Digital Policy Alert

GLOBAL DIGITAL POLICY ROUNDUP

JUNE 2026

Global Digital Policy Roundup: June 2026

The roundup is produced by Digital Policy Alert, an independent repository of policy changes affecting the digital economy. If you have feedback or questions, please contact Maria Buza.

POLICY SECTIONS

Overview. The roundup serves as a guide for navigating global digital policy based on the work of the Digital Policy Alert. To ensure trust, every finding links to the Digital Policy Alert entry with the official government source. The full Digital Policy Alert dataset is available for you to access, filter, and download. To stay updated, Digital Policy Alert also offers a customizable notification service that provides free updates on your areas of interest. Digital Policy Alert's tools further allow you to navigate, compare, and chat with the legal text of AI rules across the globe.

Drawing from the Digital Policy Alert's daily monitoring of developments in the G20 countries, it summarizes the highlights of June 2026 in four core areas of digital policy.

- **Content moderation,** including the European Parliament and Council's provisional agreement on the Directive on combating child sexual abuse material, the United Kingdom's announcement of planned secondary legislation prohibiting social media services for children under 16, the Brazilian Supreme Federal Court's final thesis on platform liability for third-party content under Article 19 of the Internet Civil Framework, Australia's bill strengthening enforcement of the social media minimum age, and Canada's introduction of the Digital Safety Act.
- **AI regulation,** including the European Parliament's passage and the Council's adoption of the Digital Omnibus on AI Regulation, the European Commission's proposal for the Cloud and AI Development Act, the signature of the Pax Silica Declaration by ten additional countries, the Joint Statement on AI Opportunity by 35 countries, and the introduction of Russia's bill on supporting the development of AI technologies.
- **Competition policy,** including the European Commission's preliminary positions that Amazon Web Services and Microsoft Azure should be designated as gatekeepers under the Digital Markets Act, the General Court's partial annulment of Meta's gatekeeper designation, and the UK Competition and Markets Authority's conduct requirements on Google in general search services.
- **Data governance,** including Canada's House of Commons' passage of the Lawful Access Act and the introduction of the Protecting Privacy and Consumer Data Act, Saudi Arabia's Data Monetisation Policy, South Korea's KRW 624 billion fine imposed on Coupang following a large-scale data breach, and the Irish High Court's judgment upholding the EUR 530 million fine against TikTok and referring questions to the Court of Justice of the European Union.

Content moderation

Europe

The **European Parliament** and the Council reached a provisional agreement on the Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material. The Directive introduces new criminal offenses relating to technological developments, including the design, adaptation, or distribution of AI systems intended to generate child sexual abuse material, paying to access livestreamed child sexual abuse, and the sexual extortion of children. The Council adopted conclusions on preventing and combating cyber violence against girls, recommending that Member States and the European Commission take measures concerning gender-based violence online, including through design requirements for online platforms and infrastructure providers.

Furthermore, the European Commission opened a consultation on draft guidelines for the trusted flagger mechanism under Article 22 of the Digital Services Act and issued the State of the Digital Decade report. Additionally, the European Commission and Brazil's National Data Protection Authority signed an administrative arrangement on the protection of children and adolescents in the digital environment.

At the judicial level, the Court of Justice of the European Union (CJEU) ruled that Member States may impose individual age verification measures on providers of pornographic content established in other Member States, while general and abstract criminal law obligations cannot be applied to such providers under the e-Commerce Directive. The CJEU also ruled that Member States may prohibit navigation service operators from rebroadcasting roadside check information and issued a judgment on jurisdiction over personality rights claims arising from audiovisual content broadcast on television and the internet.

In **Russia**, the Federation Council adopted a bill amending the Code of Administrative Offenses to introduce fines for violations of the rules governing recommender systems. The bill provides for fines of up to RUB 700,000 for legal entities, and up to RUB 1.4 million for repeat violations, for failing to inform users about recommender systems, publish rules governing their use, or comply with the Federal Service for Supervision of Communications, Information Technology and Mass Media orders.

