanate of Oman is the oldest continuously independent state in the Arab world. Its population of nearly five million has a per capita GDP of USD 47,000, making it a high-income country. Royal Decree No. 6 of 2022 promulgated the *Personal Data Protection Law 2022* (PDPL) on 9 February 2022. The Ministry of Transport, Communications and Information Technology (MTCIT), which is designated as the data protection authority under the law, will also issue executive regulations to expand on the 32 articles of the law (including on data exports). The law will come into effect a year after its promulgation. The law is as yet only available in Arabic, but commentary is available from regional law firms.[9]

Although the law does in theory cover both the public and private sectors, there is a lengthy list of exclusions from its scope, including acts by state bodies or public authorities within their legal competence, protection of various state interests and private interests, and data which is available to the public in a manner which is not contrary to the PDPL. The law requires explicit consent to any processing of personal data, unlike other laws (for example the GDPR) that make provision for non-consensual processing. However, where processing falls within any of the excluded categories, it appears that the law does not apply at all.[10] The exclusions will therefore play to some extent a similar role to non-consensual processing. The rights of

 © 2022 PRIVACY LAWS & BUSINESS

data subjects include many that are found in laws such as the GDPR, including rights to rectify, update or block, rights of erasure, access, data portability, and rights of data breach notification (with MTCIT also to be informed). The MTCIT can investigate complaints and has a variety of enforcement tools. Administrative fines may reach a maximum of OMR 500,000 (USD 1.3M).

In addition, **Kuwait's** Communication and Information Technology Regulatory Authority promulgated the Data Privacy Protection Regulation in June 2021. However, unlike the Middle East laws described above, this is not a "data privacy law" for the purposes of my global Table, because it does not have sufficient scope in either the private or public sectors. It is limited to a controller "who provides communications and information technology services" and only "when it relates to processing activities linked to transmission of advertising or marketing material or monitoring the behaviours and tendencies of data owners". It is therefore only a sectoral law, but one which imposes significant obligations on those service providers within its scope (p.25).[11]

Mongolia is the last country in **Central Asia** to enact a data privacy law. The other five countries, all previous republics of the USSR, have done so in recent years. Kazakhstan amended its law in 2021 to include provisions on data breach notification and clarify data localisation.

Mongolia – Law on Protection of Personal Information 2021 (Central Asia): Mongolia is a landlocked country between China and Russia which has become a multi-party democracy since 1989. It has a population fewer than 3.5 million and per capita GDP of under USD 15,000. In January 2022 the enactment was announced of the *Law on Protection of Personal Information*, to enter into force on May 1, 2022.[12] The law covers the public sector, but its application to the private sector remains to be ascertained.[13] The law defines terms such as personal privacy, sensitive information (including genetic and biometric data, information about sex life and sexual orientation, and medical records), controller, processor, based on the standards of other countries. It also regulates conditions for the collection, processing and use of sensitive data and their use for historical, scientific research and analysis purposes. The law also regulates surveillance by audio and video recording equipment in public places. The law is part of a package of "e-Mongolia" laws enacted to accelerate the development of digital government in Mongolia which also includes public information and open data laws, a cybersecurity law and a digital signature law.[14]

Sri Lanka – Personal Data Protection Act 2022 (Asia): In **South Asia**, Sri Lanka has won the race (against India and Pakistan) to enact a modern, if flawed, data privacy law. After four revised versions,[15] Sri Lanka's Personal Data Protection Bill[16] finally made it to the Ministerial Consultative Committee on Technology on 8 March 2022, where it was endorsed. It was then presented to Parliament on 9 March where it was given all readings and enacted on the same day, with amendments, being passed without a vote. Extensive amendments (29 pages) were proposed but it is not yet known which were adopted. The Bill (as introduced) requires that the role of Data Protection Authority of Sri Lanka must be given to an existing government body, not a new and independent body. This deficiency, plus the perceived weakness of protections for the media and academics, and the fact that this Act will override all other laws, including the Right to Information Act, has received wide criticisms from Sri Lankan and international media and free speech organisations.[17] Amendments proposed[18] included creation of a Board of Directors of five to seven eminent persons; licensing of categories of controllers and processors; and payment of compensation for harm resulting from breaches of the Act. The final Act will be reviewed in a later issue of *PL&B International Report*.

Three more **African** countries – Rwanda, Zimbabwe and Zambia – have enacted data privacy laws, bringing to 35 of the 55 African countries with such laws. The three laws give a clear illustration of the diversity of ways in which data privacy is implemented in Africa, while still maintaining strong influences of the EU GDPR.

Rwanda – Law Relating to the Protection of Personal Data and Privacy 2021 (Africa): Law No. 058/2021 of 13 October 2021 *Relating to the Protection of Personal Data and Privacy* came into force on its publication in the Official Gazette two days later. It is available from the Ministry of Justice website.[19] Enforcement powers are given to the National Cybersecurity Authority (NCSA), with transition to enforcement over two years.[20] Legitimate data processing is defined in terms similar to the GDPR. Data subject rights include, as well as broad rights of access, objection and restriction, less usual rights such as data portability, restrictions on decision-making based on automated processing, and a right to designate an heir to personal data. The obligations of data controllers and processors can include to carry out data protection impact assessments, to appoint a data protection officer (DPO), and to inform data subjects of data breaches. Data exports can be based on a number of grounds, including the NCSA being satisfied with appropriate safeguards, but there is no provision for jurisdictions being held to provide adequate protection. However, NCSA could add additional grounds, including approving standard contractual terms. Data localisation (storage in Rwanda) is required unless the controller or processor has a registration certificate permitting storage outside Rwanda. The NCSA will maintain a register of data controllers and processors and can cancel registrations for failure to comply with the law. Failure to comply with some (but not all) provisions of the law can result in administrative fines up to USD 5,000 or 1% of global turnover in the previous year. The NCSA can add other fines by regulations. Compensation may be claimed through court processes. Rwanda's law is therefore a quite strong implementation of the GDPR's approach, except in relation to data localisation and registration.

Zimbabwe – Data Protection Act 2021 (Africa): The *Data Protection Act* was enacted in December 2021. It creates the functions of a Data Protection Authority (DPA) but gives responsibility for those functions to the Postal and Telecommunications Regulatory Authority (POTRAZ). It also creates a Cyber Security and Monitoring of

Interceptions of Communications Centre (CSMC), relevant to the cybersecurity aspects of the law. The Act includes higher standards for the processing of sensitive data, and limited sets of obligations on data controllers (s. 13), and limited rights for data subjects (s. 14). Some more modern elements are included such as data breach notification, categories of processing requiring specific authorisation from the DPA, demonstrable accountability, and limits on decisions based on automated processing. Data exports are subject to requirements of an adequate level of protection in the recipient country, with such adequacy to be determined (it seems) by the DPA establishing a "black list" of circumstances where transfers are not authorised, subject to directions by the Minister responsible for the CSMC. Other methods of transfer are also specified, but without the inclusion of Standard Contract Clauses or intergroup transfers. Breaches of the Act can result in convictions leading to fines or imprisonment, but other means of enforcement are lacking. The Act also includes cybercrime offences. The Media Institute of Southern Africa (MISA) Zimbabwe has made considerable criticisms of the law, while welcoming its existence.[21]

Zambia – Data Protection Act 2021 (Africa): The *Data Protection Act 2021* establishes an Office of Data Protection Commissioner within the telecommunications Ministry. In addition to the usual functions of a DPA, it is to register controllers and data processors, and licence data auditors. The Data Protection (Registration and Licensing) Regulations, 2021 issued in May 2021, are mainly for this purpose. Processing data without the necessary permit is a serious offence (imprisonment for up to five years), and contraventions of the Act or orders of the Commissioner may lead to revocation or suspension of permits. The Commissioner's qualifications are specified, but independence not guaranteed. Inspectors are also to be appointed, with unusually broad powers to enter premises, inspect records, detail property, conduct arrests etc. Exemptions from the Act (Part VII) are limited.

The principles relating to processing personal data (Part IV) include grounds for legitimate processing (including legitimate interests), strong protections for sensitive personal data, and minimality in processing (limits on collection, use and disclosure). Duties of data controllers and processors (Part VIII) include data protection impact assessments, appointment of DPOs where the Commissioner requires, data breach notification to the Commissioner and the data subject and demonstrable accountability. Other GDPR obligations are not included. Corporations breaching these requirements of Parts IV or VII may be liable on conviction to a penalty up to 2% of turnover (presumably within Zambia) of the previous financial year. The rights of data subjects (Part IX) are comprehensive, including limits on automated processing, and data portability. They are enforced through complaints to the Commissioner (which may be against any breach of the Act), with a right of appeal to the High Court. Compensation for damage caused by breaches of data subject's rights is through court proceedings. Data export and localisation provisions (Part X) are complex and unusual. In default, all processing and storage must be on a server or data centre located in Zambia, unless the Minister prescribes "categories of personal data" that may be stored elsewhere (but not for sensitive data). Conditions allowing exports of personal data follow, including for white lists based on adequate protection and effective enforcement (decided by the Minister) and standard contracts or intragroup schemes (approved by the Commissioner or the Minister). Except for its heavy reliance on licensing provisions, use of convictions rather than administrative fines, and its data localisation provisions, Zambia's law is strongly influenced by the EU GDPR.

Belarus – Law on Personal Data Protection 2021 (Europe): Belarus is the last state in Europe to enact a data privacy law, an appropriate result for one of the most authoritarian and undemocratic regimes on the continent, and the only state which is not a member of the Council of Europe (mainly because of its lack of democracy). Russia's invasion of Ukraine from Belarus territory also puts into question whether it can be any longer regarded as an "independent" state. The Belarus Law on the protection of personal data was signed into law on 7 May 2021 and came into effect on 15 November 2021. The National Personal Data Protection Center was also established by Presidential Edict No. 422 dated 28 October 2021, but with no indication that it is an independent body. It will handle complaints and administer approval of data exports. The Law is, on paper, said to be similar in many respects to the GDPR, including data subject rights limiting decisions made solely on the basis of automated processing, and the right to data portability.[22] Enforcement is relatively light, such as fines limited to USD 2,264.

The inclusion of Belarus underlines that, while these 11 laws meet the minimum formal requirements for a data privacy law[23] on their face, this says nothing about whether the laws are effectively enforced, or about the data surveillance context in which such laws exist and which may largely nullify their potential benefits.

Revised Acts, and Bills for revised Acts

Some of the most important data privacy legislation enacted in 2021 does not appear in the above table. For example, in 2021 China[24] revised its existing patchwork of laws into its comprehensive *Personal Information Privacy Law*. In addition, India[25] and Indonesia[26] have comprehensive Bills, not yet enacted, to replace their existing sub-standard non-comprehensive laws. These are the world's three largest countries by population. Other countries enacted significant updates to existing laws in 2021, including Vietnam,[27] South Korea, Hong Kong, Kazakhstan, Russia, Andorra, Abu Dhabi, Uzbekistan, Cayman Islands and various EU member states (to implement parts of the GDPR).

Emerging trends in 2021-22

From the 11 new data privacy laws distributed globally and the significant updates to laws in 2021, some interesting features, possibly emerging trends, include:

- The EU GDPR (incorporating its predecessor, the 1995 Data Protection Directive is clearly the *global template* on which most other

 © 2022 PRIVACY LAWS & BUSINESS

countries' new laws are based, to a high extent (Ecuador, Rwanda, Zambia) or lesser extent (Belize, BVI, Oman, Mongolia, Zimbabwe).
- Most of the new laws still fail to create genuinely *independent* data protection authorities (at least BVI, Zimbabwe, Rwanda, Oman, UAE, Saudi Arabia, Belarus, Sri Lanka), although all of these laws do create or nominate some specialised enforcement body.
- *Extra-territorial* jurisdiction has become common in a few years but is often implemented differently from the GDPR (Ecuador, UAE, Saudi Arabia, Sri Lanka, China).
- Some new principles originating in the GDPR are already very commonly enacted outside the EU, like data breach notification, but others which used to be rare are increasingly being adopted, like *data portability* (Ecuador, Oman, Rwanda, Zambia, UAE, Belarus) and *demonstrable accountability* (Belize, Zimbabwe).
- Administrative penalties based on a percentage of the *previous year's turnover* of a controller do occur (Ecuador, Rwanda, China), but maximum fines based on a dollar amount are also common and are very often over USD 1 million (Saudi Arabia, Oman).
- Most new laws include *adequacy-like* data export controls based on the extent to which the receiving country's laws approximate their own (Saudi Arabia, UAE, Zimbabwe, Zambia, Sri Lanka, China), as well as allowing other bases such as contractual protections.

Some features which are not "GDPR-inspired" are also recurring in these new laws:
- Forms of *data localisation* (Rwanda, Zambia, Sri Lanka, China) are no longer rare.
- Rights of *deceased persons* are not uncommon (Saudi Arabia, Rwanda, China).
- *Registration systems* are still created (Saudi Arabia, Rwanda, Zambia), despite being superseded in the EU.

The failure of such a high percentage of laws to create independent DPAs

TABLE OF BILLS (AND OFFICIAL DRAFT BILLS) FOR NEW ACTS

Jurisdiction	Title of Bill/Draft	Region
eSwatini (Swaziland)	Data protection Bill 2020	Africa
Ethiopia	Data Protection Bill	Africa
Saint Helena, Ascension & Tristan de Cunha	Data Protection Act	Africa
Tanzania	Data Protection Bill	Africa
Malawi	The Data Protection Bill 2021	Africa
South Sudan	Draft Data Protection Bill 2020	Africa
Bangladesh	Draft Data Protection Bill 2021	Asia
Pakistan	Personal Data Protection Bill	Asia
Brunei	Draft Personal Data Protection Order	Asia
Cuba	Data Protection Bill 2022	Caribbean
Guyana	Draft data privacy Bill	Caribbean
El Salvador	Data Protection Law	Latin Am
Guatemala	Ley de Protección de Datos Personales	Latin Am
Suriname	Privacy and Data Protection Bill	Latin Am
Honduras	Draft Law on Protection of Personal Data and Habeas Data	Latin Am.
Iran	Draft Personal Data Protection and Safeguarding Act	Mid-East
Jordan	Draft Law on Data Protection	Mid-East

presents problems for those countries (i) obtaining a positive adequacy assessment from the EU, (ii) acceding to Convention 108+, and (iii) in having their DPAs become full members of the Global Privacy Assembly (GPA).

Bills for laws in new countries

There are at least 17 countries, listed in the preceding table, that do not have data privacy laws, but do have official Bills or draft laws at various stages of the political and legislative processes.

Conclusions – Ubiquity is still on track

The total of 157 countries with data privacy laws means that two thirds (67%) of the world's 232 independent jurisdictions now have such laws. For the future, there are already substantial numbers of draft Bills in new countries in Africa, Latin America, the Mid-East and Asia – and probably more that have not yet been identified. The increase in the total number of countries with data privacy laws is unlikely to stop in the near future, as we move toward a world where data privacy laws – of varying qualities – are ubiquitous.

