CIPL Comments on the FTC's ANPR on Commercial Surveillance and Data Security

Commercial Surveillance ANPR, R111004

November 21, 2022

I. Executive Summary and Key Recommendations

The Centre for Information Policy Leadership (CIPL)[1] welcomes the opportunity to comment on the Federal Trade Commission's advance notice of proposed rulemaking ("ANPR") on Commercial Surveillance and Data Security.[2]

CIPL has been and continues to be a strong supporter of federal privacy legislation, which ideally would provide organizations with a single federal standard and uniform protections for all Americans. There are legitimate questions about whether the absence of a legislative solution allows for broad-based regulatory action of the type envisioned by the Commission in the ANPR. However, our comments will not address the advisability of the ANPR itself—although we do note that rulemaking may only add to the already complex patchwork of comprehensive state and sector-specific federal laws and regulations. Our comments will focus exclusively on the **substance and nature** of the issues raised, which we place in the public record for purposes of informing whichever public body ultimately advances a federal privacy solution.

CIPL supports **outcomes-based solutions**, which focus on intended results rather than specific practices. An outcomes-based regime would provide organizations with the flexibility to tailor their compliance measures to their unique risks and use cases. Such a regime would also incorporate principles of **organizational accountability**, which go beyond pure legal compliance by incentivizing good data and security practices.

For more than a decade, CIPL has pioneered organizational accountability as a key building block of effective data privacy regulation and its corresponding implementation within companies. Indeed, **CIPL's Accountability Framework**[3] is a recognized standard for the development of best-in-class data privacy practices and organizational compliance programs.

Organizational accountability can be used by companies regardless of sector or size. Its **risk-based framework** provides assurance to government regulators and enforcement bodies that companies are identifying and prioritizing high-risk data processing. It also simplifies investigations and enforcement actions by requiring companies to be able to demonstrate compliance. If the Commission were to more explicitly recognize demonstrated accountability practices and participation in formal accountability schemes such as the APEC (now global) Cross-Border Privacy Rules (CBPR) as a

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators, and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Trade Regulation Rule on Commercial Surveillance and Data Security ANPR, 87 FR 51273.

[3] See CIPL resources and papers on organizational accountability: https://www.informationpolicycentre.com/organizational-accountability.html.

mitigating factor in the enforcement context, the Commission would be incentivizing good data practices that respect and protect consumers' personal information.

Significantly, the broad authority of the Commission to stop "unfair … acts or practices in or affecting commerce"[4] requires a **risk assessment** by both industry and the Commission. The FTC's unfairness authority applies only to practices that cause "substantial" injury to consumers that are "not reasonably avoidable by consumers themselves" and are "not outweighed by countervailing benefits to consumers or to competition."[5] Thus, the **FTC Act itself requires a balancing** of both "injuries" and "benefits" in any assessment of unfairness, providing statutory support for a risk-based model.

A **risk-based approach** would also promote innovation by requiring organizations to identify potential harms to individuals and adopt appropriate protective measures to minimize the risks associated with new uses of consumer data. Any new privacy solution should thus consider recognizing innovative and flexible legal bases (including legitimate interest) that could be used to support a wide range of data uses. Indeed, any proposed privacy regime must provide businesses with **future-proof** legal bases for processing consumer data.

To encourage and test innovative data uses within a regulated context, CIPL supports **regulatory sandboxes**, **policy prototyping**, and other innovative regulatory methods that address data privacy requirements and compliance challenges associated with new technologies and business practices.

CIPL specifically encourages the Commission to **re-evaluate its use of the term "commercial surveillance**." to **re-evaluate its use of the term "commercial surveillance**." As defined in the ANPR, "commercial surveillance" appears to cover many legitimate and necessary data practices. CIPL urges the Commission to refrain from using unnecessarily loaded terms such as "surveillance" and to recognize **appropriate and beneficial data practices**, as confirmed by a proper risk assessment. We strongly urge the Commission to evaluate data use practices in light of their **risks and benefits to both individuals and society**, with due consideration **of how those risks can be effectively managed and minimized**. Any proposed solution should not unduly restrict data-driven innovation or encumber legitimate business practices and data uses whose risks can be mitigated through a range of robust accountability measures.

Lastly, CIPL supports **dialogue and cooperation** not only with key stakeholders (consumers and industry), but also with other agencies and enforcement authorities that address privacy and data security issues. We encourage the Commission to understand the current regulatory landscape both within the U.S. and beyond to improve consistency across jurisdictions, to work toward a uniform set of protections for consumers, and to minimize regulatory overlap for businesses.

In sum, while there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR, we offer the following points to help frame the discussion on the substance and nature of the issues raised.

[4] 15 U.S.C. §45(a)(1).

[5] 15 U.S.C.§45(n).

Any potential action addressing comprehensive privacy measures should strive for an **outcomes-based approach** that:

- promotes effective, targeted protections for consumers;
- enables innovative and responsible data uses;
- provides businesses with robust, flexible, and future-proof legal bases for processing consumer data, including legitimate interests;
- incorporates accountability-based practices that include **risk assessments**;
- acknowledges that risk is inherent in any use of consumer data;
- recognizes that risk mitigation does not mean the elimination of risk, but rather the reduction of risk to the extent practicable;
- indicates that companies are best placed to understand the risks raised by their own processing activities, and, therefore, are best placed to identify and implement appropriate mitigation measures;
- endorses **contextual** risk assessments so that companies may:
  - tailor their compliance measures to their unique risks and use cases;
  - evaluate the sensitivity of data and the attendant level of risk in context;
  - identify and prioritize high-risk processing;
  - identify legitimate and beneficial uses of data;
  - evaluate individual, organizational, and societal benefits;
  - identify appropriate mitigations for a given context and a given use;
  - document their compliance and be able to explain and defend their processing decisions under relevant legal standards, such as “unfairness”;
- does not unnecessarily encumber legitimate business practices or thwart data-driven innovation;
- supports Privacy Enhancing Technologies (PETs) and Privacy Preserving Technologies (PPTs);
- provides guidance on appropriate risk criteria, frameworks, and methodologies; and
- is drafted after engagement and discussions with stakeholders.

II. Responses to Specific Questions

A. Harm to consumers

Q2. Which measures do companies use to protect consumer data?

Companies employ a wide range of data protection measures—including but not limited to privacy policies; notice-and-consent options; data minimization, retention, and destruction protocols; impact assessments; privacy by design methodologies; vendor due diligence; employee training programs; information security controls; and data transfer principles—all of which are typically grounded in an **accountability-based data privacy management program (DPMP)**.