The **United Kingdom's** Department for Science, Innovation and Technology announced plans for secondary legislation under the Children's Wellbeing and Schools Act that would prohibit user-to-user social media platforms from offering services to children under 16, prohibit under-16s from livestreaming, and require AI romantic companion chatbots to enforce a minimum age of 18. The Prime Minister also announced an initiative to require technology companies to implement device-level controls to prevent minors from creating, sharing, receiving, or viewing sexually explicit content, with legislation to be considered if industry implementation is insufficient.

The Office of Communications (Ofcom) published draft amended Illegal Content Codes of Practice for user-to-user services and search services, incorporating encouraging or assisting serious self-harm and cyberflashing as priority offenses under the Online Safety Act. Ofcom also proposed crisis protocol measures recommending that providers prepare protocols to manage risks arising from significant increases in illegal or harmful content during crises and maintain dedicated

communication channels for law enforcement. Ofcom also published an open letter to online service providers regarding civil unrest in Belfast, recommending the implementation of the crisis protocol before the formal adoption. Furthermore, Ofcom adopted recommendations on designing for media literacy and issued a statement on the categorization impact assessment under the Online Safety Act. Finally, Ofcom fined First Time Videos GBP 80,000 for failure to implement highly effective age assurance to prevent children from accessing pornography.

Asia and Australia

In **Australia**, the Online Safety Amendment (Strengthening Enforcement for the Social Media Minimum Age) Bill was introduced to the House of Representatives. The bill expands the eSafety Commissioner's information-gathering powers to cover age assurance providers and app store providers and increases the maximum penalty for systematic breaches from AUD 49.5 million to AUD 99 million. The eSafety Commissioner issued an outline on safety by design obligations to combat sextortion, highlighting measures including language analysis, classifier tools and removal of image-based abuse material. The Digital Platform Regulators Forum adopted a memorandum of understanding formalizing its operation.

Regarding **enforcement**, the eSafety Commissioner confirmed that three AI-powered nudifying services withdrew from the Australian market following its investigation into their age assurance measures. The Competition and Consumer Commission (ACCC) filed a lawsuit against Amazon over alleged unfair contract terms related to the introduction of advertising to Prime Video, confirmed that eDreams and HSK United paid fines of AUD 59,400 and AUD 79,200, respectively, over misleading pricing claims, and issued an AUD 19,800 infringement notice to WeFlex over misleading advertising. Lastly, the ACCC issued takedown requests to Amazon, eBay, Kogan, and Fruugo over listings of banned magnet toys and announced that Temu and Gumtree joined the product safety pledge for e-commerce.

In **China**, the National Cybersecurity Standardization Technical Committee (TC260) opened consultations on guidelines for the security of applications involving minors in cybersecurity and AI technologies and on a national standard on security testing and evaluation methods for critical information infrastructure. The Ministry of Industry and Information Technology (MIIT) consulted on a standard on technical requirements for industrial knowledge intelligent computing on industrial internet platforms.

Regarding **enforcement,** the MIIT issued guidance on the management of in-app information windows, prohibiting deceptive or misleading prompts such as shake-activated redirects and requiring companies to conduct self-inspections. The State Administration for Market Regulation (SAMR) and other departments interviewed seven third-party train-ticket platforms over misleading promotion and the unlawful collection of information.

In **India**, the Ministry of Electronics and Information Technology issued an order restricting access to Telegram to prevent alleged fraud and misinformation during a national examination period. Additionally, the High Court of Delhi dismissed Telegram's petition challenging the order. The Central Consumer Protection Authority also fined Physicswallah INR 500,000 over the deployment of dark patterns.

In **Indonesia**, the obligation to submit self-assessment reports under the Ministerial Regulation on Child Protection in Electronic Systems came into force. Furthermore, the Ministry of

Communication and Digital Affairs confirmed that electronic system providers, including Netflix, TikTok, ChatGPT, and Grab submitted self-assessment results on age verification measures. Further, TikTok deactivated 4.1 million child accounts, and YouTube removed 600,000 child accounts and launched a digital well-being guidebook in compliance with child protection obligations. The Ministry also issued findings on online gambling-related bot activity targeting social media comment sections.