INFORMATION

Valuable information and comments have been received from David Banisar, Article 19, Tamar Kaldani, independent consultant and Gimhani Anuththara, Open University of Sri Lanka, but responsibility for all content remains with the author.

REFERENCES

1 G. Greenleaf 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 *Privacy Laws & Business International Report*, 1, 3-5; G. Greenleaf 'Global Tables of Data Privacy Laws and Bills (7th Ed, January 2021)' (2021) 169 *Privacy Laws & Business International Report*. 6-19. There may be 146: the existence of Comoros' alleged data privacy law of June 26 2014 remains unconfirmed.
2 Rafael S. Barona 'Ecuador's draft Data Protection Bill' 5 March 2021 iapp Privacy Tracker iapp.org/news/a/ecuadors-new-data-protection-law/
3 Barona *ibid*
4 Bartlett Morgan 'Data Protection: BVI has entered the chat!' 1 April 2021 bartlettmorgan.com website
5 Wikipedia: Belize
6 Bartlett Morgan 'Belize's proposed Data Protection Law adds unique spin to the familiar' bartlettmorgan.com website
7 Dino Wilkinson and Masha Ooijevaar 'Saudi Arabia issues its first standalone data protection law' (2021) 173 *Privacy Laws & Business International Report*, 1, 3-5.
8 Dino Wilkinson and Masha Ooijevaar 'United Arab Emirates federal data protection law in force' (2022) 175 *Privacy Laws & Business International Report*, 1, 3-5.
9 Taimur Malik and Dino Wilkinson 'Data Protection Law issued in Oman' 15 February 2022, Clyde and Co website www.clydeco.com/en/insights/2022/2/data-protection-law-issued-in-oman
10 Malik and Wilkinson *ibid*
11 See p.25 in this issue.
12 Misheel Lkhasuren 'Legal environment has been created for e-transition in Mongolia' UB Post theubposts.com/legal-environment-has-been-created-for-e-transition-in-mongolia/
13 Little information is yet available in English or Russian. Details will be provided in a subsequent article.
14 B. Bolor-Erdene 'How To Do Digital Government: Experiences From E-Mongolia' 8 February 2022, Urbanet www.urbanet.info/digital-governance-mongolia/
15 The first three versions are reviewed in G. Greenleaf, 'Pakistan's and Sri Lanka's data privacy Bills move forward' (2021) 173 *Privacy Laws & Business International Report*, 24-27 and earlier articles cited therein.
16 The latest pre-parliamentary Bill is the Personal Data Protection Bill in the November 19 2021 Government Gazette documents.gov.lk/files/bill/2021/11/152-2021_E.pdf. The same Bill was introduced into Parliament on 20 January 2022 www.parliament.lk/business-of-parliament/acts-bills#current
17 Editorial 'Sri Lanka's Personal Data Protection Bill Leads To Public Uproar' *Colombo Telegraph*, 9 March 2022 www.colombotelegraph.com/index.php/sri-lankas-personal-data-protection-bill-leads-to-public-uproar/ ; Access Now Policy brief: Nine steps to protect our data and privacy in Sri Lanka February 2022 www.accessnow.org/cms/assets/uploads/2022/02/Policy_Brief_Sri_Lanka_Data_Protection_Bill_February_2022.pdf; Transparency International Sri Lanka Branch Legislative Brief: Personal Data Protection Bill 2021 1 February 2021 www.tisrilanka.org/wp-content/uploads/2021/07/TISL-Legislative-Brief_Personal-Data-Protection-Bill_13.07.2021.pdf
18 Personal Data Protection Bill (Sri Lanka) Amendments to be moved at the committee stage of the Bill.
19 Rwanda's Law Relating to the Protection of Personal Data and Privacy www.minijust.gov.rw/fileadmin/user_upload/Minijust/Publications/Official_Gazette/_2021_Official_Gazettes/October/OG_Special_of_15.10.2021_Amakuru_bwite.pdf
20 Ministry of ICT and Innovation (Rwanda) Press Release 21 October 2021 'Rwanda passes new law protecting personal data' www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Press_Release/211021_PRESS_RELEASE_Rwanda_s_New_Data_Protection_Law_ENGLISH.pdf
21 MISA 'Analysis of the Data Protection Act' 6 December 2021 zimbabwe.misa.org/2021/12/06/analysis-of-the-data-protection-act/
22 Caseguard 'The PDP, A New Standard for Data Privacy Rights in Belarus' 27 October 2021 caseguard.com/articles/the-pdp-upholding-data-privacy-rights-in-belarus/
23 For the standards applied, see a summary in G. Greenleaf 'Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority' (2015) 133 *Privacy Laws & Business International Report*, February 2015.
24 G. Greenleaf 'China's completed Personal Information Protection Law: Rights plus cyber-security' (2021) 173 *Privacy Laws & Business International Report*, 20-23
25 G. Greenleaf 'Report keeps India's DP Bill partly within GDPR orbit' (2022) 175 *Privacy Laws & Business International Report* 1, 6-9
26 G. Greenleaf and A. Rahman. 'Indonesia's DP Bill lacks a DPA, despite GDPR similarities' (2020)164 *Privacy Laws & Business International Report* 1, 3-7
27 G. Greenleaf 'Vietnam: Data privacy in a communist ASEAN state' (2021) 170 *Privacy Laws & Business International Report*, 1, 5-8

 © 2022 PRIVACY LAWS & BUSINESS

Diversification... from p.1

after the launch of its AirTags product[2] has exposed a significant privacy blind spot for the tech darling. Designed to track things, AirTags have enabled stalking[3], car theft,[4] and other safety risks. In a decidedly off-brand move, Apple's AirTags have actually introduced new privacy risks and exacerbated existing social inequalities. What's more, Apple may have inadvertently normalized and sanitized digital stalking: "It's not a spy tool marketed as a spy tool, because it's marketed as an AirTag, and it's Apple," observes the CEO of an organization focused on tackling tech-enabled abuse.[5]

The AirTag debacle highlights the need to both diversify product and privacy teams to get different perspectives and broaden the aperture for assessing privacy risk beyond the individualistic customer-centric focus.

The Apple AirTag debacle

AirTag was designed to help individuals track things in a privacy-preserving way: "Only you can see where your AirTag is. Your location data and history are never stored on the AirTag itself. Devices that relay the location of your AirTag also stay anonymous, and that location data is encrypted every step of the way. So not even Apple knows the location of your AirTag or the identity of the device that helps find it."

But AirTags can be used to surreptitiously track others against their will, creating significant privacy and personal safety risks for journalists, intimate partners, and other potential stalking targets, some of whom enjoy no contractual relationship with Apple and thus have little to no control over the tracking. Apple's original anti-stalking features – whilst better than its competitors – fell far short of the mark.[6] Yet recent improvements contain stubborn loopholes that can be easily exploited.[7] Worse, the anti-stalking features favour those privileged enough to use an iPhone, leaving Android users with weaker protections and those without a mobile phone with virtually no effective protection.[8] While Apple has tried to remedy the Android issue, it's clear it cannot solve this problem alone. It will need to collaborate with its competitors,[9] and consult outside its usual customer base.

With this foray into the tracking fob world, AirTags joins the ranks of well-intentioned digital products bringing unforeseen consequences. Per Allie Funk, a senior research analyst for technology and democracy at Freedom House www.freedomhouse.org: "AirTags are only the latest consumer tech product billed as offering convenience even as developers ignore, understate or underestimate the possibility for harm, reflecting a larger problem of the digital age: We have welcomed into our lives an entire ecosystem of dubious tracking tools designed with minimal safeguards against abuse."[10]

That not-so-illustrious list includes:

- Fertility apps that share health data with tech giants Facebook and Google;[11]
- Facial recognition systems that fail to see some people while incorrectly identifying others, leading to erasure or false arrests;[12]
- Home security systems that double as state surveillance networks for targeting Black Lives Matters activists;[13]
- Automated recruitment algorithms that hardwire bias against female candidates;[14]
- Social media personalisation features that create body image issues or hyper-target disinformation;[15]
- Direct to consumer genetic testing and sharing of genetic data to enable mass surveillance and targeting of certain populations, such as the military or minorities.[16]

In all of the above cases, the significant societal harms were only discovered after they had significantly impacted numerous victims, many of whom were innocent third parties with no direct relationship with the company. It also dealt a blow to the company's brands, sowing even greater distrust of Big Tech.

Lessons learned – the need for diversity

Why does this keep happening, and how can we prevent it?

Silicon Valley is notorious for its lack of diversity, and Apple is no exception. It neglected to include a period tracker in its first health app and other women's health features – an embarrassing fail that could have been avoided with a gender-balanced product team empowered to speak frankly.[17] This lack of diversity not only leads to unintended consequences and embarrassing omissions already mentioned, it also holds tech back.[18]

But the need for diversity is about more than representation. Quotas ensuring the-right-faces-in-the-right-places alone won't address the underlying problem.

"Insanity is doing the same thing over and over again and expecting different results." The insanity of digital tech manifests itself in a continuous stream of privacy and human rights failings, each worse and more consequential than the last. This is unsustainable, but explainable, and avoidable:

"Adaptive algorithms do not create injustice on their own, but they do amplify it when they respond to unjust laws, institutions, or human behavior … If we change algorithms without changing underlying behavior, algorithm policies could fail in similar ways," notes one scholar[19] featured on the newly launched JustTech platform, a website and community focused on exploring "questions of power, justice, and the public impact of new technologies while imagining and creating more just and equitable futures."[20]

Another contributor assessing privacy-invasive employee tracking technologies cautions Big Tech on the need to centre marginal voices: "The next generation of Big Tech must understand the range of potential harms and risks their products can introduce to society and the economy and listen to workers who are at the forefront of each."[21]

Privacy professionals can help their companies and clients avoid repeating the mistakes of Big Tech's past by broadening their horizons beyond the privacy and data protection bubble. Reading – and listening – to thought leaders who operate outside traditional corporate compliance spaces - can help break the cycle.

Lessons learned from AirTags illustrate why, and how:

1. **Legislation lags behind public expectations**: Apple's AirTags don't violate any laws, in fact Apple has voluntarily exceeded regulatory requirements. Yet in the court of public opinion, it has

failed to live up to expectations. Had Apple consulted more broadly or more deeply anticipated consequences beyond the customer relationship, it might have prevented some of the harms or determined the trade-off wasn't worth it.

Human rights impact assessments, consequence-scanning and data ethics canvas tools can help consider privacy and other risks at the design stage more broadly.[22] Cross-sectional / multi-disciplinary research can provide helpful content to inform these activities.[23]

Stepping outside the privacy and data compliance bubble – with its focus on regulatory compliance with individualistic and transactional privacy regimes – can expose a privacy professional to important lessons and perspectives of scholars, innovators and activists in the Data Justice,[24] Indigenous Data Sovereignty,[25] Decolonize DNA,[26] Digital Black Feminism and Indigenous AI movements. These rich areas of activity have highlighted privacy risks and deficiencies in many cutting-edge technologies, including automated decision-making[27], biometrics and facial recognition,[28] AI and natural language processing,[29] open data and collective privacy risks,[30] democratizing data and addressing market dominance.[31]

2. Being the best of the worst is not good enough: Apple has positioned itself as a force for change in this market, by creating above-average privacy and anti-stalking features. Yet exceeding this very low bar offers little solace to those fighting tech-enabled abuse. Many Silicon Valley innovations have marginalized or further exacerbated social inequality. This is due in part to a lack of representation at the decision-making and design table, or a stubbon refusal to listen to the diverse voices that challenge the status quo of the data economy, as Google's controversial dismissal of Black data scientist Timnit Gebru illustrates.[32]

Exchanging personal safety for convenience seems an unwise bargain, yet the victims of this trade-off often have no seat at the negotiating table. Rather than raising the bar for the tech industry, Apple may have sullied its reputation by joining the ranks of tech companies normalizing surveillance without considering consequences.

3. Privacy premiums exacerbate social inequality: AirTags offer greater convenience to an already privileged portion of society who can afford the privacy premiums associated with Apple's privacy-preserving products, while introducing significant risks of harm to others by tracking them against their will and sometimes without their awareness including people who are already at a social disadvantage due to abusive relationships or socio-economic status. Privacy is supposed to be a right, not a privilege,[33] and until we treat it that way, we will continue to reproduce inequalities in the digital ecosystem that will hold us all back.[34]

4. Need to broaden the aperture beyond the individual: The focus on individual privacy disregards the inherent connectedness of individuals and the potential for community harms, which becomes particularly relevant when it comes to genetics.[35] However, even de-identified and aggregated data – such as mobility data or mean income data – can be used to discriminate against communities, e.g. through digital red-lining, excessive policing, or hiring decisions.

5. Not every social problem requires a tech solution: Techno-chauvinism has privileged digital technology solutions when others may suffice, often leading to disproportionate data processing and increased intrusion into our lives by digital products. We are designing for humans, and sometimes that means finding human solutions to human problems.

Conclusion

Diversifying privacy is critical to avoiding the mistakes of our recent past and creating a more equitable digital future that delivers on tech's promises.

Diversifying the workforce is one step. This is not charitable endeavour – it's common sense. The misconception of some hiring managers that this entails "lowering standards" ignores the significant contributions that groups typically underrepresented in the privacy compliance space have made in the fields of digital privacy and STEM (science, technology, engineering and mathematics). With an array of perspectives, we can in fact raise the bar for digital privacy.

Yet diversifying through representation alone will not prevent the next AirTags debacle. By escaping the compliance bubble, challenging the status quo of the digital economy and centering marginalized voices, privacy and product teams can re-imagine a more just digital economy where privacy is truly baked in, not an add-on or mere theatre. One that might break the vicious cycle of endless privacy and human rights failings that currently plague Big Tech.