As mentioned in the Executive Summary, CIPL has pioneered organizational accountability as a key building block of effective data privacy regulation and its corresponding implementation within companies through comprehensive DPMPs. **CIPL's Accountability Framework**[6] is a recognized standard for the development of best-in-class data privacy practices and organizational compliance programs. A growing number of CIPL member organizations are implementing accountability-based DPMPs that align with CIPL's Accountability Framework.[7] FTC Commissioner Christine Wilson highlighted CIPL's Accountability Framework as an "excellent visual framework for businesses to design privacy programs" in a speech delivered in May 2020.[8] Notably, CIPL's Accountability Framework is consistent with privacy management programs the FTC has required of organizations in its consent orders.[9] The Framework prompts organizations to adopt specific measures that implement applicable privacy legal requirements, and it helps them to demonstrate the existence and effectiveness of such measures both internally and externally upon request.

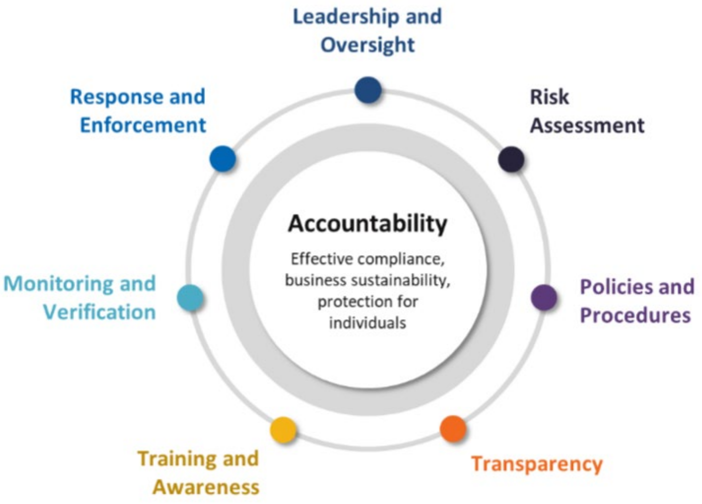
The core elements of CIPL's Accountability Framework are displayed in the image below:

[6] *Supra,* note 3.

[7] *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework,* Report of the CIPL Accountability Mapping Project, May 2020, available at https://www.informationpolicycentre.com/cipl-2020-accountability-mapping-report.html; filed herewith as Exhibit 6.

[8] Keynote Remarks of Commissioner Christine S. Wilson at the Privacy + Security Academy, May 7, 2020, available at https://www.ftc.gov/news-events/news/speeches/keynote-remarks-commissioner-christine-s-wilson-privacy-security-academy.

[9] *Organizational Accountability in Light of FTC Consent Orders,* CIPL Discussion Paper, November 13, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf; filed herewith as Exhibit 8.



The CIPL Accountability Framework

The specific elements of accountability—leadership and oversight; risk assessment; policies and procedures; transparency; training and awareness; monitoring and verification; and response and enforcement—are drawn from similar elements in other regulatory areas, which makes the framework law-agnostic. These elements are consistent with other areas of corporate law and compliance, including anti-bribery, anti-money laundering, export control and competition—making them familiar to corporate leaders.[10] Organizations, regulators, and courts have used these same elements to determine if an organization has maintained an effective and comprehensive compliance program in any given regulatory area.

CIPL's Accountability Framework requires companies to take concrete steps to operationalize all aspects of data governance, privacy law compliance, and the data cycle—from collection and generation, to use, sharing, storing, and deletion. Because a key element of accountability is the **risk assessment**, accountability focuses on, and prioritizes, the mitigation of data processing risks to individuals. This approach enables organizations to implement legal rules and privacy protections more precisely and effectively. Thus, accountability is an effective alternative to overly granular and rigid legal requirements that apply across the board regardless of the risks involved.

Specifically, organizational accountability requires companies to:

- **Establish leadership and oversight for data protection and the responsible use of data**, including governance, reporting, buy-in from all levels of management, and appropriate personnel to oversee the organization's accountability program and report to management and the board.

[10] See CIPL White Paper: *The Concept of "Organizational Accountability" Existence in US Regulatory Compliance and its Relevance for a Federal Data Privacy Law*, July 3, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_-_existence_in_us_regulatory_compliance_and_its_relevance_for_a_federal_data_privacy_law__3_july_2019_.pdf; filed herewith as Exhibit 9.

- **Assess and mitigate the risks** that data collection and processing may raise to individuals, including weighing the risk of the information use against its benefits. Risk assessment also means conducting periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology, and other factors, and adapting the program to changing levels of risk.
- **Establish internal written policies and procedures** that operationalize privacy and security legal requirements, create concrete processes and controls to be followed by the organization, and reflect applicable law, regulations, industry standards, as well as the organization's internal policies and ethical values.
- **Provide transparency to all stakeholders internally and externally** about the organization's data privacy program, procedures and protections, the rights of individuals in relation to their data, and the benefits and/or potential risks of data processing. This may also include communicating with relevant data privacy authorities, business partners, and third parties.
- **Provide training for employees to ensure** awareness of the internal privacy program, its objectives and requirements, and the implementation of its requirements in line with employees' roles and job responsibilities. This ensures that data privacy is embedded in the culture of the organization so that it becomes a shared responsibility.
- **Monitor and verify the implementation and effectiveness of the program and internal compliance** with the overall privacy program, policies, procedures, and controls through regular internal or external audits and redress plans.
- **Implement response and internal enforcement procedures** to address inquiries, complaints, data breaches, internal non-compliance, and to otherwise enforce compliance.

There is no "one-size-fits-all" formula for implementing and demonstrating accountability, but any potential law or regulation should allow flexibility for organizations to build, implement, and demonstrate their accountability frameworks.

In addition to an accountability framework such as the one pioneered by CIPL, companies may use NIST's Privacy Framework,[11] ISO standards,[12] codes of conduct, and privacy certifications to protect consumer data.

Moreover, organizations are increasingly looking to **Privacy Enhancing Technologies (PETs)** and **Privacy Preserving Technologies (PPTs)** to protect consumer data. PETs and PPTs can play an extremely important role in mitigating privacy risks while enabling beneficial data uses and data-driven innovation.

PETs and PPTs take different forms and have different use cases, but generally they refer to a range of technologies that help protect personal privacy.

Some common examples include:

- **Synthetic Data**: Artificial data that computer simulations or algorithms generate as an alternative to real-world data.

[11] The NIST Privacy Framework is available at https://www.nist.gov/privacy-framework.

[12] See, in particular, ISO/IEC 27701, available at https://www.iso.org/standard/71670.html.

- **Homomorphic Encryption**: Cryptographic methods that allow mathematical operations on data to be carried out on cipher text, instead of on plain text, that yield the same result.
- **Differential Privacy**: A system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset.
- **Secure Multi-Party Computation**: A cryptographic protocol that distributes a computation across multiple parties where no individual party can see the other parties' data.
- **Federated Learning**: A technique to train a machine learning model on local device user data without the need to transfer that data to a central location.

No single technique has yet been identified as the best model, but research shows that all of these technologies have a positive impact on privacy-compliant data analytics, which in turn will help increase companies' ability to unlock the potential of available data in a safe and accountable manner as they pursue data-driven innovation.