In **Japan**, the Ministry of Internal Affairs and Communications published a report recommending measures for youth protection in online environments, including default protection measures for young users, strengthened age verification beyond self-declaration, and mandatory requirements for operating system vendors. The Ministry also opened a consultation on a report addressing issues in information distribution in the digital space.

In **South Korea**, several bills amending the Network Act on the decriminalization of true-fact defamation, user speech rights, hate information moderation obligations, and the preservation of AI-generated labels were introduced to the National Assembly. Further bills address platform operators' liability for hazardous products in e-commerce and age verification under the Network Act.

Additionally, the Fair Trade Commission (FTC) adopted an amendment to its guidelines on reviewing labeling and advertising, requiring the disclosure of AI-generated virtual persons used in recommendations and endorsements. Additionally, the Communications Commission and other ministries signed a memorandum of understanding on technical cooperation for deepfake sexual crime response, and the Broadcasting Media and Communications Commission announced the establishment of an AI crime response inter-agency consultative body. Lastly, the Commission published the transparency report on illegal filming materials, including sexual deepfake videos and child sexual exploitation materials, covering 83 operators, including Naver, Kakao, Google, and Meta. Regarding enforcement, the FTC rejected an application by Baemin to resolve its investigation into misleading advertising of delivery times through consent decree proceedings and fined Trip KRW 10 million over consumer protection violations in airline ticket sales.

Americas

In **Brazil**, the Supreme Federal Court concluded its review of platform liability for third-party content under Article 19 of the Internet Civil Framework, holding that the provision is partially unconstitutional. The Court ruled that user-generated content platforms may be held jointly liable for unlawful third-party content in certain cases without a prior court order, including for paid advertisements, algorithmically amplified content, and specified serious criminal content, if they fail to comply with removal obligations. The decision also requires providers to implement self-regulation measures, complaint mechanisms, annual transparency reports, and appoint a legal representative in Brazil. The ruling applies prospectively from August 5, 2025, with providers given 60 days to comply with the new structural obligations.

Regarding enforcement, the National Data Protection Authority began monitoring pornographic content providers, app stores, and operating system providers for compliance with age verification and age assurance requirements under the Digital Statute of Children and Adolescents and launched a complaints channel for reporting violations.

In **Canada**, the Digital Safety Act was introduced to the House of Commons, including content moderation regulation, content moderation authority governance, design requirements, age verification requirements, and user rights. The Act would require social media operators to make child sexual abuse material and non-consensual intimate images inaccessible in Canada within 24 hours, submit digital safety plans, and, for AI chatbot operators, publish user guidelines on mitigating harmful content and addressing users expressing suicidal ideation. The accompanying Digital Safety Commission of Canada Act would establish the enforcement authority. Separately, the Minister of Canadian Identity and Culture directed the Radio-television and Telecommunications Commission to review its Canadian programming expenditure framework under the Online Streaming Act.

Artificial Intelligence

International cooperation

At the Second Pax Silica Summit, ten additional jurisdictions, including the European Union, Germany, and Argentina, signed the Pax Silica Declaration, bringing the total number of signatories to 24. The Declaration provides for cooperation across the AI supply chain and coordination on measures concerning sensitive technologies. At the same summit, 35 jurisdictions signed the Joint Statement on AI Opportunity, setting out shared principles on AI governance, cooperation on AI supply chains, and access to AI computing resources.

Europe

The **European** Parliament passed, and the Council of the European Union subsequently adopted, the Digital Omnibus on AI Regulation. The Regulation clarifies the AI Office's competences for supervising AI systems based on general-purpose AI models, extends its enforcement powers to AI systems embedded in very large online platforms and search engines, expands access to AI regulatory sandboxes, including an EU-level sandbox, and extends SME exemptions to small mid-cap enterprises. The Regulation also amends the AI Act's design, quality of service, and cybersecurity requirements for high-risk AI systems, the legal basis for processing special categories of personal data for bias detection, and the registration requirements for high-risk systems.

The European Commission submitted a proposal for the Cloud and AI Development Act. The proposal introduces four Union assurance levels with cumulative technical and organizational criteria for cloud computing services to be recognized as providing sovereignty assurance, verified through self-assessment or independent third-party audits, alongside cybersecurity provisions and public procurement access rules.