AUTHOR

Abigail Dubiniecki is a privacy lawyer and consultant based in Canada who helps clients in the UK and Canada implement GDPR and other privacy and data protection laws. She specializes in operationalizing Privacy by Design and is a privtech and emerging tech enthusiast. Contact: www.linkedin.com/in/abigaild

REFERENCES

1 thehustle.co/01042022-apple-airtag
2 Product page: www.apple.com/airtag
3 www.bloombergquint.com/business/apple-boosts-privacy-of-airtags-after-they-re-used-for-stalking
4 www.techspot.com/news/93062-apple-airtag-quickly-becoming-perfect-tool-stalking-android.html
5 www.theverge.com/2022/3/1/22947917/airtags-privacy-security-stalking-solutions
6 www.theverge.com/2021/6/3/22516178/apple-airtags-tracking-devices-update-play-sound-privacy-android-app
7 www.theverge.com/2022/3/1/22947917/airtags-privacy-security-stalking-solutions
8 www.washingtonpost.com/opinions/2021/05/13/apple-airtag-tracking-threats-abuse
9 appleinsider.com/articles/22/02/21/collaboration-needed-to-address-stalking-by-airtag-tile-and-other-devices
10 www.washingtonpost.com/opinions/2021/05/13/apple-airtag-tracking-threats-abuse/

 © 2022 PRIVACY LAWS & BUSINESS

REFERENCES

11 www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about
12 See The Coded Gaze : Unmasking Algorithmic Bias: youtu.be/162VzSzzoPs and abcnews.go.com/US/black-man-wrongfully-arrested-incorrect-facial-recognition/story?id=71425751
13 www.eff.org/deeplinks/2021/06/ring-changed-how-police-request-door-camera-footage-what-it-means-and-doesnt-mean
14 www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.
15 See www.theguardian.com/technology/2021/sep/14/facebook-aware-instagram-harmful-effect-teenage-girls-leak-reveals www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires time.com/4783932/inside-russia-social-media-war-america/ and www.thedrum.com/news/2019/08/22/carole-cadwalladr-slams-missing-action-bbc-amid-cambridge-analytica-fallout
16 The US Army has cautioned the military about national security risks that may arise from genetic testing: www.army.mil/article/232314/osd_advises_service_members_against_using_dtc_genetic_testing. An American scientist unwittingly contributed to genetic surveillance of the Uighur minority in China: www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.
17 www.engadget.com/2018-09-07-fitness-health-tracking-pregnancy.html
18 www.msn.com/en-us/news/technology/op-ed-silicon-valleys-huge-diversity-problem-holds-tech-back/ar-AAUITDp.
19 Matias, Nathan and Lucas Wright. "Impact Assessment of Human-Algorithm Feedback Loops." Just Tech. Social Science Research Council. March 1, 2022. DOI: doi.org/10.35650/JT.3028.d.2022
20 Miller, Michael. "Introducing the Just Tech Platform." Just Tech. Social Science Research Council. February 15, 2022. DOI: doi.org/10.35650/JT.3026.d.2022. SSRC is a US-based think tank.
21 Negrón, Wilneida. "A 'Just' Tech Boom." Just Tech. Social Science Research Council. DOI: doi.org/10.35650/JT.3019.d.2022
22 Sample Human Rights Impact Assessment toolkit: www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox/introduction-human-rights-impact-assessment Consequence scanning toolkit: doteveryone.org.uk/project/consequence-scanning the Data Ethics Canvas: theodi.org/article/the-data-ethics-canvas-2021
23 The JustTech platform is an excellent resource: just-tech.ssrc.org/. Season 3 of the podcast *How To Citizen* includes many highly relevant interviews on topics related to technology, democracy and privacy: www.howtocitizen.com/episodes
24 See e.g. Ruha Benjamin's Race After Technology: www.aaihs.org/race-after-technology/
25 FNIGC, 'The First Nations Principles of OCAP®' fnigc.ca/ocap-training/; Video, 'The Two Faces of Research: the Havasupai experience with Arizona State University.' youtu.be/zsAlp2Dua2o Webinar, 'Acknowledging the Land without Acknowleding the Peoples: Are Individualistic Data Policies and Designs Fuelling Digital Colonialism?' illustrates with the speaker's personal experience: vimeo.com/653038251 The 'Decolonizing Digital' blog series ends with practical tips for software developers: animikii.com/news/decolonizing-digital-our-data-is-our-right
26 See e.g. decolonize-dna.org/ and listen to www.ted.com/talks/krystal_tsosie_our_dna_is_not_our_identity and www.howtocitizen.com/episodes/23-and-not-me-with-krystal-tsosie
27 See, e.g. Safiy Noble's *Algorithms of Oppression* and Cathy O'Neil's *Weapons of Math Destruction*.
28 The Algorithmic Justice League, founded by Dr. Joy Buolamwini, who was featured in the film Coded Bias for her ground-breaking work exposing bias AI in facial recognition: www.ajl.org.
29 hiswai.com/protecting-indigenous-languages-using-automatic-speech-recognition-news-northeastern
30 www.stateofopendata.od4d.net/chapters/issues/indigenous-data.html
31 See also . animikii.com/news/decolonizing-digital-our-data-is-our-right d4bl.org/ nativebio.org/decolonize-dna/ www.indigenous-ai.net/position-paper hiswai.com/protecting-indigenous-languages-using-automatic-speech-recognition-news-northeastern nmhumanities.org/Podcast.
32 See edition.cnn.com/2020/12/04/tech/google-timnit-gebru-ai-ethics-leaves/.
33 Carissa Véliz addresses this in *Privacy is Power*.
34 See Heather McGhee's *The Sum of Us*, which posits that addressing systemic racism and injustice will lead to more prosperous societies for everyone.
35 Many of the references cited earlier highlight this, however see this article regarding the trouble with individual consent:www.nature.com/articles/s41576-019-0161-z.epdf

Italy fines Clearview AI €20 million

In addition to the €20 million fine, Italy's Data Protection Authority, the *Garante*, has also ordered the company to delete data relating to people who are in Italy, and prohibited further collection and processing through its facial recognition system.

The *Garante* says that Clearview AI has breached GDPR's principles – collecting data without adequate legal basis, and not properly informing individuals of data collection.

The DPA also asked Clearview AI to designate a representative in the territory of the European Union to act for the data controller based in the United States. €600,000 of the €20 million fine was due to the company's failure to appoint a representative in the European Union.

Clearview AI is said to have a database of over 10 billion images of people's faces from around the world, extracted from public web sources via web scraping (such as news sites, social media and online videos).

This 30-page 17,000+ word decision provides valuable insights into the *Garante's* case against Clearview and the company's defence arguments.

• *See (in Italian) www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751323*

Netherlands: Major privacy class action dismissed by court

Nicole Wolters Ruckert and **Tim Sweerts** of Allen & Overy discuss the €11 billion class action claim of a Dutch NGO against Oracle and Salesforce at the Court of Amsterdam.

In force since January 2020, a new Dutch class actions law (the WAMCA[1]) empowers foundations and associations to claim damages on behalf of injured parties on an opt-out basis. In its 2020 writ of summons, The Privacy Collective (TPC) foundation asserted that Oracle and Salesforce violated the privacy rights of approximately ten million Dutch Internet users and claimed damages on their behalf.

TPC alleged that Salesforce and Oracle unlawfully processed personal data of Dutch Internet users in violation of the General Data Protection Regulation (GDPR) and Article 11.7a of the Dutch Telecommunication Act (the "cookie rules"). TPC argued that defendants were not permitted, through their Data Management Platform service, to collect data through cookies, combine it with other additional information and then subsequently create individual profiles of users. The profiles were used to offer personalised online advertisements and were shared with ad tech providers in a process known as Real Time Bidding (RTB).

'Support with one click'

To prevent frivolous claims, the WAMCA sets out admissibility requirements for organisations bringing class action procedures, including a requirement that the claimant represents a sufficiently large proportion of the injured parties (often referred to as a "representativeness requirement").

To substantiate the representativeness requirement, TPC asserted that over 75,000 individuals had clicked on a "support" button on its website dedicated to this class action. In this case, that proved insufficient. The Court found that 75,000 clicks on a general "support" button that did not provide details on the legal proceedings, the names of the parties being sued or a description of the injured parties being represented, was not enough to substantiate that TPC had obtained support from a sufficient number of the Dutch Internet users. In addition, the court considered it relevant that TPC had not registered any contact details and was therefore not able to communicate with its alleged supporters (which made it impossible to meet requirements of transparency and governance for WAMCA based claims) and that it was unclear whether "likers" were injured parties[2].

In the eyes of the Court, these failings were not mitigated by support from other privacy rights organisations. To be representative, the Court argued, TPC's constituency should consist of injured parties and not of other organisations sympathetic to the relevant cause. Consequently, the Court declared the claim inadmissible; TPC failed to demonstrate that it represented the alleged injured parties and therefore did not have legal standing.[3] It is likely that these specific failings could be avoided by other NGOs if they register support differently.

GDPR damages in opt-out proceedings?

Article 80 of the GDPR provides that a data subject can mandate a representative that meets certain requirements[4] to lodge the GDPR complaint on his or her behalf. The parties debated whether this provision precludes a class action on an opt-out basis, because the nature of such proceedings is that this mandate is not given, but that the proceedings are nonetheless binding on the relevant class. The Court did not answer this fundamental question because the claim was rejected on formalities, but the Court did highlight the importance of this issue for future GDPR class actions. An additional question is how claimants will substantiate actual damages of the individuals they seek to represent.

Continuing proliferation of class actions

The 2020 overhaul of the Dutch class action system has resulted in a significant proliferation of claim vehicles and class action suits in the Netherlands. GDPR-related class actions are pending against, amongst others, Facebook and TikTok. Recently, None of Your Business (NOYB) set up shop in the Netherlands in a newly formed joint venture. The outcome of the Salesforce/Oracle case has not appeared to slow down this trend.

AUTHORS

Nicole Wolters Ruckert is a data protection lawyer, specialising in advising on online advertising privacy matters. She is a counsel at A&O Amsterdam and leads the data protection team. Tim Sweerts specialises in class actions, impact litigation and governance disputes. He is a senior associate in Allen & Overy's litigation department.
Emails:
Nicole.WoltersRuckert@AllenOvery.com
Tim.Sweerts@AllenOvery.com

REFERENCES

1 'Wet Afwikkeling Massaschade in Collectieve Actie' in full.
2 The decision is at https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:7647 (in Dutch)
3 District court of Amsterdam, 29 December 2021, ECLI:NL:RBAMS:2021:7647 (Salesforce/Oracle)
4 Under article 80 of the GDPR, the representative must be a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, have statutory objectives which are in the public interest, and be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data.

© 2022 PRIVACY LAWS & BUSINESS

US update: Key features of the Colorado Privacy Act

Colorado's data privacy statute bears similarities to other state privacy laws and European law, but also departs in some significant respects. By **Elizabeth Canter** & **Natalie Dugan** of Covington & Burling.

On 8 July 2021, Colorado Governor Jared Polis signed the Colorado Privacy Act (CPA) into law, making Colorado the third US state to pass a comprehensive data privacy statute. The CPA will take effect on 1 July 2023 on the heels of a flurry of legislative activity. Indeed, in relatively quick succession, California adopted comprehensive privacy legislation in the form of the California Consumer Privacy Act (CCPA) (adopted June 2018; effective January 2020); California strengthened the CCPA (see *PL&B International Report* December 2020, pp.13-17) through adoption of the California Privacy Rights Act (CPRA) (adopted November 2020; effective January 2023); and Virginia adopted the Virginia Consumer Data Protection Act (VCDPA) (adopted March 2021; effective January 2023).[1]

Colorado's CPA was adopted within months of Virginia's VCDPA and bears a number of similarities to the Virginia law. Like the VCDPA, the CPA borrows many of the principles found in the California frameworks, which we refer to collectively as the CPRA except where it makes sense to distinguish the CCPA. In addition, like the VCDPA, the CPA draws on provisions found in the General Data Protection Regulation ("GDPR"), adopted by the European Union in 2016.

The CPA's legislative declaration makes no explicit reference to the GDPR. It notes that other US states are enacting data privacy requirements to "exercise the leadership that is lacking at the national level," and, further, that "Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate."[2]

Finally, although the CPA borrows many of the privacy principles found in other laws, the Act also differs in significant ways. Among them, these differences include several references to business obligations with respect to personal data as "duties," as well as specific statutory requirements to recognize global opt-out controls. This article highlights key features of the GDPR and other state privacy laws that are reflected in the CPA, as well as some of these potentially material differences.

Scope

Both the CPA and the VCDPA borrow key terminology from the GDPR, including the concepts of "controllers" and "processors." Specifically, "controllers," are entities that alone or jointly with others determine the purpose and means of data processing, and "processors" are those entities which process data on behalf of a controller. As under the GDPR, Virginia and Colorado primarily impose obligations on controllers, but processors are required to adhere to the instructions of a controller and assist controllers in meeting their obligations. The CPRA, on the other hand, does not use a dichotomy of "controllers" and "processors," and instead distinguishes among "businesses," "service providers," and "contractors."

> Both Colorado's CPA and Virginia's VCDPA borrow key terminology from the GDPR, including the concepts of 'controllers' and 'processors'.

While the GDPR applies comprehensively across industries and sectors, Colorado's CPA retains and expands on exemptions found in California's CPRA for businesses that are regulated under a number of sector-specific privacy laws. However, like the VCDPA, the CPA departs from both the GDPR and CPRA to exempt personal data processed in a commercial or employment context. One area where the CPA has narrower exemptions than the CPRA – and, even the VCDPA – relates to non-profit entities. While California and Virginia exempt non-profit entities from their statutory requirements, the CPA does not.

Data subject access rights

Like the GDPR and other state privacy laws, the Colorado law affords state residents a number of data subject rights. Specifically, consumers have rights in at least some circumstances to:

- Confirm whether a controller is processing personal data concerning the consumer and to access the consumer's personal data;
- When exercising the access right described above, obtain the personal data in a portable and, to the extent technically feasible, readily useable format;
- Correct inaccuracies in the consumer's personal data; and
- Delete personal data concerning the consumer.

Like Virginia, the CPA departs from the California frameworks by affording consumers the right to appeal a controller's decision with respect to a denied request. Likewise, the CPA makes clear that certain qualifications to deletion rights afforded under the CPRA (such as for processing activities designed to prevent fraud and malicious activity) are exceptions to all of the data subject rights under the CPA. That said, Virginia and Colorado's deletion rights are broader than the CPRA, insofar as they cover personal

data collected not just from a consumer – but also data obtained about or concerning a consumer.

The GDPR affords additional data subject rights to individuals, including rights to (1) restrict data processing (e.g., where accuracy is contested or where the controller no longer needs personal data); and (2) object to certain data processing.

Opt-out and consent rights

Whereas the GDPR has other relevant rights and protections, the CPA – like California and Virginia – affords consumers rights to opt out of certain defined processing activities. First, the CPA includes a right for consumers to opt-out of the sale of their personal data to third parties. The CPA echoes elements of California's definition of "sale" that captures exchanges of personal data made for monetary or other valuable consideration. Virginia, on the other hand, limits its definition of "sale" to exchanges made for monetary consideration only.

Second, the CPA, like California and Virginia, provides consumers with certain opt-out rights relating to targeted advertising activities. The GDPR and member state implementations of the e-Privacy Directive also have provisions relevant to online advertising, but the CPA tracks more closely to the other US states.

Like Virginia, the CPA affords consumers the right to opt out of the processing of their personal data for "targeted advertising" – i.e. the display to a consumer of an advertisement that is selected based on personal data obtained or inferred over time from the consumer's activities across different online services.

This is somewhat distinct from a new right under the CPRA for consumers to opt out of the "sharing" of their personal data for "cross-context behavioral advertising," although both seem to reflect an interest in providing consumers choices with respect to online advertising activities. Like Virginia, Colorado provides businesses some flexibility in terms of permissible opt-out mechanisms. A notable provision of the CPA requires controllers, as of 1 July 2024, to honor user choices exercised through a universal opt-out mechanism that meets certain forthcoming technical specifications to be established by the Colorado Attorney General. The CPRA contemplates that businesses should have choices about whether to post a "Do Not Share My Personal Information" link or honor global opt-out signals.