Of course, PETs/PPTs are not a silver bullet and will always have to be considered in combination with other mitigation measures. As with other technologies and uses of data, organizations should be held accountable for their use of PETs/PPTs. Thus, companies must deploy technical and organizational measures to ensure and demonstrate the appropriateness of these methodologies.

To ensure the effectiveness and trustworthiness of PETs/PPTs, legislators and regulators should encourage vendors in the space to consider the "explainability" of their technologies from the earliest stages of development, just as Privacy by Design requires engagement of privacy principles from day-one of product development. Vendors could, for example, build dashboards or reporting capabilities with appropriate explanations of how a tool was deployed, how risks of re-identification or singling-out were minimized, and which risk thresholds were used based on the intended use case, release model, and aggregation level of the output.

Companies using PETs/PPTs should also be required to demonstrate that they have made appropriate investments in their controls and auditing, which may include the retention of privacy counsel, privacy engineers, and auditors with expertise in the area.

Finally, CIPL encourages the Commission to stay actively involved in the global conversation surrounding PETs/PPTs, given that rapid advancements in the technology are expected in the next few years. Academic and commercial research into PETs/PPTs may favor certain technologies over others or may demonstrate that certain use cases are lower- or higher-risk than others. Continued engagement in this area will encourage research and innovation tailored to legislative/regulatory interests and concerns.[13]

[13] For example, on Sept. 7, 2022, the U.K.'s Information Commissioner's Office (ICO) published draft guidance on PETs, as noted in a press release available at https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/. The press release further notes that U.K. and U.S. governments "have launched a set of prize challenges to unleash the potential of PETs to tackle combat global societal challenges ….".

Q3. Which of these measures or practices are prevalent? Are some practices more prevalent in some sectors than in others?

Accountability measures and practices are prevalent in organizations that have adopted an accountability-based data privacy compliance framework, such as CIPL's Accountability Framework, which can be used by organizations regardless of sector or size. Principles of organizational accountability are often incorporated into outcomes-based laws and regulations,[14] which provide organizations with flexibility to tailor their compliance measures and practices to their unique risks and use cases. Within an outcomes-based regime, the specific practices employed will vary from company to company.

CIPL's **Accountability Mapping Project**[15] consisted of interviews and document reviews of mature data privacy management programs (DPMPs) of 17 organizations in various sectors, sizes, and regions. The main goals of this research were to understand how these organizations build and implement effective data privacy practices, and how these practices map to the CIPL Accountability Framework.

In the white paper published in May 2020,[16] CIPL identified common trends concerning accountability, most notably:

- **Organizations proactively manage privacy risks and adopt risk-based approaches to DPMPs.** Participating organizations built and implemented their DPMPs by taking into account the risk of their processing operations to individuals, as well as the risks to their organizations. Risk management enables them to prioritize their accountability measures and make their programs more effective in practice.
- **Organizations view accountability as a journey and an internal change management process.** In order to embed data privacy in the company DNA, participating organizations recognized that accountability is not a one-off project that gets delivered once and then forgotten about; rather, it is an ongoing endeavor driven by continuous risk assessments and constant improvements. Implementing an accountable DPMP is an iterative and dynamic process that requires organizations to adapt constantly to internal and external factors; address regulatory, legal, and technological change; and mitigate new risks. Even the most mature DPMPs must undergo constant and ongoing adaptation and improvements.
- **Accountability is sector agnostic and scalable.** Our mapping exercise revealed that organizations of all types, sizes, sectors (including the public sector), geographical footprints, and cultures can develop and implement an accountable DPMP. However, the particular

[14] See, for example, the Dubai International Financial Centre (DIFC) Law No. 5 of 2020, available at https://www.difc.ae/business/laws-regulations/legal-database/data-protection-law-difc-law-no-5-2020/. See also the proposed Canadian Consumer Privacy Protection Act (part of the draft "Digital Charter Implementation Act, 2022"), introduced in the House of Commons as Bill C-27 on 16 June 2022. is the first of three statutes included in the draft "Digital Charter Implementation Act, 2022," available at https://www.parl.ca/LegisInfo/en/bill/44-1/c-27.

[15] See CIPL, Organizational Accountability, available at https://www.informationpolicycentre.com/organizational-accountability.html.

[16] *Supra*, note 7.

program, the specific activities (policies, procedures, controls, and tools), and the human and financial resources will be different, as appropriate to the specific context, risks, goals, and size of each organization. In particular, while smaller organizations can and do take steps to be accountable, they calibrate measures differently (sometimes with more agility) than do larger, multinational organizations. But the overall accountability architecture, as suggested by the CIPL Accountability Framework, remains the same, irrespective of industry sector and size.

- **Both controllers and processors implement accountability.** Participating organizations included both controllers (i.e., those determining the collection and use of personal data) and processors (i.e., third-party service providers). Our findings confirmed that accountability practices are not limited to controllers. Indeed, many processors, especially the large ones, implement DPMPs to ensure that their clients' data (i.e., the data received from controllers) is managed in accordance with contractual and legal privacy and data security requirements.

Generally speaking, those sectors with a significant history of privacy-related regulation (such as the financial and health sectors) have more mature DPMPs than other sectors. Similarly, multinational companies tend to have more developed privacy programs, due in large part to the impact of the European Union's General Data Protection Regulation (GDPR), Brazil's *Lei Geral de Proteção de Dados* (LGPD), and other international data protection laws. And since the enactment of the California Consumer Privacy Act, business-to-consumer companies in the U.S. are generally more attuned to DPMPs than are B2B companies.

It is important to note that DPMPs are more than just legal compliance tools. Empirical research demonstrates that business interests and privacy interests align around organizational accountability. Cisco's Data Privacy Benchmark Study 2020 found "strong correlations between organizations' privacy accountability and lower breach costs, shorter sales delays, and higher financial returns."[17] Notably, the CISCO study found the average ratio of benefits-to-spend was 2.7, meaning that for every dollar of privacy investment, the company received $2.70 worth of benefit.[18]

Further, CISCO's 2021 Data Privacy Benchmark Study[19] found that external privacy certifications (e.g., ISO 27701, APEC Cross-Border Privacy Rules, and EU Binding Corporate Rules), all of which are formal accountability schemes, are an important buying factor for 90% of organizations when choosing a product or vendor.

Finally, in CIPL's forthcoming joint white paper with CISCO, we explore new empirical data on the business benefits and return-on-investment of DPMPs. This paper will show that organizations are experiencing a wide range of benefits from investing in DPMPs, including risk management,

[17] *From Privacy to Profit: Achieving Positive Returns on Privacy Investments*, Cisco Data Privacy Benchmark Study 2020, https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf.

[18] *Id.*, at 5.