The Commission published the draft Code of Practice on the marking and labeling of AI-generated content under Article 50 of the AI Act and established the AI Act Advisory Forum and the AI Act Scientific Panel. Additionally, the Commission closed its call for evidence on the review of the Copyright in the Digital Single Market Directive, released the EU Open Source Strategy, and issued the Strategic Roadmap for Digitalisation and AI in the Energy Sector.

Germany's Digital Committee approved the bill implementing the EU AI Act. It designates the Federal Network Agency as the primary AI market surveillance authority, while assigning financial sector oversight to the Federal Financial Supervisory Authority. It also requires the establishment of at least one AI regulatory sandbox by 2 August 2026.

In **Russia**, the bill on supporting the development of AI technologies was introduced to the State Duma. It establishes a governance framework for large foundation AI models, including government powers to determine state support measures, mandate the use of sovereign or national models in specific cases, and set risk prevention requirements. The bill also includes design requirements, security requirements, copyright protection regulations, and a data localization requirement. Separately, the State Duma rejected a bill on the mandatory labeling of AI-generated video materials. Finally, Russia and Vietnam announced a cooperation agreement on emerging technologies.

In the **United Kingdom**, the Ministry of Justice launched the Legal Services Advisory AI Growth Lab, a supervised testing environment for AI applications in legal services.

Asia and Australia

China's Ministry of Industry and Information Technology (MIIT) issued implementation opinions on the development of AI in the information and communications sector, setting out measures relating to telecommunications, AI infrastructure, sectoral applications, and governance. MIIT also opened a consultation on a list of selected typical cases of AI applications, including Huawei Cloud's ModelArts platform for large model industrialization, Baidu's PaddlePaddle deep learning framework, and humanoid and embodied intelligence robot applications from firms such as UBTECH and Leju Intelligent.

In **India**, the Ministry of Communications established a national working group on AI to coordinate AI standardization activities and to support India's participation in international AI standardization processes. Further, the Prime Minister issued a statement on ensuring the safe, rapid, and efficient rollout of AI, "proposing the promotion of safe-by-design AI systems, developing common standards, testing frameworks, and regulatory sandboxes, and strengthening global cooperation against deepfakes, misinformation, and cyber fraud. India concluded agreements with Slovakia covering AI, the Internet of Things, and machine-to-machine applications, and with South Africa on AI and digital infrastructure.

Japan's Digital Agency adopted guidelines for the procurement and utilization of generative AI in government administration, requiring contracted vendors to meet obligations including incident response procedures, data handling and quality controls, and security measures against prompt injection and denial-of-service attacks.

In **South Korea**, three bills amending the Framework Act on the Development of Artificial Intelligence were introduced to the National Assembly. The first bill addresses the use of non-personal training data in AI development. The second bill expands the Act's category of AI vulnerable groups to include children and adolescents. The third bill establishes a dedicated governance framework to promote and support the development of physical AI. Additionally, the Ministry of Science and Information and Communication Technology consulted on an amendment to the Enforcement Decree of the Framework Act, which defines AI-vulnerable groups and establishes an AI product and service verification system for public procurement.

Competition

Europe

The **European Commission** opened consultations on proposed regulations on multimodal booking and rail ticketing. The proposals would require multimodal booking services to display products neutrally and online rail ticketing platforms to host products on non-discriminatory terms. The Commission also submitted the proposal for the Chips Act 2.0, including measures on eligibility for state aid-compatible support for European semiconductor technology initiatives.

Regarding enforcement, the Commission adopted interim measures requiring Meta to restore and maintain free access to the WhatsApp for Business API for rival general-purpose AI assistants until the conclusion of its investigation. The Commission found that Meta's fee-based access policy was equivalent to an access ban and posed a risk of harm to competition in the AI assistant market.