Further, Colorado makes no distinction for advertising directed at minors, while California requires opt-in consent to target children under 16 with cross-context behavioral advertising.

Like the VCDPA, the CPA requires businesses to provide consumers the choice to opt out of the processing of their personal data for the purposes of "profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." This is similar to a GDPR right for consumers, in some circumstances, to opt out of decisions based solely on automated processing, when such decision has legal impact or significantly affects the given consumer. There may be some convergence on this issue in the US, as the CPRA contemplates forthcoming regulations which will address potential opt-out rights for automated decision-making (including profiling).

Like the GDPR, the CPA generally requires consent to process certain categories of sensitive personal data, such as race and sexual orientation. This also is the case under the VCDPA. In contrast, California affords consumers the right to limit the use and disclosure of their sensitive personal data – at least where such data is processed to infer a consumer's characteristics. In that way, Colorado and Virginia more closely follow the GDPR sensitive data framework.

Data retention and minimization

In Colorado, controllers' obligations are framed as "duties." These duties include:

- A duty of purpose specification – i.e. to specify the express purposes for which personal data collected and processed;
- A duty of data minimization – i.e. to limit collection of personal data to what is adequate, relevant, and limited to what is reasonably necessary in relation to the specified purposes for which the data are processed;
- A duty to avoid secondary use – i.e. not to process personal data for purposes that are not reasonably necessary or compatible with the specified purposes for which the personal data are processed without consent; and
- A duty of care – i.e. to take reasonable measures to secure personal data during both storage and use from unauthorized acquisition.[3]

These generally converge with principles under other state laws and the GDPR, even if those other jurisdictions do not use the same language around "duties." The "duty of care" language is used in other federal and state proposals, such as a New York proposal, but the "duty of care" language under the CPA is defined much more narrowly than in those proposals.

Contracting with suppliers and service providers

The CPA sets forth required contractual provisions for agreements between controllers and processors which largely track those set forth in the VCDPA and strongly echo similar terms found under Article 28 of the GDPR. For example, the CPA, the VCDPA, and Article 28 of the GDPR each require contracts between controllers and processors to set out (among other terms) (1) the subject matter of the contract; (2) the duration of the processing of personal data; (3) the nature and purpose of the processing; (4) the type of personal data involved; and (5) the categories of data subjects and the obligations and rights of the data controller. The CPRA has its own idiosyncratic language that it contemplates for contracts between businesses and service providers or businesses and contractors.

Likewise, the CPA does not expressly require any specific contract terms in so-called controller-to-controller agreements. In contrast, the CPRA has specific requirements for contracts between businesses and third parties to whom data is sold or shared for cross-context behavioral advertising.

Risk and Data Protection Assessments

Under the CPA, controllers must conduct and document data protection assessments for processing personal data for certain higher risk processing

 © 2022 PRIVACY LAWS & BUSINESS

activities. This is similar to the parallel provision under the VCDPA and may reflect some influence by the GDPR approach, as the GDPR similarly requires data controllers to carry out an assessment of the impact any processing may have on individuals, where such processing of personal data is likely to result in "high risk to the rights and freedoms" of those individuals.

In contrast, under the CPRA, this topic is to be addressed by forthcoming regulations.

Rulemaking

Finally, as in California, the CPA authorizes the state Attorney General to adopt rules pursuant to the Act which further govern privacy in the state.

AUTHORS

Elizabeth Canter is a Partner, and Natalie Dugan is an Associate at Covington & Burling US.
Emails: ecanter@cov.com
ndugan@cov.com

REFERENCES

1 While certain aspects of the CPRA (e.g., extensions of partial exemptions for employee and business-to-business data) went into effect earlier, the key substantive provisions are scheduled to become operative 1 January 2023. The California legislature also made some clarifying edits to the text of the CPRA in October of 2021. See AB-694 (Privacy and Consumer Protection: Omnibus Bill). Note that following California, Virginia, and Colorado, the Utah legislature recently passed its own comprehensive privacy law, on March 2nd, 2022, which generally tracks the VCDPA and the CPA. See SB-227 (Utah Consumer Privacy Act). Nevada also passed and has since amended narrower privacy legislation focused on opt out of sale rights for online services and data brokers. See SB-260 (Nevada Privacy of Information Collected on the Internet from Consumers Act).
2 CPA § 6-1-1302(b)(II) - (c)(I).
3 See CPA 6-1-1308 ("Duties of controllers").

US state Utah adopts privacy law

The Utah Consumer Privacy Act was signed into law on 24 March. Following California, Colorado and Virginia, this is further action at state level whilst a federal level law is not progressing.

The law applies to any controller or processor who:

- Conducts business in the state of Utah or produces products or services targeted toward consumers who are residents of the state;
- Has an annual revenue of $25 million or more;
- Satisfies one or more of the following thresholds:
  (i) during a calendar year, controls or processes personal data of 100,000 or more consumers; or
  (ii) derives over 50% of the entity's gross revenue from the sale of personal data and controls or processes personal data of 25,000 or more consumers.

The Act enters into force 31 December 2023.

- *See le.utah.gov/~2022/bills/static/SB0227.html*

Human error accounts for 41% of reported data breaches in Australia

After four years of operating a data breach notification system, the Office of the Australian Information Commissioner (OIAC) reports that malicious or criminal attacks were the main source of data breaches (55%). This was followed by human error which accounted for 41% of notified breaches.

The authority's latest Notifiable Data Breaches Report shows the OAIC received 464 data breach notifications from July to December 2021, an increase of 6% compared with the previous period. Most reports were received from the health sector, followed by finance.

Australia's Information and Privacy Commissioner, Angelene Falk, said the Notifiable Data Breaches scheme is well established after four years of operation and the OAIC expects organisations to have strong accountability measures in place to prevent and manage data breaches in line with legal requirements and community expectations.

"The scheme is now mature and we expect organisations to have accountability measures in place to ensure full compliance with its requirements," she said.

"If organisations wish to build trust with customers, then it is essential they use best practice to minimise data breaches and, when they do occur, they put individuals at the centre of their response."

The OAIC is still finding that some organisations are falling short of the scheme's assessment and notification requirements.

- *See www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021*

Using MPC technology to enhance privacy in data sharing

The encryption-based Multi-Party Computation (MPC) technology enables data collaboration without the parties actually sharing the personal data. By **Laura Linkomies**.

A user case from the Netherlands under the aegis of the Data Sharing Coalition brings positive news for those grappling with data sharing challenges. Private, public and the civil sector actors collaborated in a project that was based on cross-domain data sharing for the purpose of preventing and monitoring human trafficking. In this case, information obtained by law enforcement agencies of victims of forced prostitution was processed together with information from victims obtained by NGOs. The Sustainable Rescue Foundation (an NGO), Roseman Labs and others worked with privacy experts at Pinsent Masons to develop a system based on MPC (Multi-Party Computation) technology to help overcome the privacy law challenges so that sensitive data could be processed in confidence.

The main challenge in this use case was to enable collaboration between the parties without having to share sensitive personal data. The law enforcement agency has a list of names of individuals who are potentially engaged in criminal activities. A small number of people are put under observation. The NGO's also hold a list of names – that is those of the informants - and wants to ensure that none of the informants is put under observation by the law enforcement agency. How can the parties achieve this, if they are unwilling (or, not allowed) to share these lists with each other? An additional complexity is that not all names are spelled correctly.

MPC is based on four decades of academic research in theoretical cryptography. It enables several participants to perform a computation on their joint input data, while their inputs remain mutually private (the input from each participant remains secret to all other participants), and without involving a trusted third party.

"In theory, MPC technology has been available for quite some time," Andre Walter, Head of Data Law Solutions at Pinsent Masons Netherlands said. "It is not just about encrypting data but about the ability to process encrypted data without lifting the encryption at any moment in time".

In this user case, Roseman Labs, a high-tech software company that enables organisations to collaborate on privacy sensitive data through MPC, ran the process on encrypted data in real time. The process mitigates the risks because no personal data is exposed. Only the end result, in this case a short list for the law enforcement agency is revealed to the agency.

Ian Wachters, Commercial Officer at Roseman Labs, explained that each bit of data is divided into separate signifiers (numbers) which will reconstruct the information only if put together. The data is held on three separate servers and no one has access to these three servers in parallel.

> The main challenge in this use case was to enable collaboration between the parties without having to share sensitive personal data.

"MPC is the most powerful privacy enhancing technology that is available," Wachters said. "The technology is now at a tipping point of being practical because of recent mathematical innovations and faster computers and networks. It can therefore now be applied to everyday problems."

But given that the technology is not something you come across every day, how were the NGOs convinced that their users' data would be safe?

"We explained the process thoroughly. Then Roseman Labs assisted the organisations in running an 'MPC ceremony': three laptops, located at three different cities in the Netherlands, ran Roseman Labs' MPC protocol over the Internet, " Walter said.

Each laptop was provided with a list of the individuals' data the organisation had in that city. A Roseman Labs person assisted the organisation during execution of the protocol.

"User trust is paramount and it is very important that all concerned are kept informed," Walter said.

MPC and GDPR-compliance

"Although under a strict interpretation of GDPR the encrypted data is still not considered anonymous, MPC provides a tremendous help in complying with GDPR principles such as purpose limitation and data minimisation" Walter said.

The outcome of an MPC ceremony is defined beforehand, and that way the algorithm, and with it the processing of the data, is run to achieve only the envisioned purpose.

In terms of data minimization, all data provided by the participating parties is encrypted at the source and hence not visible to anybody else during the process. Only the end result is revealed, and only to the designated party. MPC therefore enables collaboration where parties would not previously have trusted each other.

"MPC does not try to avoid the GDPR but can be used to enhance compliance. We take the same strict view as the Netherlands' DPA – encrypted data is not anonymous data as it can be reconstructed. Therefore, the GDPR still applies," Wachters said. MPC technology makes possible processes that previously were not because the parties would not trust each other. Now when using MPC technology, they do.

 © 2022 PRIVACY LAWS & BUSINESS

EDPB promotes this type of technology

EU DPAs acknowledge that technical measures may supplement other safeguards for data transfers to third countries, and they say that new technologies may still emerge.

The European Data Protection Board said in its 21 June 2021 guidance on international transfers that as a supplementary measure to a data transfer, split or multi-party processing is acceptable. Its use case (number 5 in annex 2) proposes the following scenario:

"The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data."

Multi-party computation can be used as a technical supplementary measure if there is no evidence of collaboration between the public authorities located in the respective jurisdictions, the DPAs say.

Going forward – an eye on international transfers

MPC solutions are ready to be used commercially. In fact, big players such as Coinbase and PayPal are already deploying MPC where they need extra security and privacy for cryptographic key management.

Rosie Nance, Practice Development Lawyer at Pinsent Masons said she is very excited about the technology's potential to overcome challenges around *Schrems II*, data localisation laws, and other restrictions around sharing certain types of data.

"The solution could enable collaboration and data sharing that would otherwise not be possible due to strict data localisation laws, *Schrems II*, local restrictions around data used for purposes like law enforcement, or a combination of all three of these factors. As lawyers based in the EU or UK, shifting processing to the EU or UK might seem like a solution to the challenges that arise on projects requiring international data sharing – and that would generally address *Schrems II* concerns. However, global organisations face complex and sometimes conflicting compliance requirements, and that would only deal with one piece of the puzzle."

Nance foresees potential for further application of the technology in the financial sector, particularly in fraud prevention. Wachters agrees: "Anti-money laundering is a good example. If a bank only monitors their own transactions, it may not get a clear picture of what is happening. With the help of MPC, it can work with other collaborators to flag those that fulfil fraudulent criteria. Those transactions will then be looked at but only within that organization – so data is not shared with third parties."

Similarly, MPC technology could aid insurance companies to share their loss data in a privacy friendly way in order to better understand risk profiles, Wachters said. Other potential uses could be found in marketing. For example, two retailers with different product categories but both running loyalty schemes could understand their consumers' behaviour better as micro-segments can be created without actually sharing personal data.

MPC can also be used in the health sector and Wachters says this is very much a focus of Roseman Labs. The technology becomes useful when different health providers need to collaborate but data cannot be shared due to compliance reasons. For example, several hospitals can collaborate in a clinical study without revealing patient records to each other, and only reveal the conclusions of the study. Another question is how this technology could be explained to patients in a health system context, as the use of MPC would most likely require their informed consent.

Other possible uses could be in genetic testing to let people check their own genetic profile, or keeping bids private in sealed-bid auctions.

Roseman Labs stresses that MPC provides both the strongest technical and organisation safeguards as required under the GDPR.

However, MPC will not solve every compliance challenge around sharing personal data: "MPC is not a silver bullet but it provides some legal certainty for data used for these types of data collaborations," Walter said. "Now that the EU Data Governance Act is about to be adopted, there will be increased pressures for data sharing and this needs to take place in a secure environment."

INFORMATION

rosemanlabs.com/assets/video/explainer_video_mpc.mp4
www.qredo.com/blog/what-is-multi-party-computation-mpc
www.fireblocks.com/what-is-mpc/
datasharingcoalition.eu/app/uploads/2021/04/data-sharing-canvas-30-04-2021.pdf

DATA SHARING COALITION

The Data Sharing Coalition, an international project operating in the Netherlands, encourages new members to join. Participants are expected to contribute to the work by

- Contributing to the definition and realisation of cross-sectoral use cases of data sharing
- Providing input and expertise to determine the harmonisation potential between data sharing initiatives (Data Sharing Canvas)
- Driving knowledge sharing about (cross-sectoral) data sharing.

The initiative started in January 2020, after the Netherlands' Ministry of Economic Affairs and Climate Policy invited the market to seek cooperation in pursuit of cross-sectoral data sharing. The Data Sharing Coalition, supported by the Ministry, was started as a direct result.

See datasharingcoalition.eu/joining-the-data-sharing-coalition/

GDPR hearing: Enforcement, One-Stop-Shop need improving

The European Parliament heard from DPAs and other guest speakers on whether they regard the GDPR a success four years after implementation. By **Laura Linkomies**.

In the hearing chaired by Civil Liberties Committee Chair, *Juan Fernando López Aguilar*, on 17 March, MEPs heard presentations on data subjects' rights, enforcement and significant cross-border cases.

Ursula Pachl, Deputy Director General, European Consumer Organisation BEUC, said that in her view, we have mixed results with the GDPR. While the Regulation is at the forefront of businesses minds and can be seen as a global standard, individuals still often face incomprehensible privacy policies. Also problematic is illegal online tracking and profiling. Enforcement of the surveillance economy has been particularly disappointing, she said.

Transparency is not sufficient for individuals. When making a Data Subject Access Request (DSAR), people do not always receive a response in time, or it is not comprehensive. The right to data portability is not often used as it is not practical. Consent is still a big problem – there is sometimes difficulty in withdrawing consent.

"The issue of resources has not been sufficiently dealt with. Some DPAs lack resources but sometimes it is also about the mindset of the authorities. The DPAs need to assist individuals much more in the complaints process. Harmonised templates would help in this respect. There should also be legal aid available," Pachl said.