[19] *Forged by the Pandemic: The Age of Privacy*, CISCO's 2021 Data Privacy Benchmark Study. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2021.pdf.

compliance benefits and the ability to provide trust to external stakeholders, including customers, investors, and regulators. Specifically, the study found:

- The majority of organizations are using a variety of privacy maturity models to implement accountability: the CIPL Accountability Framework, ISO standards, Generally Accepted Privacy Principles, the NIST Privacy Framework, and the Privacy Shield Framework (now known as the EU-U.S. Data Privacy Framework[20]), among others.
- Sixty-six percent of CIPL members who participated in this study experienced at least $1 million in benefits from investing in privacy over the past year. Twenty-seven percent experienced over $10 million in benefits.
- Risk and compliance benefits—such as avoiding regulatory scrutiny and fines, experiencing fewer breaches, and avoiding damage to reputation—are currently the most immediate benefits from implementing a DPMP, but organizations are also realizing greater agility, growing innovation, increased efficiencies, and elevated interest from investors.
- While legal, compliance, and data security concerns have served as traditional drivers for the implementation of DPMPs, there is increasing recognition that they enable broader innovative uses of data, serve as a competitive edge, and boost consumer trust and confidence in businesses' responsible use of data.

Upon its anticipated publication in December 2022, CIPL will share this report with the Commission.

Finally, as noted in the first bullet above, many organizations engaging in cross-border data flows have specifically implemented measures and practices in accordance with the Privacy Shield Framework (a.k.a. the EU-U.S. Data Privacy Framework).[21] These certifications have been instrumental in developing privacy practices and controls with regard to EU data transferred to the U.S. Over time, some certified organizations have extended these practices and controls to non-EU data, as it has become more difficult to compartmentalize data within a business and apply different rules to different data co-mingled in the system. In that respect, the Privacy Shield Framework has had a positive impact on building a data privacy culture in the U.S., notwithstanding the lack of a federal data privacy law.

Q7. How should the Commission identify and evaluate these commercial surveillance harms or potential harms? On which evidence or measures should the Commission rely to substantiate its claims of harm or risk of harm?

Before addressing potential harms from so-called "commercial surveillance," CIPL encourages the Commission to re-evaluate its use of the term "commercial surveillance." According to the ANPR, "commercial surveillance" refers to "the collection, aggregation, analysis, retention, transfer, or

[20] See *President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework*, October 7, 2022, available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

[21] *Id.* For additional information on the Privacy Shield, see the International Trade Administration's website, available at https://www.privacyshield.gov/welcome.

monetization of consumer data and the direct derivatives of that information."[22] As noted in the Dissenting Statement of (now former) Commissioner Noah Joshua Phillips, the term is defined "so broadly (and with such foreboding) that it captures any collection or use of consumer data."[23] In addition to its broad sweep—which appears to cover many legitimate and necessary data practices—the use of the term "surveillance" in the commercial context carries an inappropriately negative connotation that should be reserved for nefarious data practices.

There are many use cases and examples of **legitimate data practices**—indeed, practices essential in the context of the digital economy and society—that could fall within the term "surveillance" as used in the ANPR. We identify 11 use cases below. Any potential action should take these and other practices into consideration.

- **Use Case #1: Use of Consumer Data in Fraud and Identity Theft Prevention**

  Collection and use of consumer data can be of significant benefit in fraud and identity theft protection.

  The Federal Trade Commission's Consumer Sentinel Network (CSN)[24] took in over 5.7 million reports in 2021, of which 49 percent were for fraud, and 25 percent for identity theft. CSN's 2021 Data Book indicates that consumers reported losing more than $5.8 billion to fraud in 2021 – an increase of $2.4 billion over 2020.

  Relatedly, a survey conducted by Aite-Novarica[25] notes that identity theft typically occurs in one of two ways: (1) an unauthorized party uses a victim's personal information to apply for a financial account, loan, or some type of benefit (e.g., Medicare), or (2) an existing account or benefit (e.g., medical insurance, rewards for a hotel or airline) owned by the victim is accessed or used by an unauthorized person.

  In order to improve the accuracy of fraud detection, leading organizations must use AI and machine-learning algorithms powered with "all available data."[26] Indeed, the need for data is vital to businesses' ability to identify and address fraudulent practices. As McKinsey reports in

[22] NPRM, 87 FR 51273, at 51277.

[23] *Id.*, at 51294 (emphasis added; footnotes omitted).

[24] Consumer Sentinel Network Data Book 2021, available at https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf.

[25] *U.S. Identity Theft in 2021: Adapting and Evolving*, Aite-Novarica, June 2022, available at https://giact.com/identity/us-identity-theft-adapting-and-evolving-report/.

[26] *A new approach to fighting fraud while enhancing customer experience*, McKinsey & Co., November 8, 2022, available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience.

a recent article,[27] companies need a "technology-enabled solution and multidisciplinary approach" incorporating data from both internal and external sources:

> Internal data, which should be combined across product silos, could be related to fraud, identification, transactions, account and customer profiles, and connected interactions across channels. External sources could include device, biometric, transaction, and social data. The model should also be updated to include new value-added data sources continually. Additionally, it requires an orchestration layer that integrates different systems and allows fraud management teams to think across the value chain, capture complex fraud patterns, and identify fraud earlier. It should also enable them to orchestrate the response and communication to customers so team members can handle the experience in a personalized and empathic way.[28]

Large, multi-country data sets supported by AI models provide insights on authentication patterns that can help reduce fraudulent transaction risks.[29] AI has proven to be extremely valuable in this context, but it relies heavily on large data sets, as fraudsters will use similar methods from one country to another and then attempt to take them globally. While human logic would be slower or possibly unable to identify such complex patterns in the first place, AI makes this process more efficient and effective. As a result, when a new authentication request comes in, the models immediately attribute a risk score and reason code to each payment transaction.

- **Use Case #2. Creation and/or Use of Watch Lists to Meet Anti-Money Laundering (AML), Politically Exposed Persons (PEP), Anti-Fraud, or Diligence Obligations**

To protect the international financial system, financial institutions must screen new and existing customers or vendors against watch lists to determine if a business relationship might result in financial risk or crime. Watch lists include personal data that is publicly available or extracted from sanctions published by national or international organizations.

Financial institutions and society, in general, have a legitimate interest in preventing and combating money laundering, and ensuring the stability of the financial system. Organizations that perform checks against the officially published watch lists and conduct the screening activities have a legitimate interest in processing the data of the individuals on the lists.

Moreover, individual cardholders expect their payment transactions to be processed in an efficient, safe, and secure way. Individuals also reasonably expect that organizations process

[27] *Four key capabilities to strengthen a fraud management system*, McKinsey & Co., November 8, 2022, available at https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/four-key-capabilities-to-strengthen-a-fraud-management-system.

[28] *Id.*

[29] See *Fraud Detection and Prevention: A Synopsis of Artificial Intelligence Intervention in Financial Services Smart Card Systems*, Solomon Lawal, September 23, 2021, available at https://ssrn.com/abstract=4117507.

their personal data for the purpose of meeting regulatory requirements, such as in relation to AML, according to market standards.

- **Use Case #3. Processing of Internet Protocol (IP) Addresses for Delivery of Online Content and Security**

  IP addresses are used to deliver web pages and content, for cybersecurity purposes, and to measure website traffic. Internet Service Providers (ISPs) have information linking IP addresses to individual subscribers in order to provide services such as technical support, fraud prevention, and billing.