The Commission reached the preliminary position that Amazon Web Services and Microsoft Azure should be designated as gatekeepers under the Digital Markets Act (DMA) based on their cloud computing services. Further, at the judicial level, the General Court of the European Union issued a ruling partially annulling the gatekeeper designation of Meta Platforms under the DMA. The Court upheld the designation of Facebook Messenger as a standalone core platform service but annulled the designation of Facebook Marketplace, finding that the Commission had applied an incorrect legal time frame and had not adequately explained why Marketplace still qualified as an online intermediation service following listing restrictions implemented in 2023.

The **Italian** Competition Authority opened an investigation into Apple over alleged violations of the DMA's interoperability provisions. The Authority will investigate whether Apple ensures that third-party consumer cloud providers have free and effective interoperability with iOS and iPadOS on equal terms with Apple's iCloud. The investigation was opened following complaints submitted in April 2025 and subsequent complaints. The Authority's findings will be shared with the European Commission to support its role as the sole enforcer of the DMA.

The **United Kingdom** Competition and Markets Authority (CMA) imposed conduct requirements on Google following its strategic market status designation in general search services. The fair ranking requirement obliges Google to rank organic search results, including within search generative AI features, based on objective and non-discriminatory criteria and to give publishers advance notice of ranking changes, while further requirements cover data portability and the use of publisher content in general search services.

The CMA also opened consultations on proposed steering conduct requirements for Apple's and Google's mobile platforms, and opened a call for evidence on near-field communication access conditions on Apple's mobile platform. Finally, the CMA consulted on final undertakings pertaining to Getty Images' acquisition of Shutterstock and opened an investigation into eBay's proposed acquisition of Depop.

Asia and Australia

The **Australian** Competition and Consumer Commission (ACCC) granted interim authorization to the application store settlement agreement between Google and Epic Games on the basis that the interim conduct is unlikely to reduce competition for Australian users. The ACCC further issued a determination denying authorization for Screen Producers Australia to collectively bargain with streaming services on model contract terms.

In **China**, the State Administration for Market Regulation issued rectification measures against Lalamove pertaining to anti-monopoly compliance, requiring the company to cease algorithmic freight price suppression, refund drivers RMB 120 million in unreasonable fees, cut its commission rate from approximately 11% to approximately 9%, and establish a RMB 50 million driver assistance fund.

In **South Korea**, the bill on audiovisual media services was introduced to the National Assembly. It would repeal the existing broadcasting laws and establish a unified regulatory framework for over-the-top (OTT) services and content-sharing platforms. It sets out obligations regarding service provision, contractual practices, and the use of viewer data, and authorizes the Broadcasting Media and Communications Commission to order corrective measures and impose administrative surcharges for non-compliance. The Fair Trade Commission (FTC) published a report on algorithm-based self-preferencing by digital platforms, finding that artificially favorable ranking increased purchases of a platform's own product by approximately 34% and decreased purchases of the top-ranked competing product by approximately 32%. Regarding enforcement, the FTC rejected applications by Coupang and the operator of Baemin to resolve investigations into alleged most-favored-nation clause demands through consent decree proceedings.

Americas

Argentina's National Competition Authority approved Telecom's acquisition of Telefónica Móviles, subject to structural and behavioral remedies. Telecom must divest certain mobile, fixed-line, and fiber assets and provide the new operator with access to roaming and infrastructure. The decision also imposes obligations related to non-discrimination, service quality, and wholesale access.

Brazil's National Telecommunications Agency (Anatel) announced an inquiry into the Internet of Things and machine-to-machine communications markets. The inquiry will examine business models, connectivity investments, network impacts, and barriers to market entry. The findings will support Anatel's monitoring of wholesale connectivity markets, dispute resolution, and potential future regulation to promote competition.

Africa

The Competition Commission of **South Africa** closed its consultation on the review of regulations that may restrict competition and the entry or expansion of firms, with a particular focus on small and medium-sized enterprises. The review examines licensing frameworks, sectoral policies, and other regulations that may create unnecessary barriers to market entry, competition, or investment. The findings will inform potential regulatory reforms aimed at reducing barriers while preserving legitimate policy objectives. The Commission also approved the acquisition of Warner Bros. Discovery by Prince Sub, subject to conditions.