Mikko Niva, Global Privacy Officer at Vodafone made remarks on the need to review the GDPR and its relationship with other proposed legislation at EU level. In his view, we do not want to create a very diverse body of law to regulate the same issues in different laws. "But there are problems that need to be solved, so we need to aim for a holistic, understandable piece of law. For example AI is not just about personal data, so the GDPR is therefore not the right instrument to regulate it fully, but also the AI Act should not be in conflict with the GDPR."

"The GDPR is there to protect people. Companies need to invest heavily in getting it right. We have 100 plus people working in privacy and are taking it very seriously."

Niva said that contrary to some views, authentication is necessary when verifying who is making a DSAR. At Vodafone, they see many cases where people pretend to be someone else in order to gain access, often in relation to jealousy issues in relationships. He said that Vodafone therefore needs to perform checks.

"It is about protecting the people. Data of one person also tells a lot about other people. It is a relationship matter. We need to balance the rights and freedoms but what is the standard? We have a methodology at Vodafone, but it is an ethical analysis which is not straightforward. We need to understand the harms involved better," Niva said.

Sophie Genvresse, Deputy to the Head of the Service for the Exercise of Rights and Complaints in the Directorate for the Protection of Rights and Sanctions, at France's DPA, the CNIL, thought that there is no need to revise the GDPR. It is a high-level regulation, and we have to acknowledge that 2018 was quite recent, she said.

We can now see the effect of the pandemic but different authorities have made many investments to build a coherent framework. Some time is needed to achieve a comprehensive approach.

Focus on enforcement schemes

Mar España Martí, Director, Spanish Data Protection Authority (AEPD). said that the GDPR has not solved the problem of harmonisation completely. There are still different national implementations across the EU and this makes it difficult to process complaints. But all DPAs have worked hard to make the One-Stop-Shop work, she said.

In Spain, there are some 320 cross border cases. The One-Stop-Shop is a new way of working and there are still many issues to solve. Lack of harmonisation can be seen regarding transparency. In Spain, the DPA shares data willingly during the process, but some other countries cannot be as transparent and can only share data when the investigation has been completed. So there is lack of coordination, she said. Interpreting timelines under national legislations can also cause issues.

"The One-Stop-Shop works pretty well, and most DPAs are doing what they can, but much remains to be done."

Martí referred to the large online companies that have generated many complaints. The complexity of these cases is increasing, she said.

Tobias Judin, Head of the International Section, Norway's Data Protection Authority (Datatilsynet) said that data protection has come a long way since the GDPR which in itself has been a learning process. "More and more enforcement is being carried out. However, we have enforcement challenges and these need to be discussed candidly."

"In Norway, we try to focus our efforts on the big impactful cases. But we struggle with resources. Lack of resources also manifests itself in the One-Stop-Shop. Even if just one DPA lacks resources it can have an impact for the rest of the countries."

He said that as Norway's DPA is not competent to enforce the e-privacy rules on its own, but needs to cooperate with two or three other Norwegian authorities, the new e-privacy rules will further complicate the situation.

He stressed that national enforcement is impacted by the EU One-Stop-Shop. "While the One-Stop-Shop now works very well in most cases, it may not always work well in cases where all DPAs are concerned. The Lead Authorities are mostly from the same jurisdictions. This means that the enforcement burden is very unevenly shared."

 © 2022 PRIVACY LAWS & BUSINESS

So much depends on how smoothly and timely the Lead Authority resolves the cases.

"For cross border cases that involve two-thirds of all DPAs, maybe another enforcement model would be better to share the burden more evenly," Judin said.

He thought that there could also be some modifications to make the EDPB's role more active.

Gwendal le Grand, Head of activity for enforcement support and coordination at the European Data Protection Board (EDPB), described how the Secretariat's workload has increased with very strict deadlines.

He said that enforcement is ramping up at the national level. There is more cooperation work – almost 2,000 cross border cases now and 362 final decisions.

"The secretariat must draft documents to support national DPAs in their decision-making process. Urgent binding decisions need to be issued within two weeks so there are tight deadlines. At the same time, the EDPB must produce guidance and joint opinions, statements etc. The result is that the secretariat has had a massive increase in its workload in 2022."

Le Grand said that the regulators have shifted to enforcement in a fragmented way as there are insufficient human resources. In February, the EDPB launched its first coordinated enforcement action on the use of cloud in the public sector (see *PL&B* News 15 February, www.privacylaws.com/news/eu-dpas-start-coordinated-enforcement-action-on-cloud-in-the-public-sector). The results will be analysed in a coordinated manner, and a report is expected at the end of the year.

The DPAs are looking for new ways to coordinate their efforts. A support pool of experts is being drawn up to facilitate the analysis of cases that have strategic importance. A call for external experts was published in February. The group will share information on national case law etc. The aim is to achieve a common enforcement culture. The EDPB will publish guidance on fines shortly.

Gloria González Fuster, Research Professor at Vrije Universiteit Brussel (VUB) and Co-Director of the Law, Science, Technology & Society (LSTS) Research Group, highlighted the difficulties individuals have with enforcing GDPR Article 78 - the right to a judicial remedy against a supervisory authority.

"Thousands of data subjects are in limbo as they do not know whether a DPA is going to handle their complaints."

Sweden's DPA acknowledges every case as a complaint but also interprets them as a 'tip' about issues with organisations' compliance.

"Sometimes complaints are just ignored. So either there is an investigation or a live procedure which is not consistent."

González Fuster said that other DPAs, for example in Poland, say that 'if everyone is happy there is no need to proceed and they can close the case'. In Ireland it is even worse she said.

"We need clarity. This is about harmonisation of practices. The DPAs have a transparency register where we can read decisions but there are irregularities," she said.

Judin from Norway's DPA said in a response to Q and A: "It is difficult to prioritise cases. We are mindful that we have to handle all complaints under the GDPR. But many complaints are due to misunderstandings and it takes a lot of resource to clarify. The time could be used on cases with wider implications."

España Martí of EAPD Spain explained that the Spanish DPA also deals with all complaints as required by the GDPR.

Big cases and cross-border challenges

Maximilian Schrems, Honorary Chairman, European Center for Digital Rights (NOYB) said that there are still many procedural issues in cross-border cases. There are differences between the availability and responsiveness of the DPAs.

When it comes to the One-Stop-Shop, Schrems said that some DPAs withhold information. Some DPAs are much more transparent about the process than others.

Maria Magierska, PhD Researcher, European University Institute, talked about the importance of cross-border cases as an example of how the GDPR framework works. There are still some issues with collaboration, she said. If some DPAs are not willing to cooperate, this leads to very long delays as the GDPR does not specify a deadline for draft decisions. She said it would be useful to introduce some deadlines.

Olivier Micol, Head of Unit, DG JUST at the European Commission, spoke about the One-Stop-Shop. According to him it works well and further improvements have been made, for example the EDPB's guidelines for cross-border collaboration. DPAs have challenges at the national level be it lack of resources or dealing with Big Tech with endless resources and willingness to pursue cases in court.

INFORMATION

A recording of the event is available at multimedia.europarl.europa.eu/en/webstreaming/committee-on-civil-liberties-justice-and-home-affairs_20220317-0900-COMMITTEE-LIBE

Greece's DPA issues €9.25 million fine

Greece's Data Protection Authority issued its largest fine to date on 31 January against Cosmote and telecommunications company, OTE, for multiple violations of the GDPR. The fines stem from a 2020 data breach that affected more than 10 million subscribers and included large sets of personal data.

OTE Group belongs to Deutsche Telekom, and is the largest telecommunications conglomerate in Greece.

"The leaked databases were processed by Cosmote for network fault management and general data analytic purposes," Antonios Broumas, Digital Law Manager at EY Law Greece writes.

The Authority imposed a fine of €6,000,000 on Cosmote, as well as a sanction of interruption of data processing and destruction; and imposed a fine on OTE of €3,250,000 .

- *See www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-gia-peristatiko-parabiasis-prosopikon-dedomenon-kai-mi-nomimi*

Enforcement by European DPAs against data transfers

What can organisations do if they have relied on Google Analytics to measure the effectiveness of their website? **Katharina A. Weimer** of Fieldfisher Germany explores the issues.

In the immediate aftermath of the ECJ ruling *Schrems II* (C311/18), there was a stunned silence, while companies and data protection authorities alike grappled with the consequences. The data protection authorities started issuing guidelines and opinions, making it quite clear that there was no grace period for making the necessary changes and that it was their obligation to enforce the ruling, with all its consequences. And of those there are many. Most notably, any transfer (including making available) of personal data from the EU/EEA to a recipient outside of the EU/EEA now entailed a whole host of new assessments and documentation, without the help of the Privacy Shield for transfers to the US. It seemed that all of a sudden, the question of "adequate level of safety" for the data transferred was now to be taken seriously, even for transfers to the US.

What this means in practice is that for all transfers, the data exporter must assess (i) its data transfers, (ii) the transfer mechanism relied upon (i.e. standard contractual clauses, binding corporate rules, individual consent, or other), (iii) effectiveness of the transfer mechanism (by assessing inter alia the laws and practices in the recipient country), and (iv) the supplementary measures necessary, if any, to ensure the adequate level of safety for the personal data which is to be transferred (organizational, contractual and technical measures).

Without recapping all the details of the legal landscape in the US which was subject to the *Schrems II* ruling, and going into the fineprint of the US Clarifying Lawful Overseas Use of Data (CLOUD) Act, the implications of these legislative acts seem clear:

They generally allow for access to (or request for) personal data of EU citizens in the control of (certain types of) US companies and/or their subsidiaries outside of the US, by certain US governmental and/or national security bodies and agencies, subject to certain conditions. Such access cannot be barred by the companies which are subject to these laws, although there are legal remedies against this access/request. It can also not be excluded by contract, due to the very nature of national administrative laws granting powers to governmental or national security agencies.

In essence this means that transfer of personal data to the US seems possible only with comprehensive technological safeguards which render a deciphering of the personal data by unauthorized recipients in the US (and elsewhere) impossible.

In recent months, there have been several decisions by courts and data protection authorities relating to such transfer to recipients outside the EU/EEA, all of them relating to the US. What seems important is the level of detail in which the transfers have been investigated, and the arguably negligible amount and type of data that was transferred. While it had seemed clear to most companies transferring data to recipients outside the EU/EEA that they would have to investigate their main business activities, the material data transfers and in particular assess any transfers of sensitive data, this regulatory and judicial review goes far beyond any such initial review. It aims at the fundamental principles of the functionalities of the Internet and global communication as we currently use it, and requires meaningful changes that will come at a price.

Hochschule RheinMain

In a preliminary injunction administrative proceeding before the administrative court in Wiesbaden (Hessen), an individual required the Hochschule RheinMain, a public educational institution (Hochschule), to refrain from using the service "Cookiebot" for the purposes of obtaining consent to cookies if that includes the transfer of personal or personally identifiable data (including IP address) to servers operated by US group Akamai Technologies Inc.

The Hochschule uses a Cookiebot for its cookie consent management tool. The Cookiebot collects the IP address (although it was in dispute as to whether it was anonymized with the last three digits set to "0", or not), date and time of consent, user agent of the browser, URL, an anonymous, random and encrypted key, and the consent status of the data subject. For its services, it uses the content delivery network of Akamai Technologies, Inc. (Akamai) for requesting the consent script which is hosted on Akamai's servers. According to the data processing agreement provided by Akamai, the time stamps of the visited websites and the respective IP addresses, as well as the geographical location based on the IP address and telemetric data are also collected.

The administrative court of Wiesbaden held that this constitutes a transfer which is without legal basis and therefore not permissible, as none of the legal bases of Art. 48/49 GDPR are applicable. The user has not consented to the transfer, a legitimate interest cannot be determined, and there is no indication for any other justification. The court went into great detail to determine how the collected data can be combined to identify the user, with the help of the IP address – even if the name of the user is not known, the individual can be identified.

The fact that the contractual partner of the Cookiebot operator Cybot A/S is the German Akamai Technologies GmbH, was of no relevance because the server structure of the parent company Akamai Technologies Inc. was being used for the Content Delivery Network services. The existence of model clauses between Cybot A/S and Akamai was also not discussed.

 © 2022 PRIVACY LAWS & BUSINESS

The decision was upturned upon appeal but only because the Higher Administrative Court held that there were no grounds for a decision in preliminary proceedings due to lack of urgency. In the Higher Administrative Court's opinion, the complexity of the case, as well as its importance, do not permit a decision in preliminary proceedings, and have to be assessed in proceedings on their merits. This case on the merits is currently pending with the Administrative Court of Wiesbaden.

The takeaway from this proceeding is that users and courts are now prepared to take a deep-dive into the details of functionalities that are being used, and that companies have to be prepared to respond to this method in a granularity previously unseen. This extends to seemingly irrelevant / unimportant data such as (anonymized) IP addresses, URLs, time stamps, and other machine information, as the combination of these can lead to creating profiles of individual users. Transfers of such personal data to recipients outside the EU/EEA require a valid justification (e.g. consent).

Google Analytics

The last couple of months have also seen several decisions by Data Protection Authorities (DPAs) involving Google Analytics. Some of these decisions result from investigations following complaints launched by NOYB, the organisation founded by Max Schrems. NOYB had submitted roughly 100 formal complaints with all European data protection authorities regarding the use of cookies (including Google Analytics) on websites. It is important to note that the European DPAs have orchestrated their responses / decisions on these complaints.

a) Austria's DPA: In December 2021, the Austrian DPA decided on a complaint by NOYB against a website operator who had implemented the cost-free version of Google Analytics. The Austrian DPA determined that the combination of information collected by Google Analytics (such as browser type, operating system, host name, referrer and language, screen resolution, and others) with the Unique User Identification (UUI) numbers (which uniquely identify the browser and the device, respectively, of the user) placed by Google Analytics cookies, and the IP address, together with, in this specific case, the information on the Google Account user (because the individual complainant was logged into his/her Google Account at the time of surfing) constitutes personal data of the individual who is surfing and whose browsing behaviour is tracked. It is not necessary, in the view of the Austrian DPA, that a specific "face" of an individual, meaning in particular his/her name, is identifiable, with reference to the possibility of "singling out" an individual set forth in recital 26 of GDPR. In addition, a digital footprint is commonly deemed sufficient for uniquely identifying a device, and thereby a concrete user, and thus constitutes personal data. The circumstance that another person (in this case, Google in the US because of the log-in into the Google Account, and possibly US surveillance agencies) had access to further information which may lead to the identification of the individual was a supporting factor in the determination of the individual being identifiable, and thus the data being personal data.

Because the website operator transferred personal data to the recipient outside of the EU by using Google Analytics, it had to comply with the requirements set out by Art. 45, 46, and 49 of the GDPR. While the parties had agreed on standard contractual clauses as a transfer mechanism, it is clear since the *Schrems II* judgment that adopting standard contractual clauses alone cannot provide an adequate level of data protection. Following this judgement, Google has implemented supplementary measures to provide for additional protection and thereby, in its view, afford European personal data the level of protection required by the GDPR.