  ISPs have a legitimate interest in processing IP addresses linked to the routine performance of their services. Internet content owners and users have a legitimate interest in having content and services protected from bad actors.

- **Use Case #4. Processing of Personal Data Received in the Context of an Employee Investigation or Disciplinary Process**

  In some cases, organizations need to process personal data of individuals who are not their employees in the context of an employee investigation or disciplinary process—e.g., text messages exchanged by an employee with another individual outside of work which may violate an employer policy.

  The employer has a legitimate interest to uphold its business policies, to ensure that any breaches of its policies are appropriately investigated, to investigate alleged breaches of the law, to protect its employees, and to protect its products and brand reputation.

  Society has a legitimate interest in the prevention and detection of crimes.

- **Use Case #5. Business-to-Business CRM in the Healthcare Sector**

  In the pharmaceutical sector, business-to-business customer relationship management (CRM) activities include documenting face-to-face visits with health care professionals (HCPs), providing scientific and promotional information to HCPs about medicines that can help their patients, and inviting them to attend events. To do so, the company may process some of the HCP's personal data. It may also combine data directly obtained from the HCPs with publicly available data taken from medical societies' websites, hospitals' websites or medical publications. Pharmaceutical companies may classify data stored in their CRMs into pre-determined categories and use such data to identify specific actions that the company should take with respect to these categories, such as sending timely informational emails about the efficacy of certain medicines, which may help HCPs when treating patients.

  Pharmaceutical companies have a legitimate interest in processing data for CRM purposes in order to facilitate their business. HCPs have a legitimate interest in obtaining information from pharma companies about new diseases and available treatments. Patients of HCPs (third parties) have a legitimate interest in having access to the most efficient treatment and medicines.

- **Use Case #6. Measuring Customers' Satisfaction**

Measuring consumers' satisfaction on a product or service provides high value to businesses and is seen as a key performance indicator. In a competitive marketplace, customer satisfaction is considered a key differentiator.

Companies have a legitimate interest to ask their customers for their opinions, and to contact them for the purpose of conducting surveys (in product or by other means such as emails) to measure their satisfaction with a product or service. Other customers have a legitimate interest to receive products or services that have been improved on the basis of feedback provided to the provider.

The severity and likelihood of risk of harm is very low for the customer. The data processed is limited and customers can freely decide whether to respond to surveys and share additional personal data. Customers have reasonable expectations that they may be contacted for the purpose of providing their level of satisfaction with a product or a service's performance. Customers may have a self-interest to provide feedback (e.g., on the interface or functionality of a certain service so that it is improved).

- **Use Case #7. Use of CCTV for Security Purposes**

  Use of security cameras is a common practice. This may involve monitoring employees.

  Organizations have a legitimate interest in securing their premises. Employees and customers have a legitimate interest in having their physical safety protected. Society has a legitimate interest in the prevention and detection of crime.

  Employees have reasonable expectations that their privacy will not be intruded upon disproportionately by the installation of CCTV. Employees may also expect employee monitoring to take place where employment laws allow for it.

- **Use Case #8. Processing of Data in Relation to Merger and Acquisition (M&A) Transactions**

  M&A transactions may require the potential acquirer and their advisors (lawyers, IT consultants, financial auditors) to review various types of documentation containing personal data of various individuals in order to determine the initial and final scope of the subject-matter of the acquisition.

  Controllers have a legitimate interest to process personal data in the context of M&A transactions to ensure that they have an accurate and thorough understanding of the risks, scope, and purpose of the transaction.

  Individuals involved reasonably expect their personal data to be processed as this is in line with market practice.

- **Use Case #9. Imagery Collection to Improve Mapping Applications**

  Mapping applications offer users digital and navigable representations that enable them to enjoy a reliable navigation experience. To provide state-of-the-art applications, a service provider needs to collect the necessary imagery that enables it to reproduce accurate representations of physical environments, including multi-dimensional representations of streets and buildings. Imagery may be collected through, for example, vehicles and dedicated personnel tasked with collecting GPS traces (e.g., heading, latitude, longitude of road networks), still images (e.g., traffic signs, lane markings and speed limits), and other information based on radio signals that help identify the projected dimensions of building and other structures for multi-dimensional representation. The data collection is focused on stationary objects, but it may unavoidably capture items that could be classified as personal data, such as still images of individuals and vehicle license plates.

Mapping application service providers have a legitimate interest in building and making improvements to offer the best product and user experience. To achieve this goal, the service provider needs to build the necessary mapping data to take advantage of innovation, to ensure the quality of the data, and to allow the service provider to ensure the best privacy experience to meet its user's expectations.

- **Use Case #10. Using Real-World Customer Data and Machine-Learning to Improve Digital Voice Assistant Services**

The core function of a digital voice assistant is to accurately recognize and respond to customers' spoken requests. Some organizations use supervised machine-learning involving processing of real-world customer voice data to maintain and improve such services.[30] In these cases, a service provider may manually review a small fraction of customers' voice data, annotate the data, and use the annotated data to train a machine-learning model to correctly respond to a voice input and to ensure that the service works well for all customers.

Traditional computation methods relying on hard-coded logic are unable to accurately understand and respond to the varied, dynamic speech used by customers in the real world. Supervised machine-learning using real-world customer voice data is state-of-the-art for making service improvements and new features possible for digital voice assistants such as improving the ability to "wake up" only when invoked, understand and respond to new types of requests (such as COVID-19 or digital certificates), play new music content, recognize innovative new smart home devices, and understand all users equally well.

Using real-world customers' voice data also makes some of these services commercially viable. For example, expanding to new languages would be extremely costly to customers if digital voice assistants could not learn and improve from real-world customer use. Customers would suffer from less usability, diminished improvement, fewer features, and fewer service options if service providers could not train digital voice assistants using real-world customer data.

Digital voice assistant service providers have a legitimate interest in maintaining their service, and making improvements and service developments that meet users' expectations, such as improving the general accuracy of their services, improving existing features, accommodating population-based differences in speech and language, and developing new service features. This also benefits third parties and society more generally.

[30] Note that this case study does not apply to digital voice assistants that do not process personal data (e.g., that anonymize data at the outset).

- **Use Case #11. Research and Development Activities Aimed at Training and Prototyping Machine-Learning Algorithms**

  Training and prototyping machine-learning algorithms can help organizations create more user-friendly software applications. Machine-learning technology supports improvement in areas such as task automation or contextual searches. The ultimate goal is to provide users with an optimized and more powerful user experience. In most cases, the data will have been collected for other purposes and, therefore, further processed for the purpose of training and prototyping machine-learning algorithms. In these cases, organizations may have to include a compatibility test in the legitimate interests assessment in order to determine whether they can lawfully further process such personal data in that particular context.