Data governance

International cooperation

The **G7** Data Protection and Privacy Authorities adopted a statement on privacy-preserving age assurance. The statement sets out seven data protection principles for the design and deployment of age assurance mechanisms. The Five Eyes cybersecurity agencies issued a statement on the cyber risks posed by AI. The agencies encouraged the use of AI to strengthen cybersecurity operations and emphasized secure-by-design and secure-by-default principles. They also noted that AI systems may introduce new vulnerabilities, including zero-day vulnerabilities. Finally, the Asia-Pacific data protection authorities, including those of Japan and South Korea, launched a working group on the illegal distribution of personal information.

Europe

In the **European Union**, the Regulation on horizontal cybersecurity requirements for products with digital elements came into force. The Regulation establishes cybersecurity requirements for hardware and software products with digital elements placed on the EU market and sets rules for the designation, notification, and oversight of conformity assessment bodies responsible for assessing compliance. Additionally, the European Data Protection Board opened a consultation on a common template for data breach notifications, and the European Commission signed a Digital Partnership with Brazil covering cross-border data flows, AI, and e-commerce.

At the judicial level, the Court of Justice of the European Union ruled that national courts may use unlawfully collected personal data as evidence subject to data minimization requirements, and clarified that national supervisory authorities may not reject a complaint under Article 77 of the General Data Protection Regulation (GDPR) solely on the ground that judicial proceedings under Article 79 are pending.

At the member-state level, the Spanish and Belgian Data Protection Agencies adopted recommendations for the video game industry on personal data protection and children's rights. The Irish High Court upheld the Data Protection Commission's findings and EUR 530 million fine against TikTok over violations of the GDPR's data transfer provisions, while referring questions on the fining methodology to the Court of Justice of the European Union.

In the **United Kingdom**, the commencement no. 6 and transitional and saving provisions regulations brought into force Section 103 and Schedule 10 of the Data (Use and Access) Act concerning data protection complaints. The provisions establish a statutory right for individuals to submit complaints directly to data controllers and require controllers to provide at least one means of submitting complaints, acknowledge complaints within 30 days, investigate them without undue delay, and notify complainants of the outcome.

The Department for Science, Innovation and Technology (DSIT) adopted the draft Revised Telecommunications Security Code of Practice. The draft updates governance, risk management, and technical security guidance for medium and large public telecommunications providers, reflecting evolving cyber threats and clarifying compliance with statutory security duties. The DSIT also opened a consultation as part of its inquiry into data intermediaries. The consultation seeks views on measures to clarify the role of data intermediaries and improve how data controllers

handle delegated personal data access requests. Additionally, the Information Commissioner's Office released guidance for consumer Internet of Things products and services, and the Office of Communications issued revised network and service resilience guidance for communications providers.

Asia and Australia

In **Australia**, the Cyber Security Centre opened a consultation on the evolution of the Essential Eight cybersecurity framework and published guidance on quantum technology pertaining to sensing with recommended controls including signal validation, hardware provenance checks, and secure development practices. Further, the Information Commissioner closed consultations on the Children's Online Privacy Code and guidance for transparency in automated decision-making. The Information Commissioner also issued guidance on the use of tracking pixels in healthcare provider websites, recommending monitoring of tracking technologies, limiting data collection, obtaining consent, and considering privacy-by-design measures for sensitive or vulnerable-group services. Regarding enforcement, the Information Commissioner ordered Monash and Medmate to cease collecting sensitive information through tracking pixels, and the Privacy Commissioner published a determination against Optus over its failure to protect personal information in a data breach.

In **China**, the National Information Security Standardization Technical Committee opened consultations on national standards on automated tools for data security collection, a zero trust capability maturity model, and a personal information security specification.

The Cyberspace Administration (CAC) and other Ministries adopted the measures for the risk assessment of network data security and adopted security requirements and implementation rules for cybersecurity labeling of consumer-grade connected cameras. Further, the CAC identified 30 mobile applications in violation of personal information protection requirements, including failure to disclose collection and use rules, unnecessary device permission requests, and lack of a valid account cancellation function.