The Austrian DPA though, in its examination of the supplementary measures, questioned whether the contractual and organisational measures (such as information to the data subject in case of a request and publication of a transparency report) supported by Google are even effective in ensuring additional protection. The same applies, in the DPA's view, to the technical measures – encryption and protection in transit and "on-site security".

The relevant take-aways of the Austrian DPA's decision in summary:

- Information collected and transferred by Google Analytics constitutes personal data;
- A digital footprint is sufficient to count as personal data;
- The supplementary measures implemented by Google to protect the data transferred through Google Analytics are not effective measures.

b) France's DPA: France's DPA, the CNIL issued a press release according to which it has received complaints by NOYB regarding the data collected by Google Analytics and investigated the conditions of this service. It also comes to the conclusion, in line with the decision by the Austrian data protection authority, that such transfers are illegal. Consequently, it ordered a French website manager to comply with the GDPR (within one month) and, if necessary, discontinue using this service.

In substance, the CNIL makes the same determinations as the Austrian data protection authority and adds the noteworthy point of using Recital 30 GDPR as additional support for the analysis that online identifiers (such as IP address and cookie information) can commonly be used to identify an individual.

As the CNIL also finds that the data transferred constitutes personal data, it reviews the transfer mechanism, standard contractual clauses, which needs to be supplemented by the supplementary contractual, organisation and technical measures. It highlights the general issue with contractual measures that they can of course not bind the authorities of a third country and therefore require combining them with technical and organisational measures. However, the same applies to organisational measures which, in itself, are again not sufficient to ensure meeting the "essential equivalence" standard required by EU law. It comes down to adopting appropriate technical measures so that potentially infringing access by foreign authorities cannot identify the data subjects.

The CNIL also investigates the measures implemented by Google and

comes to the same conclusion as the Austrian data protection authority that neither the contractual and organisational, nor the technical measures implemented by Google factually prevent or reduce access.

c) Norway's DPA: Norway's DPA announced on 28 January this year an audit of Telenor ASA and confirmed that it was investigating a complaint regarding Telenor's use of Google Analytics.[1]

Information on a case before Norway's DPA, *Datatilsynet* references both the Austrian data protection authority's case as well as the CNIL's decision. In its press release it refers to the decision of Austria's and France's DPAs on the use of Google Analytics.[2]

d) EDPS: Similarly, the European Data Protection Supervisor (EDPS) issued a decision against the European Parliament in which it found that the European Parliament violated data protection laws ("GDPR for EU institutions", 2018/1725) in using Google Analytics, among others. This decision also followed a complaint by NOYB in January 2021 and confirmed that an internal Corona testing website transferred personal data to the US without ensuring contractual, technical or organisational measures to ensure essential equivalence of the level of protection.

What is next?

It seems clear that other European DPAs will follow suit regarding the NOYB complaints pending with them, and issue orders of compliance and/or cessation. Website operators are currently in limbo: often their entire analytical framework for website traffic is based on Google Analytics, and they have made considerable investments into this structure, leaving them reluctant to investigate alternatives which may not provide the level of insight Google Analytics can provide. However, it is currently not possible for them to use Google Analytics in a GDPR-compliant manner – or is there a way?

While there is no official "way forward" from Google yet, the use of server-side tagging[3] may bring some light to the end of the tunnel. Google claims that the server container for the tags and the data runs in the website operator's own platform or environment, and it has complete control over which data is sent and to where. Without having investigated the technical details, it seems to present a potential solution if the website operator is willing to invest the time to adopt and configure this solution carefully.

However, it can also be expected that Google will react to this concentrated effort at a more general level to address these fundamental concerns.

Conclusion

With the ever-increasing use of the Internet by individuals, and the information about individuals' preferences, likes, and activities that can be deducted through such individuals' use even by only collecting mere technical information (the digital footprint), Internet users become increasingly transparent for website operators. In fact, they have been for a long time and companies have capitalized on this knowledge for years – and have gotten away with it because the information was "only technical information".

However, it is now abundantly clear that such technical information is the gateway to the digital individual, and data controllers have to concern themselves with all the details of the technical information they collect and ensure compliance with GDPR (and of course other legislation).

AUTHOR

Katharina A Weimer is a Partner at Fieldfisher Germany.
Email:
Katharina.Weimer@fieldfisher.com

REFERENCES

1 www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/tilsyn-med-telenor/
2 See (in Norweigan) www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/google-analytics-kan-vare-ulovlig/
3 See developers.google.com/tag-platform/tag-manager/server-side/intro

Ireland fines Meta €17 million for 2018 data breaches

In a cross-border case that was initiated in 2018, Ireland's Data Protection Commission announced on 15 March that it is fining Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) €17 million for breaches of GDPR Articles 5(2) – accountability regarding data protection principles - and 24(1) – implementing appropriate technical and organisational measures.

The DPC found "Meta Platforms failed to have in place appropriate technical and organisational measures which would enable it to readily demonstrate the security measures that it implemented *in practice* to protect EU users' data, in the context of the twelve personal data breaches."

"The DPC's decision was subject to the co-decision-making process outlined in Article 60 GDPR, and all of the other European supervisory authorities were engaged as co-decision-makers. While objections to the DPC's draft decision were raised by two of the European supervisory authorities, consensus was achieved through further engagement between the DPC and the supervisory authorities concerned," Ireland's DPA says in a statement.

It has not been announced whether the fine was increased or decreased as a result of the objections, or which DPAs objected.

- *See www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry*

 © 2022 PRIVACY LAWS & BUSINESS

China's Draft Regulations on push notifications apply to apps and websites

Gabriela Kennedy and **Joshua T. K. Woo** of Mayer Brown in Hong Kong report on the important aspects of these draft regulations which affect all companies with websites accessible in China. The devil is in the detail.

On 2 March 2022, the Cyberspace Administration of China ("CAC") issued draft regulations on the administration of internet pop-up push notifications (the "Draft Regulations"). The Draft Regulations were issued pursuant to a number of laws, including the Cybersecurity Law.

The Draft Regulations bid to further tighten government control over the news followed a human trafficking controversy that erupted on Chinese social media after a woman was found chained by the neck in Xuzhou last month, and the invasion of Ukraine.

However, the regulations also address other aspects of push notifications – including prohibition of algorithmic models that profile minor users and encourage user addiction. This is in keeping with the Chinese government's broader efforts to reduce the influence of Big Tech, and aligns with the recently issued Internet Information Service Algorithmic Recommendation Management Provisions that came into force on 1 March 2022.

The Draft Regulations

(a) Scope of Application

The Draft Regulations apply to all owners and operators of operating systems, terminal devices, application software, websites and other such services (Service Providers) that provide push notification services (Push Notification Service Providers) in China.

(b) Types of Prohibited Information

Various categories of prohibited information in push notifications include:

1. illegal and negative information as defined in the Provisions on Ecological Governance of Network Information Content (the Provisions) that includes content that[1]:

1. opposes the basic principles established by the constitution;
2. endangers national security, divulges state secrets, subverts state power, or undermines national unity;
3. harms national honour and interests;
4. distorts, defames, desecrates or negates the deeds and spirit of heroes and martyrs, or infringes upon the names, likenesses, reputations, or honors of heroes and martyrs by insulting, slandering, or otherwise;
5. advocates terrorism or extremism or incites the commission of terrorist or extremist activities;
6. incites ethnic hatred or ethnic discrimination, undermining ethnic unity;
7. undermines the state's religious policy and advocating cults and feudal superstitions;
8. spreads rumors and disrupts economic and social order;
9. spreads obscenity, pornography, gambling, violence, murder, terror, or instigating crimes;
10. insults or slanders others, infringes upon the reputation, privacy, and other lawful rights and interests of others;
11. uses exaggerated headlines, where the content is seriously inconsistent with the title;
12. hypes up scandals, bad deeds, and so forth;
13. improperly comments on natural disasters, major accidents, or other disasters;
14. with sexual innuendo, sexual provocation, or other such elements that are likely to cause people to have sexual associations;
15. displays bloody, frightening, cruel, or other such acts that cause people physical or mental discomfort;
16. incites crowd discrimination, regional discrimination, and so forth;
17. promotes vulgar or kitsch content;
18. that might cause minors to imitate unsafe conduct, conduct that violates social morality, induce minors to have bad habits, and so forth;
19. other content that has a negative impact on the network ecology; or
20. other content prohibited by laws or administrative regulations;

2: information that violates public order and good customs, such as malicious speculation, entertainment gossip, extravagance and ostentation of wealth, and distasteful information[2];

3: information that maliciously stirs up old news[3];

4: content that hypes up sensitive events, exaggerates vicious content and disasters, and incites social panic[4].

Push notifications containing news reports are required to adhere to additional rules, including a requirement for the source of news to come from the list of 1,358 government-approved news sources published by the CAC in October 2021[5].

This means that news reports from unlicensed sources such as private institutions and individuals cannot be included in push notifications.

Accordingly, Push Notification Service Providers need to ensure that push notifications of news reports do not alter the original meaning and content of sanctioned headlines and are traceable to the original source. They are also required to obtain approval from the relevant source before publishing news content in push notifications[6].

Collectively, these prohibitions are

very broad and enhance the risks of breaching the law when pushing prohibited news-related notifications – or information that may be construed to fall within the above categories.

(c) Responsibilities of Push Notification Service Providers

Push Notification Service Providers will be required to put additional processes in place in order to comply with the Draft Regulations.

One such requirement is for them to set up a manual review system[7] for the review of screening, editing, pushing of content and other related work processes. Together with the content prohibitions highlighted in (b), they have to review the guidelines, policies and processes that they have in place when vetting pushed content.

Push Notification Service Providers are also expected to prioritise user protection and to:

1. clearly inform subscribers of the content and frequency of their push notifications, as well as how subscriptions to their push notifications can be cancelled[8];
2. refrain from differentiating between ordinary users and users who are members when determining the frequency of their push notifications[9];
3. not interfere with users closing pop-up push notification windows[10];
4. clearly display the identity of the relevant Push Notification Service Provider in push notifications[11];
5. conspicuously mark "advertisements" to notify users of their nature[12];
6. allow notifications for advertisements to be closeable with one click[13];
7. prohibit push notifications that contain links or QR codes to third-party sources[14]; and
8. establish complaint and reporting avenues[15].

The Draft Regulations also provide further guidance on the use of algorithmic models for push notifications[16], in concert with the Internet Information Service Algorithmic Recommendation Management Provisions that came into force earlier in March.

This prohibits Push Notification Service Providers from using algorithms which induce users to consume excessively, violate laws and regulations and are not ethical, or abusing personalised push notifications such as leveraging algorithms to block or over-recommend information.

To protect minors, algorithms must not be abused to target minors or to subject minors to information that adversely affects their physical or mental health.

(d) Penalties

Penalties under the Draft Regulations include warnings, fines, suspension of push notifications and even suspension of business operations.

Conclusion

The Draft Regulations apply not just to news organisations but to all Push Notification Service Providers – including any service providers with a mobile application, such as shopping centres, banks, gaming companies, food delivery companies, etc.

In summary, all companies with websites accessible in China, or mobile applications downloadable from Peoples Republic of China mobile application stores, should review their use of push notifications and associated policies, processes and guidelines.

AUTHORS

Gabriela Kennedy is a Partner of Mayer Brown in Hong Kong and head of the Asia IP and TMT group.
Joshua T. K. Woo is a registered Foreign Lawyer (Singapore) in the IP and TMT practice of the same office.
The authors would like to thank Vanessa Leigh, Trainee Solicitor at Mayer Brown, for her assistance with this Legal Update.

REFERENCES

1 Art 6, 7 of the Provisions.
2 Art 5(2) of the Draft Regulations.
3 *Ibid*.
4 Art 5(5) of the Draft Regulations.
5 www.cac.gov.cn/2021-10/18/c_1636153133379560.htm
6 Art 5(3) of the Draft Regulations.
7 Art 5(6) of the Draft Regulations.
8 Art 5(7) of the Draft Regulations.
9 *Ibid*.
10 *Ibid*.
11 *Ibid*.
12 Art 5(9) of the Draft Regulations.
13 *Ibid*.
14 Art 5(10) of the Draft Regulations.
15 Art 6 of the Draft Regulations.
16 Art 5(8) of the Draft Regulations.

EU DPAs issue €1.1 billion in GDPR fines

The amount of fines issued by EU DPAs in 2021 accounts for a sevenfold year on year increase, a survey by law firm DLA Piper reveals.

The highest fines (up till January 2021) had been issued in Luxembourg, Ireland and France (€746m on Amazon, €225m on Whatsapp and €50m on Google).

In terms of smaller, single fines combined together, Luxembourg, Ireland and Italy are the top three regulators.

John Magee, Partner and Head of Data Protection & Information Security at DLA Piper Ireland, commented on the report: "It is four years since the implementation of GDPR and we are now seeing significant fines imposed for a wide range of infringements of Europe's rigorous data protection laws. This year, regulators have issued record fines surpassing one billion euro and Ireland now ranks second overall for total fines to date, demonstrating the significant position and influence of the Data Protection Commission (DPC) in the EU. Given that Ireland is home to some of the world's largest-data businesses there is no doubt that the DPC will continue to play a central role in the enforcement of GDPR in Europe."

• *See www.dlapiper.com/en/ireland/news/2022/01/european-data-regulators-issued-over-eur1-billion-in-gdpr-fines/*

 © 2022 PRIVACY LAWS & BUSINESS

Kuwait adopts Data Protection Regulation

Regulations are GDPR-influenced but narrow in scope. By **Nada Ihab** of Access Partnership.

Businesses operating in Kuwait or processing the data of Kuwaiti residents must by 1 July 2022 comply with the provisions of the Data Protection Regulation and the recent Cloud Computing Regulatory Framework. Businesses should therefore start assessing their activities and security systems, ensure corporate policies and procedures align, and train internal staff on the core principles and obligations of the Regulation. Furthermore, cloud service providers are expected to register or obtain a license from the Regulator as required by the Cloud Computing Regulatory Framework by the end of March 2022.

Over the past two years we have witnessed the global introduction of "GDPR-inspired" data protection regulations around the world. Most regulations represent a positive move towards global harmonisation, particularly in relation to the adoption of the wider GDPR principles such as accountability, transparency, data retention and security.

In the Middle East, the risk of data protection compliance is on the rise with legacy security concerns strongly influencing governments' rush to regulate. As such, there have been a few updates to existing data protection regulations, and more importantly, the drafting of several new laws in jurisdictions with no previous comprehensive data protection laws.

In Kuwait, the Communication, Information Technology Regulatory Authority (CITRA) published the country's first comprehensive Data Privacy Protection Regulation (the Regulation)[1] in July 2021. This new Regulation seeks to address an important regulatory gap in Kuwait and will apply to both public and private sector entities processing the personal data of Kuwaiti citizens and domestic and overseas residents of Kuwait.

Prior to the issuing of Kuwait's Data Protection Regulation and Cloud Regulatory Framework, there was a general lack of central guidance for cloud policy and data governance which led to sectoral authorities to largely ignore cloud. This resulted in uncertainty over future regulation inhibiting tech adoption and the further implementation of the Policy.