  Organizations have a legitimate interest in processing aggregated datasets for the purpose of training and prototyping machine learning algorithms, as they want to ensure that their customers have access to new technologies that facilitate and improve user experience.

  Individuals also have a legitimate interest in such data processing given that they will benefit from improved services.

Additional use cases are set forth in CIPL's White Paper on Legitimate Interests,[31] which we incorporate by reference. But, of course, beneficial uses of data are potentially limitless. Consider, for example:

- **Use of data for task allocation.** An organization may choose to use an AI-based task allocation system to distribute tasks amongst a group of volunteers for charity work (e.g., in the context of COVID-19) or short-term assignments (e.g., in another department or region) based on the volunteers' respective skills. Such a use matches up relevant skillsets and interests with relevant volunteering activities or short-term assignments.
- **Use of data for a safer internet.** Tech companies like Google,[32] Apple,[33] and Meta[34] issue transparency reports that highlight uses of data to facilitate a safer internet for users, such

[31] CIPL White Paper: *How the Legitimate Interests Ground for Processing Enables Responsible Data Use and Innovation*, July 1, 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_how_the_legitimate_interests_ground_for_processing_enables_responsible_data_use_and_innovation__1_july_2021_.pdf; filed herewith as Exhibit 4.

[32] Google Transparency Report, available at https://transparencyreport.google.com/?hl=en.

[33] Apple Transparency Report, available at https://www.apple.com/legal/transparency/.

[34] Meta Transparency Report, available at https://transparency.fb.com/data/.

as Google Safe Browsing,[35] Email encryption in transit,[36] HTPPS encryption on the web,[37] Android ecosystem security,[38] and Combating Child Sexual Abuse Material.[39]

- **Use of data in urban planning**. Insights based on anonymized and aggregated spending data have helped with challenges faced by low-income communities by offering a more detailed, nearly real-time glimpse into not just what communities spend their money on, but *where* they spend. This aids public- and private-sector entities to ensure investments meet local needs and lower the cost of living.
- **Use of data to support disaster relief efforts**. Data can show changes in consumption patterns following a natural disaster, such as greater spending for medical services, thereby offering a picture of what communities need in the aftermath of severe weather.
- **Use of data for economic recovery.** Data insights helped governments and other key market stakeholders minimize the impact of the COVID-19 pandemic and boost economic recovery.
- **Use of data for refugee housing.** Polish officials used data insights to support the economic inclusion and housing of Ukrainian refugees.
- **Use of data to address demographic challenges.** Local governments and small businesses can use data to prevent displacement in gentrifying communities, to mitigate depopulation and community decline, and to encourage inclusive growth.

Moreover, the FTC itself has highlighted beneficial uses of data in a 2016 report,[40] which noted that big data is being used to:

- increase educational attainment for individual students;
- provide access to credit using non-traditional methods;
- provide healthcare tailored to individual patients' characteristics;
- provide specialized healthcare to underserved communities; and
- increase equal access to employment.

In sum, before identifying and evaluating alleged "harms" from so-called "commercial surveillance," the Commission should recognize that many uses of data can benefit both consumers and society. Such practices should be encouraged and supported—not labeled with a derogatory term like

[35] *Google Safe Browsing*, available at https://transparencyreport.google.com/safe-browsing/overview?hl=en.

[36] *Email encryption in transit*, available at https://transparencyreport.google.com/safer-email/overview?hl=en.

[37] *HTTPS encryption on the web*, available at https://transparencyreport.google.com/https/overview?hl=en.

[38] *Android ecosystem security*, available at https://transparencyreport.google.com/android-security/overview?hl=en.

[39] *Combating Child Sexual Abuse Material*, available at https://transparencyreport.google.com/child-sexual-abuse-material/reporting?hl=en.

[40] *Big Data: A tool for inclusion or exclusion? Understanding the Issues*, FTC Report, January 2016, available at https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

"surveillance." Moreover, CIPL cautions that any wholesale restriction of uses by organizations that do not collect data directly from consumers can inadvertently prohibit legitimate and necessary uses.

Consequently, in order to support legitimate business uses and encourage data-driven innovation, data use practices should be evaluated in light of the **risks and benefits to both individuals and society**, with due consideration of **how risks can be effectively managed and minimized**.

Significantly, the broad authority of the Commission to stop "unfair … acts or practices in or affecting commerce"[41] requires a **risk assessment** by both industry and the Commission. The FTC's unfairness authority applies only to practices that cause "substantial" injury to consumers that are "not reasonably avoidable by consumers themselves" and are "not outweighed by countervailing benefits to consumers or to competition."[42] Thus, the **FTC Act itself requires a balancing** of both "injuries" and "benefits" in any assessment of unfairness, providing statutory support for a risk-based model.

The best way to promote such a balancing would be through **dialogue and engagement** not only with key stakeholders (consumers and industry), but also with other agencies and enforcement authorities that address privacy and data security issues. All affected parties need to come to a consensus about the **risks** and **harms** that must be considered and mitigated to clarify consumer expectations and business responsibilities.

In an effort to build consensus around the importance of and the key elements of privacy risk assessments, CIPL initiated a **Privacy Risk Framework Project** that, among other things, sought to create a practical blueprint for businesses to implement principle-based privacy obligations by identifying, prioritizing, and mitigating privacy risks.[43] Thus, one component of the project was to seek consensus on what is meant by privacy risks to individuals and society. This resulted in the creation of two possible risk matrices (or approaches) to a risk assessment methodology that set out a range of risks, harms, or threats that must be evaluated in terms of their **likelihood** to materialize and their **seriousness** (or severity) if materialized. We also highlighted the importance of weighing the benefits of a proposed data use in the context of a risk assessment.

The two draft risk matrices annexed to CIPL's white paper are reproduced below.[44]

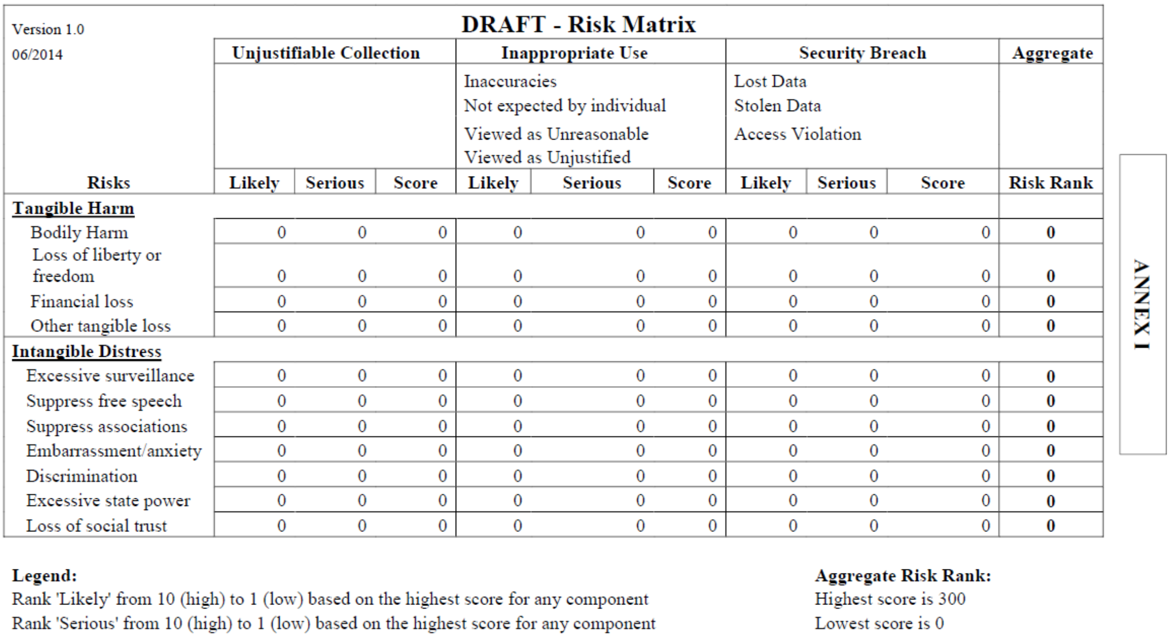
[41] 15 U.S.C. §45(a)(1).