In **Japan**, the Personal Information Protection Commission and the Financial Services Agency closed their consultation on amended guidelines for the protection of personal information in the financial sector. Furthermore, Japan–Singapore memoranda of cooperation on the mutual recognition of IoT cybersecurity labeling schemes came into force, and the Japanese and Philippine data protection authorities signed a memorandum of cooperation on personal data protection and privacy enforcement. Regarding enforcement, the Personal Information Protection Commission published a summary of its monitoring and supervisory activities on personal information handling by digital operators, issuing guidance on cases including unpatched vulnerabilities, exposed databases, unlawful collection of pre-order-completion data for marketing, and unauthorized third-party data sharing.

The **Saudi** Data and Artificial Intelligence Authority issued the Data Monetization Policy, governing the commercialization of data-driven products derived from government-generated data, and structured around seven core principles, including treating data as a national asset, privacy by design, and preventing monopolistic practices.

In **South Korea**, several bills were introduced to the National Assembly to establish victim protection funds under the Personal Information Protection Act and the Network Act, to

consolidate location information obligations with the Personal Information Protection Act, and to set data protection rules for physical AI development.

The Ministry of Science and Information and Communication Technology issued a roadmap for software supply chain security, including supply chain security standards and guidelines, expanded vulnerability reporting through bug bounty, and coordinated vulnerability disclosure frameworks. The Personal Information Protection Commission (PIPC) opened consultations on amendments to the Enforcement Decree of the Personal Information Protection Act covering data protection regulation, authority governance, reporting and certification requirements, and data portability for large-scale employment platforms. The PIPC also issued a revised guide on the right to request the transfer of personal information, blockchain service personal data protection guidelines, and guidance on credential management for cloud services. Additionally, the PIPC signed memoranda of understanding on data protection cooperation with its counterparts in Hong Kong and Singapore.

Regarding **enforcement**, the PIPC fined Coupang KRW 624.7 billion, comprising KRW 423.575 billion in fines for a data breach affecting approximately 37.55 million individuals, caused by negligent management of authentication signing keys and inadequate access controls, and KRW 201.106 billion in fines for the unauthorized collection of third-party online activity records affecting approximately 11.17 million users, with additional violations including failure to notify affected individuals within 72 hours. The PIPC also fined Bithumb KRW 210 million over cross-border data transfer violations and announced an investigation into Tving over an alleged data breach.

Americas

In **Brazil**, the National Data Protection Authority adopted guidelines for the National Personal Data Protection and Privacy Policy and submitted them to the Ministry of Justice and Public Security. Jointly with the Comptroller General of the Union, the Authority consulted on a guide to transparency and the protection of personal data, and closed a consultation on guidance for suppliers of information technology products and services under the Digital Statute of Children and Adolescents.

In **Canada**, the Critical Cyber Systems Protection Act received royal assent. The Act requires designated operators in critical sectors to implement cybersecurity programs, manage supply chain risks, report cybersecurity incidents, and comply with government cybersecurity directions. It also amends the Telecommunications Act to authorise the government to direct telecommunications providers to take measures to secure their networks. The Lawful Access Act (Bill C-22), including provisions on government access to data and cybersecurity regulation, passed its third reading in the House of Commons. The bill expands the powers of police and national security agencies to require telecommunications and electronic service providers to provide digital evidence, user identifiers, and metadata. Additionally, the Protecting Privacy and Consumer Data Act (Bill C-36) was introduced to the House of Commons. The Bill establishes rules on the collection, use, and disclosure of personal information, including consent, data minimization, legitimate interests, privacy management programmes, and breach notification. It also grants individuals rights relating to access, automated decision-making, and data mobility. The bill also includes measures regarding enforcement and cross-border data transfer regulation.

Regarding enforcement, the Office of the Privacy Commissioner found X in breach of the consent and appropriateness requirements of the Personal Information Protection and Electronic Documents Act in relation to the generation of sexualized deepfakes.

Digital Policy Alert

Contact
Written by Tommaso Giardini and Maria Buza
Please send questions and suggestions to maria.buza@sgept.org

The independent Digital Policy Alert is a pillar of the Swiss-based
St. Gallen Endowment for Prosperity Through Trade

St.Gallen Endowment
for Prosperity through Trade