Scope of the regulation

The Data Protection Regulation has a narrow scope – it applies to all ICT service providers, particularly those that provide cross border data services (i.e. public telecommunications networks, website operators, digital applications, or cloud computing services), either permanently or temporarily, using automated means or any other means that are part of a data storage system.

Kuwait's Regulation does not differentiate between data controllers and processors. Rather, the regulation defines a communications and information technology service provider (Service Providers) as: "a natural or legal person who provides communications and information technology services in Kuwait and who provides, manages, establishes, creates a public communications network, operates a website, smart application or cloud computing services, collects or processes personal data or directs another party that collects and processes personal data on its behalf through information centres that they own or use directly or indirectly."

Lawfulness and transparency

While conducting these services, providers must comply with the following conditions: a) provide users with user-friendly access to their data policies and protections; b) maintain a clear purpose for data collection (purpose limitation) and how the data will be used; c) an obligation to legally protect the data through continuous confidentiality, integrity, availability and flexibility of processing systems; and d) ensure appropriate processing and encryption of personal data as per Kuwait's Data Classification Policy (further highlight below).

The Regulation therefore aligns with the GDPR's 'lawful basis' for processing, as well as some aspects of the transparency principle. Although fairness is not explicitly mentioned in the Regulation, transparency is considered fundamentally linked to fairness.

Furthermore, similar to the recently introduced legislation in Saudi Arabia and the United Arab Emirates, there is no express acknowledgment of a controller's "legitimate interests" as a basis for the processing of personal data. This is often relied upon by companies as the legal justification for processing under other best practice legislation such as the GDPR.

Data subject rights and consent

In terms of the rights afforded to data subjects, individuals will be able to: a) withdraw consent; b) request data access, rectification and deletion; and c) receive a notification from a service provider if they intend to transfer any personal data beyond the borders of Kuwait (which will be in accordance with the Data Classification Policy). Data subjects are therefore provided with a number of rights largely based on the GDPR, but applicable only to ICT providers.

Furthermore, processing of personal data is generally prohibited unless there is a legal ground such as consent, the performance of a contract, protection of Data Subjects, or a legal provision in law.

Purpose limitation and data minimisation

The Regulation requires any processing of personal data to be conducted in accordance with specific principles, such as data minimisation.

Integrity and confidentiality (security)

All service providers must ensure appropriate levels of protection for risk response, considering the latest technology, and taking into account the potential risks and impact in respect of the rights and freedoms of natural and legal persons. The Regulation

therefore requires Service Providers to encrypt personal data in accordance with standards to be determined by CITRA and the Data Classification Policy.

Confidentiality, integrity, availability and flexibility of processing systems and services must be guaranteed on a continuous basis. However, the Regulation provides discretionary powers to CITRA, which can issue rules or directives at any time, regarding business continuity, disaster recovery and risk management. Furthermore, no limitation on data storage was mentioned in the Regulation.

Breach and notification

Service providers must notify any breach incident involving personal data to CITRA and the data owner within a period not exceeding 72 hours following discovering the incident. The Regulation, however, does provide certain exemptions to notifying data owners. This is the case when the service provider takes the following steps: a) appropriate technical and regulatory protection measures were applied to personal data affected by the breach; b) subsequent measures were taken to ensure that risks associated with the rights and freedoms of data owners are not escalated.

Data classification requirement

Unlike the GDPR, data classification is mentioned in Article 3 of the Regulation as a mandatory requirement for all entities wishing to contract a service provider in Kuwait, with a clear reference to the Data Classification Policy[2]. This requirement also mentions the possibility to follow data classification global best practices, which in most cases is an indirect reference to the GDPR.

Although the Regulation itself does not present any challenges, the outcomes of the regulatory text will have a significant impact on existing cloud-based companies operating in the country. Moreover, the subsequent Data Classification Policy, when read in conjunction with the Cloud Computing Regulatory Framework, introduces new registration and licensing processes, as well as clear data localisation requirements.

Data classification policy

The data classification process established in the separate Data Classification Policy (the Policy) is considered the foundation step of any organization's migration to the cloud in Kuwait because of its process in identifying the type of data that can be migrated to the cloud, as well as identifying their sensitivity level, protection methods, and choosing the suitable cloud model. Initially, the Data Classification Policy only listed three levels of data classification. In the subsequent amended policy, four levels were listed and additional categories were considered based on global best-practice. Tier 3 and Tier 4 data must be stored and processed within the territory of Kuwait.

Tier 1 data in Kuwait is defined as any non-classified data that is available to the public or that is not protected from public disclosure or subject to withholding under any law, regulation, or contract, and may not entail any encryption, as it does not relate to the Data Owner or government or private sector.

Tier 2 data is any private non-sensitive data and any data owned by public or private sectors or by persons indicating the identity of the Data Owner. Unauthorised disclosure of such data will not lead to infringing privacy of the Data Owner (e.g. first and last names, job title, email and age).

Tier 3 data is private sensitive data. It means any data owned by public or private sectors, or by individuals, that indicates the identity of the Data Owner and is related to this person. Data that indicates the identity of the Data Owner and is related to the content of the Data Owner. It may include a part of the non-sensitive data. Unauthorised disclosure of such data will infringe the privacy of the Data Owner (e.g. internal project reports, medical records and criminal fingerprints).

Finally, **Tier 4** data is highly sensitive data – it means any private data of a high sensitive nature. Unauthorised disclosure of such data may cause serious infringement of the privacy of the Data Owner or data owned by government, private sector, individuals or at the national level. Therefore, such data may be only circulated to a very specific category of individuals who require authorisation to such data. Such data contains high encryption requirements and needs the highest level of protection and security (e.g. political documents and sensitive information of a military nature).

Ultimately, Tier 3 and Tier 4 of the Data Classification Policy provide extra protections and considerations for individuals and service providers. CITRA grants licenses to cloud computing service providers who host the third and fourth data levels, and who have data centres within the State of Kuwait. If the data is classified above level three under the Data Classification Policy, the data owner must encrypt the data.

Data classification has been around for a very long time. In fact, it first appeared in the UK in the late 19th Century and formed part of the Official Secrets Act 1889 entitled "An Act to prevent the Disclosure of Official Documents and Information". Yet, despite it having been around for over 125 years, it's still mainly only government bodies and large financial institutions that seem to do it well.

As a best practice since the adoption of the GDPR, organizations have classified data in order to ensure correct security management measures are in place. Moreover, statistics indicate that anything up to 70% of unstructured data on a network could be considered 'ROT-ten' (Redundant, Obsolete or Trivial).[3] By only storing what you need to for as long as you need to, you will reduce your storage costs, which is also a key consideration under GDPR.

The cloud computing regulatory framework

Shortly after the publication of the Regulation and Policy, CITRA published a Cloud Computing Regulatory Framework[4] (the Framework) on 21 September 2021 to regulate the use of cloud computing services within the State of Kuwait. The framework is applicable to all cloud computing service providers licensed by CITRA which have data centres within Kuwait and who host third and fourth level data; all cloud computing service providers registered and approved by CITRA who host first and second level data; for public sector subscribers; all public sector subscribers of cloud computing services; and private sector subscribers who host government data.

 © 2022 PRIVACY LAWS & BUSINESS

Strong data localisation requirement

Article 3.1.4 allows both private sector and public sector entities to seek assistance and services from cloud computing service providers located outside the jurisdiction of Kuwait. However, although Tier 3 data can be stored and processed in private or hybrid cloud models, when Article 3.1.4 is read in conjunction with Article 4.2.1, the Cloud Computing Regulatory Framework presents a clear data localisation requirement on both Tier 3 and Tier 4 data.

In addition to the Framework, CITRA issued a set of mandatory policies and guides that support the provisions contained within the Framework, which now include the Data Protection Regulation. Other policies include: the Data Classification Policy, Cloud First Policy, Data Privacy Protection Regulation, Cloud Service Providers Regulations and Commitments, Subscribers Guide to Cloud Services and Cloud Migration Guide.

Unlike the GDPR, which does not contain any registration requirements, all cloud service providers now have to obtain a licence from or register with CITRA to process data, and will likely require local infrastructure to process Tier 3 and Tier 4 data.

Data protection challenges in Kuwait and the GCC

The majority of states in the Gulf Cooperation Council (GCC) lack personal data limitations around identifying, identifiable, and sensitive information on a human rights basis, with Kuwait as a primary example of the limited implementation of any such principles. The distinction within the GDPR that differentiates between "non-sensitive" and "sensitive" personal information operates similarly within Kuwait now with the data classification policy. However, it should be noted that in the EU, under the European Convention of Human Rights, those details and characteristics are protected much more explicitly as part of a larger comprehensive rights framework. This is a relatively predictable distinction between the GCC and EU, given the EU's much more robust and long-standing commitment to human rights.

A 2019 study[5] on the growth of Big Data in the GCC, for example, showed how further regulatory and governance implementation was necessary to utilize and grow data industries to their full potential in the GCC. The study also indicated that data governance should not only revolve around controlling and preventing misuses of data but should also support additional and improved use of data. In short, an approach that places data purely in a defence and security context, rather than understanding data within a larger framework, will inevitably be less effective, as well as exposing potentially vulnerable people to personal harm.

Implications of Kuwait's new Regulations

Data related regulations and frameworks such as those issued last year in Kuwait are designed to supervise and maintain the engagements between different stakeholders while making sure that the rights and interests of each party will be fully respected and protected. Therefore, it is crucial to observe the impact of the existing regulations and laws on the daily activities of individuals, companies, and governments at large, in order to enhance the efficiency and sustainability of the existing frameworks as well as ensure that no one is left behind.

Despite burdensome data localisation requirements as well as licensing and registration of services now in place, Kuwait's new Data Protection Regulation is an opportunity to develop the private sector's ability to operate, digitize and compete in international markets. As part of their efforts to facilitate the transition to the digital economy, Bahrain and Qatar for instance, introduced the region's first data protection laws, which aim to lead the two countries toward establishing international best practices and guarantee the compliance of businesses operating in their jurisdictions with the GDPR standards.

The ultimate goal of this legislation is to attract foreign investments by offering a comprehensive framework for data protection. For example, the main motive behind issuing Bahrain's data protection law was to prepare the country to be the region's hub for data centres, with AWS and Huawei Technologies planning to expand their data centres in Bahrain. For international business operating in Bahrain, one of the key features of its data protection law that will enhance their international operations is the concept of "data embassies," which "enables foreign clients to store their data in Bahrain while ensuring that their data is being subject to domestic laws and regulations in their country of residence as well as those of their country of origin."

As a result, however, other GCC countries such as Kuwait are now looking to compete in the same way. Overall, Kuwait's modernization of legislation and pursuit to match regulatory frameworks with international principles and protocols in terms of data privacy and protection will be essential to putting them on the region's economic map. Strict collaboration and compliance by the private sector is recommended.

REFERENCES

1 Kuwait's Data Protection Regulation Available here: www.citra.gov.kw/sites/en/LegalReferences/Data_Privacy_Protection_Regulation.pdf
2 Kuwait's Data Classification Policy available here: www.citra.gov.kw/sites/en/LegalReferences/Data_Classification.pdf
3 Veritas Global Databerg Report available here: www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data
4 Cloud Computing Regulatory Framework available here: www.citra.gov.kw/sites/en/LegalReferences/Cloud_computing_regulatory_framework.pdf
5 Deloitte Article titled "Big Data in the GCC" – ME PoV Summer 2019 Issue – Available here: /www2.deloitte.com/ye/en/pages/about-deloitte/articles/revolution/big-data-gcc.html

AUTHOR

Nada Ihab is Policy Manager at Access Partnership in London.
Email: nada.ihab@accesspartnership.com

Dark patterns: Here to stay or not going away?

Are confusing privacy dialogues, like this headline, really the future for online services? What is the way forward for businesses and will proposed regulation actually work? **Tom Cooper** reports.

Dark patterns[1] proliferate on the Internet, from hard to leave subscriptions to unfathomable double negatives. Is this the inevitable result of a "race to the bottom" in privacy driven by competitive pressures? Or are these practices as bad for business as they are consumers? These were some of the questions addressed at a recent *PL&B* webinar 'Shining the light on dark patterns'.[2]

A useful working definition of dark patterns is: "User interface design choices that benefit an online service by coercing, manipulating or deceiving users into making unintended and potentially harmful decisions."[3] Dr Jennifer King, Privacy and Data Policy Fellow, Stanford Institute for Human-Centered Artificial Intelligence, chose this definition as she opened the online discussion.

Dark patterns are typically found at "decision points," online, King said. "That's where someone wants to persuade you, or push you towards a decision that favours them over potentially your own autonomous decision."[4] These patterns take advantage of the way people make decisions – either via shortcuts in the way humans make choices (heuristics) or quirks in the way people think (cognitive bias). These are generally universal aspects of human thinking, King said.

Examples of commonly seen dark patterns include false urgency – for example "only three left" splashed over an e-commerce checkout screen, or an accelerating countdown timer. "Often these are false," King said. Guilt shaming is another approach, sometimes as blatant as having to click "I am a bad person". Coercive and confusing dialogs proliferate in privacy-related aspects of online interactions. Sometimes there is scant real choice, or if there is, it can be hard to decide if you are agreeing or disagreeing to something, she said.

Hot topic

Dark patterns are a "hot topic" now and King asked the panel why. Finn Myrstad, Head of Digital Services Section, Norwegian Consumer Council, said this was due to widespread use, coupled with increased public scrutiny. "People feel annoyed, manipulated, and feel stupid. It impacts our integrity, autonomy even our freedom of thought," Myrstad said. "At a societal level we also believe that, over time, it erodes trust in digital service, many of which are useful, helpful, and necessary to participate in society."

Dr Dan Hayden, Director, Data Strategy at Meta, said dark patterns gave a term "to the frustration that many people feel online." Hayden is co-lead of TTC Labs – a co-creation and design lab focused on improving user experiences around personal data. "What is really useful about the concept of dark patterns is that it raises the bar for good design," he said. Broadly that is good for the industry – these are the interfaces we have with consumers, the relationship we have that reflects the trust people have for our services, he said.

But he warned the term could become so broad it stopped being useful. We need to tell people what they need to avoid – what does coercion look like online, what does manipulation look like online, what are the right bounds of "this is a fair commercial offering" and what isn't, he said. "But some of that also means not trying to take every kind of issue on at the same time and continually expanding the scope," he said.

Consent

Obtaining fair and informed consent online is a problematic area. This could be a difficult design problem, Hayden said. But it was an "entirely reasonable" ideal. There was no simple checklist. "Fairness is the quality you need. You need to work within the constraints that exist in terms of people's time and their attention. You need to make consents clear and unambiguous. You need to represent clear choices to people, and you need to ask people a question that relates to what they are trying to do and that makes sense to them."

"The good news is the tools we have as designers, of listening and talking to people, experimentation and prototyping, are really well suited to helping to do that better," he said. "The main job now is to spread the good practices as widely as possible."