[42] 15 U.S.C.§45(n).

[43] CIPL White Paper: *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, June 19, 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf; filed herewith as Exhibit 18.

[44] *Supra*, note 43.

Draft Risk Matrix: Option 1



DRAFT - Risk Matrix

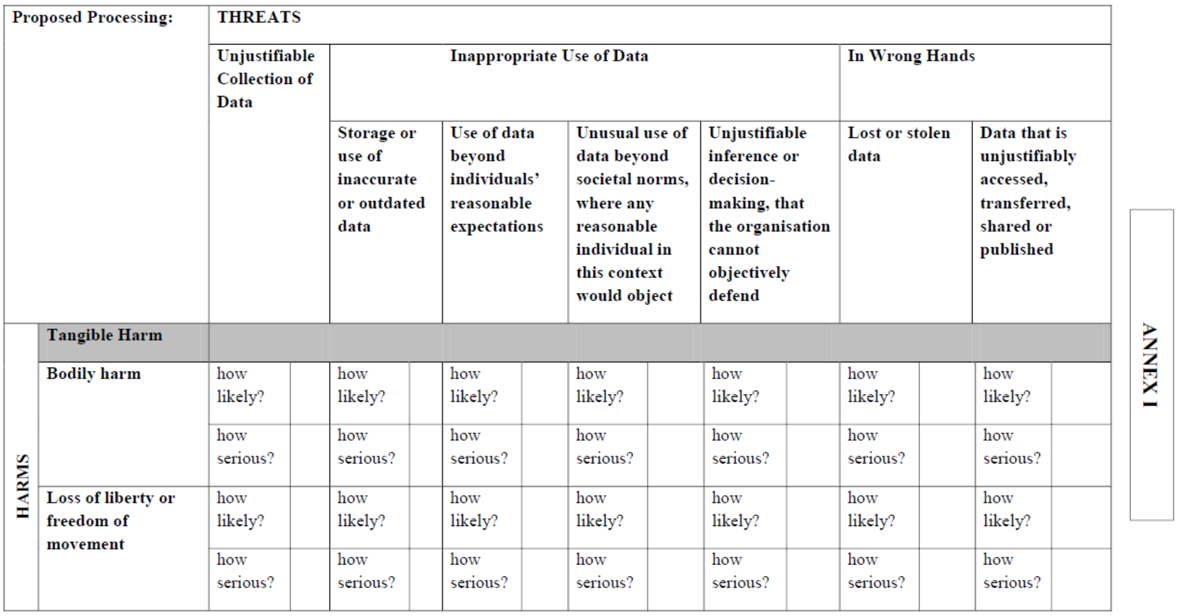
Version 1.0 06/2014	Unjustifiable Collection			Inappropriate Use			Security Breach			Aggregate
				Inaccuracies Not expected by individual Viewed as Unreasonable Viewed as Unjustified			Lost Data Stolen Data Access Violation			
Risks	**Likely**	**Serious**	**Score**	**Likely**	**Serious**	**Score**	**Likely**	**Serious**	**Score**	**Risk Rank**
Tangible Harm										
Bodily Harm	0	0	0	0	0	0	0	0	0	**0**
Loss of liberty or freedom	0	0	0	0	0	0	0	0	0	**0**
Financial loss	0	0	0	0	0	0	0	0	0	**0**
Other tangible loss	0	0	0	0	0	0	0	0	0	**0**
Intangible Distress										
Excessive surveillance	0	0	0	0	0	0	0	0	0	**0**
Suppress free speech	0	0	0	0	0	0	0	0	0	**0**
Suppress associations	0	0	0	0	0	0	0	0	0	**0**
Embarrassment/anxiety	0	0	0	0	0	0	0	0	0	**0**
Discrimination	0	0	0	0	0	0	0	0	0	**0**
Excessive state power	0	0	0	0	0	0	0	0	0	**0**
Loss of social trust	0	0	0	0	0	0	0	0	0	**0**

ANNEX I

Legend:
Rank 'Likely' from 10 (high) to 1 (low) based on the highest score for any component
Rank 'Serious' from 10 (high) to 1 (low) based on the highest score for any component

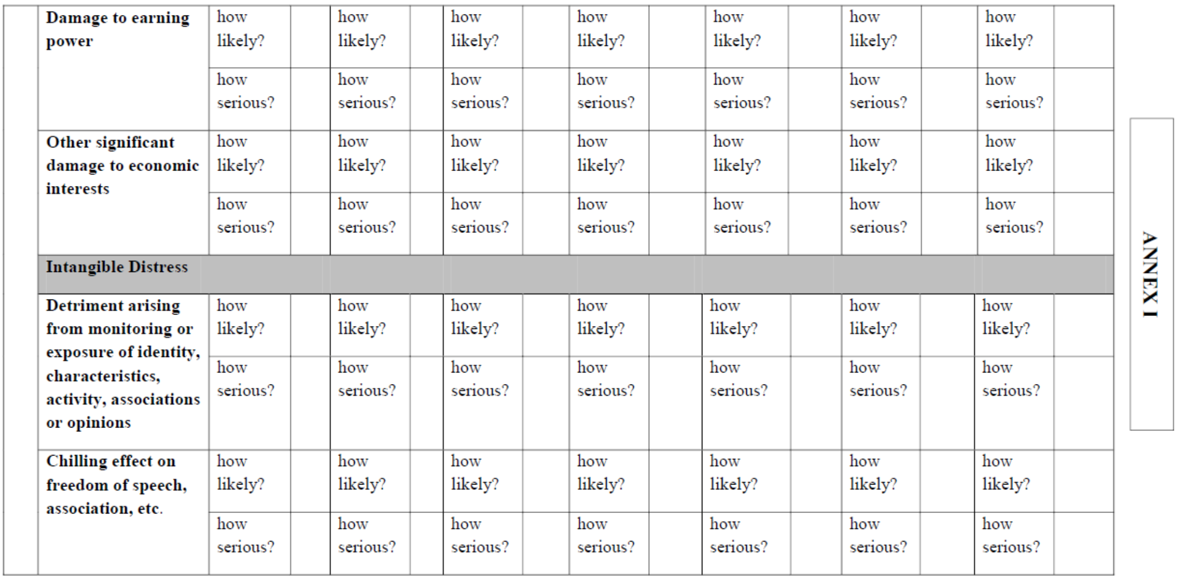
Aggregate Risk Rank:
Highest score is 300
Lowest score is 0