Myrstad argued for a completely different approach to the issue. "If companies used PbD (Privacy by Design) you would have a lot less need for consents in the first place," he said. "If the principles of PbD, and purpose limitation are respected, a lot of these problems would go away." Current business models were based on collecting as much data as possible. "I wish we could change that dynamic. We could still have digital services, still provide advertisements, but without collecting so much data," he said. "These data-hungry business models are driving the use of dark patterns."

Jane Hunt, Senior Legal Counsel at travel technology company Amadeus, came in on this point. There was always commercial pressure for getting as much data as possible "just in case". But there were alternatives, such as data aggregation. A business might need to know how many people travel to Silicon Valley in a given month, she said "But do you need to know who?"

Amadeus provides technology to the travel industry including airlines, hotels, and travel agencies. "It grew as a computer reservation system," Hunt said. It was the first system to connect travel agencies with airlines. It has grown to provide a wider range of services. She explained that in the early days of the reservation system there was regulation – so everyone saw the

 © 2022 PRIVACY LAWS & BUSINESS

same information. Now there was little regulation and no standardisation. "That makes it difficult to compare one product to another," she said. "That lack of standardisation creates a lack of trust."

Hayden agreed that industry could be more precise or narrower in collecting data. But many services were data driven, not just for the business model, but for the service being provided. Examples from the social-network world would include tailoring a user's news feed and picking the posts you are providing. The views of experts had to be reconciled with people's "day-to-day use of services they find useful, and what they find annoying," he said.

Research

The key questions from the empirical work were what are the perceived harms, what are the negative experiences of digital services and where am I really frustrated, Hayden said. Work by Luguri and Strahilevitz[5] identified bad patterns, and many areas for improvement. But it also showed people want a "guided experience" in many areas, he said.

"The goal I would pursue is fairness. How do you provide online experiences and in those important moments especially, set the right boundaries, the right safeguards avoid unfair practices?" Practices that made users feel insecure, disrespected, or uncertain should be avoided. "Those are toxic both to brands and the relationship," he said, "and also toxic in the basic name of the responsible use of data."

Myrstad took a more cautionary lesson from the research results. Much of it showed that certain people were more vulnerable than others, he said. People could be targeted based on vulnerabilities, for example to gambling or taking out loans or they might be insecure about their looks. "These are real examples of ads that are targeted at vulnerable people or people in vulnerable situations today."

"When you can profile users in the way that we can today, to the level of identifying vulnerabilities, you can really tailor messages towards those groups and exploit those vulnerabilities." More research was welcome but dark patterns should be stamped out now. "Some of them are very obvious and should just be ended," he said.

Regulation was needed. Some companies wanted to do better but felt they couldn't because of what their competitors were doing . "If we could raise the bar it would be better for everyone," Myrstad said.

Race to the bottom?

King said that in the US, where there was very little privacy law, she saw a "race to the bottom" in privacy. "Businesses that don't engage in the same practices as their competitors will find themselves at a disadvantage," she said.

Hunt said that was an everyday debate within companies. "Genuinely, some businesses want to do right," she said. But there was often financial pressure based on what competitors were doing. Privacy standards could, however, be a commercial positive. "We are finding it can be a selling point – we are a European company we use European standards and we like to impose those rights globally," she said. "There is often an internal wrangle in businesses," she said. "But there is always that nagging doubt in the end – my competitor is doing this, why can't I?"

Regulation

King steered the discussion back towards regulation. What is the way forward?

Myrstad said regulation should be principle based – for example it should be as easy to leave a service as to join[6]. But there was also scope for specific bans of certain practices. "I'm hoping we can create laws in the US and Europe where many of these companies are based," he said.

King said the "dark patterns" amendment to the proposed EU Digital Services Act[7], went into some specific design guidelines – such as equal visual prominence. She asked Hayden, as a designer, was this a good idea? "What does it mean to have neutral design in those decision points we have mentioned?"

Hayden said there were practices "that clearly shouldn't exist". These frustrated users, making it deliberately hard for people to achieve what they wanted to do. "Eliminating those practices is clearly in the common interest," he said. But it was hard for prescriptive guidance to keep up with trends in the design of user interfaces, and it could "create a worse experience for people."

Past experiments with legal standards were "not covered in glory." Industry-set guidelines had worked better and there was an incentive for the industry to set these, as bad practices – such as persistent nagging, double negatives and forced timers – reflected on everyone. "We need to hold bad actors to account we need to eliminate the worst practices," Hayden said.

REPORTING DARK PATTERNS

darkpatterns.org – the site by the creator of the term 'dark patterns' Harry Brignull. Since the webinar this has been retitled 'Deceptive Design' and redirected to www.deceptive.design

darkpatternstipline.org/ – does what it says. Hosted by Digital Civil Society Lab at Stanford PACS and run by a team including Dr King. Includes sightings of dark patterns classified by type.

REFERENCES

1 UX specialist Harry Brignull coined the term "dark patterns" and launched the website darkpatterns.org in 2010. This now redirects to www.deceptive.design "in an effort to be clearer and more inclusive."

2 A recording of the session is available at www.privacylaws.com/events-gateway/events/darkpattern22/

3 Arunesh Mathur, Jonathan Maayer, and Mihr Kshirsagar in What Makes a Dark Pattern…. Dark?: Design Attributes, Normative Considerations, and Measurement Methods. Conference on Human Factors in Computing Systems (CHI '21)

4 For a comprehensive list of types of dark patterns see www.deceptive.design/types

5 academic.oup.com/jla/article/13/1/43/6180579?login=false
Shining a Light on Dark Patterns
Jamie Luguri, Lior Jacob Strahilevitz
Journal of Legal Analysis, Volume 13, Issue 1, 2021, Pages 43–109, doi.org/10.1093/jla/laaa006
Published: 23 March 2021

6 The Norway Consumer Council has started legal action against Amazon arguing that it makes it difficult to unsubscribe from Amazon Prime. See www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/.

7 For the latest amendments agreed by the European Parliament see https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.html in particular Article 13a and Recital 39a

New EU-US data transfer deal agreed in principle

The political statement is yet to be followed by concrete details on how the framework will work and the differences from the old Privacy Shield. By **Laura Linkomies**.

The United States and the European Commission announced on 25 March that they have committed to a new Trans-Atlantic Data Privacy Framework. According to the White House, the US has made unprecedented commitments to:

- strengthen the privacy and civil liberties safeguards governing US signals intelligence [intelligence-gathering by interception of signals] activities;
- establish a new redress mechanism with independent and binding authority; and
- enhance its existing rigorous and layered oversight of signals intelligence activities.

The US administration says that this means, for example, that "signals intelligence collection may be undertaken only where necessary to advance legitimate national security objectives, and must not disproportionately impact the protection of individual privacy and civil liberties."

EU individuals may seek redress before an independent Data Protection Review Court [DPR Court] that would consist of individuals chosen from outside the US Government. They would have full authority to adjudicate claims and direct remedial measures as needed.

In addition, US intelligence agencies will adopt procedures to ensure effective oversight of new privacy and civil liberties standards.

"We managed to balance security and the right to privacy and data protection", Ursula von der Leyen, President of the European Commission said. The EU says there will be 'specific monitoring and review mechanisms'.

Why a new deal?

A new framework is needed due to the invalidation of the EU-US Privacy Shield. The Court of Justice of the European Union (CJEU), in the *Schrems II* case of July 2020 decided that the US legislative framework did not provide sufficient protections to EU personal data due to possible access by intelligence agencies. The Court also said that the Ombudsman mechanism needed improvements to the redress mechanism.

Since then, companies have relied on Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs) or Codes of Conduct, all of which have challenges and costs associated with them.

When will the deal be ready?

The details of the new deal will still need to be ironed out but are expected this Spring. The EU announced that the EU and US negotiating teams "will now continue their cooperation with a view to translate this arrangement into legal documents that will need to be adopted on both sides to put in place this new Trans-Atlantic Data Privacy Framework. For that purpose, these US commitments will be included in an Executive Order that will form the basis of the Commission's assessment in its future adequacy decision."

Hogan Lovells lawyers comment in their blog that Executive Orders cannot create new federal law[1].

"An obvious question from the European perspective is why the US Government has not chosen to sidestep these questions by establishing the DPR Court by means of primary legislation. The practical answer may relate to the length of time that passing such legislation would likely take and the urgent need to find a solution in light of recent European regulatory action relating to the new Standard Contractual Clauses."

"However, this does not mean that 'essential equivalence' cannot be met by means of an Executive Order. For example, the US Attorney General, a member of the US Executive, has existing procedures in place by which it can appoint independent Special Counsel to investigate circumstances which could otherwise give rise to a conflict of interest. It is possible that appointments to the DPR Court would be similarly modelled, in order to ensure sufficient independence."

Amsterdam-based Andre Walter, Head of Data Law Solutions at Pinsent Masons said: "While the announcement of a new transatlantic data privacy framework is welcome, it lacks the detail that businesses will be looking for to understand how the new framework addresses the concerns of the CJEU from its *Schrems II* decision[2]."

"We do not yet know how the new commitments around oversight and redress will look in practice and there is also no indication of how long it might take for the framework to be finalised and then given legal effect. For businesses, there is also a timing issue in respect of compliance. They have a major contract remediation project to engage in, in respect of data processing to transition to new standard contractual clauses the European Commission has developed before the end of the year. There is no time to wait for the new Privacy Shield 2.0 and hope it supersedes the need for SCCs," he said.

New legal challenge ahead?

Another type of challenge may be forthcoming. *Max Schrems* declared: "We already had a purely political deal in 2015 that had no legal basis. …. we could play the same game a third time now."

"The final text will need more time, once this arrives we will analyse it in depth, together with our US legal experts. If it is not in line with EU law, we or another group will likely challenge it. In the end, the (CJEU) will decide a third time. We expect this to be back at the Court within months from a final decision."

The announcement of the forthcoming deal was received enthusiastically by many. Julie Brill, Corporate

 © 2022 PRIVACY LAWS & BUSINESS

Vice President for Global Privacy and Regulatory Affairs, and Chief Privacy Officer at Microsoft wrote in her blog: "Microsoft is committed to embracing the new framework and will go beyond it by meeting or exceeding all the requirements this framework outlines for companies. We will do this through enhancements to how we handle legal requests for customer data and providing further support for individuals concerned about their rights."

But some commentators remain sceptical as to whether the framework is different enough from the Privacy Shield to prove viable.

Industry views and the UK's special case

A day prior to the announcement, a panel discussion at the IAPP data privacy conference in London pondered the future of international data transfers. *Vivienne Artz*, Senior Data Strategy and Privacy Advisor at the Centre for Information Policy Leadership questioned whether we want to encourage SCCs all over the world. UK businesses already face the dilemma over whether to use the new UK SCCs or the revised EU ones. Instead, we need consistency of data flows, she said. Codes of Conduct are challenging as they need to be approved by the DPAs. But industry bodies could come up with suggestions, and build risk assessment sides to the codes, she said.

The UK ICO recently issued its version of the EU SCCs. *Emma Bates*, General Counsel at the ICO said that the ICO wants to hear from industry about their experience and ideas about transfer tools. Our door is open, she said – the ICO wants to remove unnecessary burdens. After Brexit, there may be some scope to improve BCRs in the UK, she said.

In a separate panel, *Eduardo Ustaran*, Partner at Hogan Lovells said that companies in the UK are too concerned about losing adequacy. It is perfectly possible to retain adequacy and modify the law, he said.

Ruth Boardman, Partner at law firm Bird & Bird said that Brexit has added a bit of friction for transfers but it can be overcome with 'clever drafting'. She thought that it is very difficult for organisations to carry out a risk assessment for data transfers, and it would be helpful to have an outcome on this from the UK government consultation on revising the UK data protection framework. This means not adding to the uncertainty by creating a unique UK system that increases bureaucracy.

Both Ustaran and Boardman sit on the newly created UK government steered data transfer council, which is an advisory body. The DCMS's (UK government department in change of data protection policy) Deputy Director *James Snook* said that the UK is committed to retaining its EU adequacy. One of the issues highlighted as a possible challenge by the EU is onward transfers from the UK, possibly to the US. Snook said that the UK has separate conversations with the US and these negotiations are not tied to the progress made with the EU-US deal.

In fact, the UK government is conducting negotiations on international data transfer agreements with 10 priority countries with the aim to complete them this year. In response to a question from *PL&B's* Stewart Dresner, *Vince Weaver*, the DCMS head of these negotiations, in his role as Head of Governance, International Data Transfers, said that each agreement would be announced when it is reached. There is no intention to wait for an announcement until the tenth agreement.

INFORMATION

www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/

ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

REFERENCES

1 www.engage.hoganlovells.com/knowledgeservices/news/eu-and-us-on-course-to-adopt-schrems-ii-compliant-transfers-framework
2 www.pinsentmasons.com/out-law/news/new-framework-for-eu-us-data-flows-moves-closer

events diary

Making your case in Europe: Defending against DPA inquiries and sanctions
18 May 2022 9am-1pm
London and online
In cooperation with Latham & Watkins, this event will help you negotiate with DPAs in France, Germany, Ireland and Spain.
Chair: **Gail Crawford**, Partner, L&W, UK
Speakers: **Myria Saarinen**, Partner, L&W, France; **Tim Wybitul**, Partner, L&W, Germany; **Brian Johnston**, Partner, Mason Hayes & Curran, Ireland; **José Maria Alonso**, Partner, L&W, Spain; **James Lloyd**, Partner, L&W, UK.
www.privacylaws.com/europe2022/

PL&B Roundtable on proposed reform to UK DP legislation
25 May 2022, 9am-3pm
London
In cooperation with Norton Rose Fulbright, this roundtable will enable companies and their advisors to provide feedback to Julia Lopez, DCMS Minister, on proposals to reform UK data protection legislation.
www.privacylaws.com/uk2022/

CPDP
15th Computers, Privacy & DP International Conference
23-25 May 2022
Brussels, Belgium
PL&B is pleased to be a Media Partner for this conference.
For information, programme and registration see cpdpconferences.org

PL&B 35th Anniversary International Conference: Winds of Change
4-6 July 2022
St John's College, Cambridge and online
This conference brings you into contact with privacy regulators, challenges conventional wisdom and offers a great networking experience.
Confirmed speakers include:
Wojciech Wiewiórowski, European DP Supervisor, Brussels; **Bruno Gencarelli**, International Data Flows and Protection, European Commission, Brussels; **Karolina Mojzesowicz**, DP Unit, European Commission, Brussels; **Michael McEvoy**, Information & Privacy Commissioner for British Columbia, Canada; **Emilie Brune**t, Legal Advisor, International Service, CNIL, France; **Claudia Berg**, General Counsel, ICO, UK.
www.privacylaws.com/plb2022

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 168+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 168+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

> "*PL&B International Report* is a very useful and business-friendly publication that allows our team to easily and frequently keep up with developments in countries outside our jurisdictions of activity."
>
> **Magda Cocco and Inês Antas de Barros, Partners and Isabel Ornelas, Managing Associate, Information, Communication & Technology Practice, Vieira de Almeida, Lisbon**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.