Draft Risk Matrix: Option 2



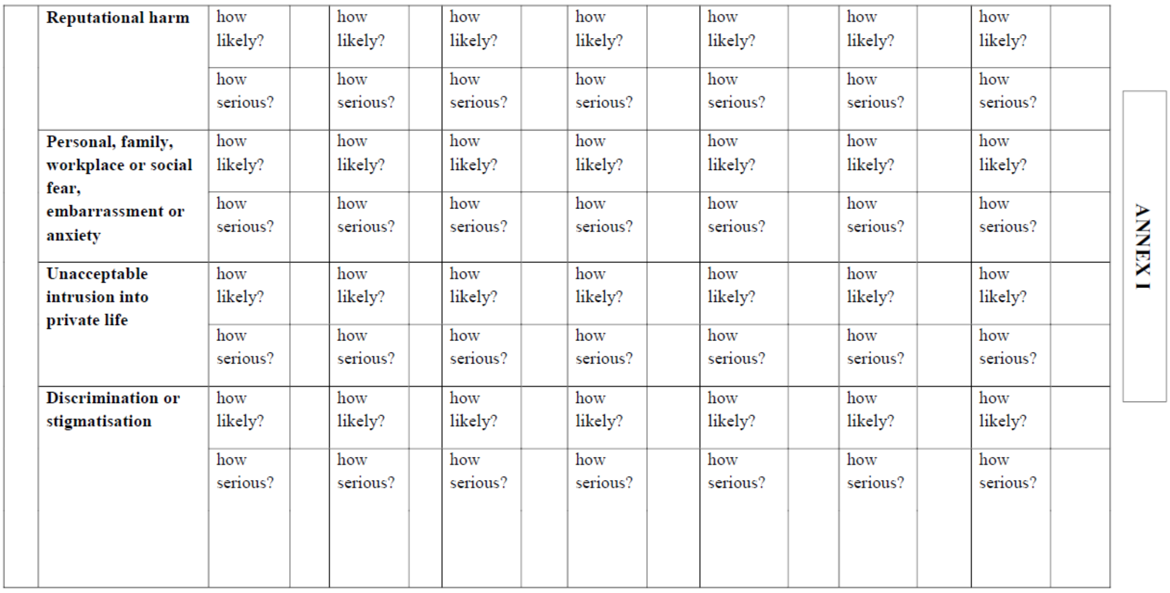
Proposed Processing:		THREATS													
		Unjustifiable Collection of Data		Inappropriate Use of Data								In Wrong Hands			
				Storage or use of inaccurate or outdated data		Use of data beyond individuals' reasonable expectations		Unusual use of data beyond societal norms, where any reasonable individual in this context would object		Unjustifiable inference or decision-making, that the organisation cannot objectively defend		Lost or stolen data		Data that is unjustifiably accessed, transferred, shared or published	
HARMS	Tangible Harm														
	Bodily harm	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Loss of liberty or freedom of movement	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX I



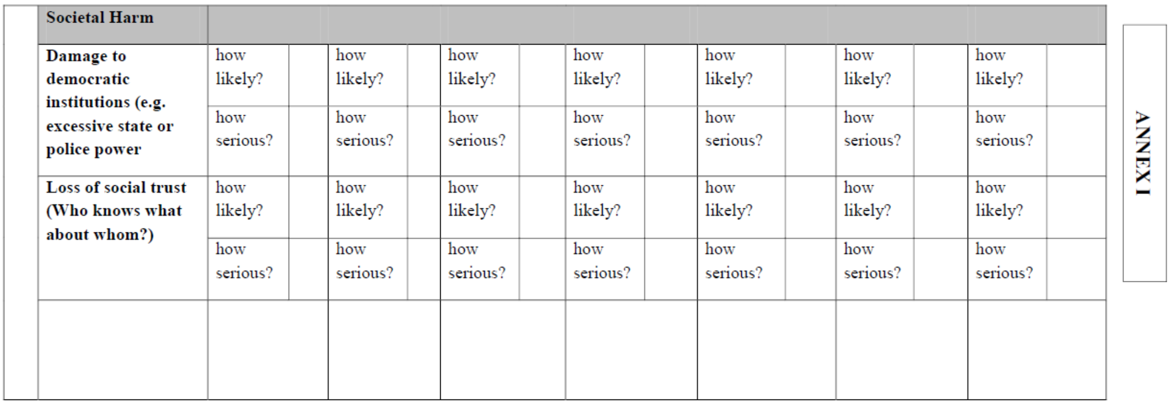
	Damage to earning power	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Other significant damage to economic interests	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Intangible Distress														
	Detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Chilling effect on freedom of speech, association, etc.	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX I



	Reputational harm	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Personal, family, workplace or social fear, embarrassment or anxiety	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Unacceptable intrusion into private life	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Discrimination or stigmatisation	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX I



	Societal Harm														
	Damage to democratic institutions (e.g. excessive state or police power	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	
	Loss of social trust (Who knows what about whom?)	how likely?		how likely?		how likely?		how likely?		how likely?		how likely?		how likely?	
		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?		how serious?	

ANNEX I

Significantly, risk management matrices such as the ones devised by CIPL may also be a useful tool for policymakers and regulators. A consensus based on the language and methodology of a matrix could help regulators fix and communicate their own priorities for interpreting and enforcing rules. This would be welcomed by businesses as it would give them improved predictability and a better idea of where to focus their own risk assessments.

Q10. Which kinds of data should be subject to a potential trade regulation rule? Should it be limited to, for example, personally identifiable data, sensitive data, data about protected categories and their proxies, data that is linkable to a device, or non-aggregated data? Or should a potential rule be agnostic about kinds of data?

As mentioned in the Executive Summary, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[45] our comments below will focus exclusively on the substance and nature of the issues raised in this question.

Any potential solution should promote an accountability-based framework that requires organizations to collect and use data based on a proper risk assessment. The risk assessment would include an evaluation of the "sensitivity" of the data and any risks associated with the intended use of that data, **based on the particular context**, rather than solely on the type of data at issue.

Sensitivity and risk-level may vary depending on the context and purpose of use. Thus, instead of attempting to draft definitions on different types of data or categorical classifications such as "sensitive data," CIPL encourages the publication of guidance on what should be regarded as "high-risk" data use and processing. This could include guidance on what types of data might be particularly sensitive or high-risk in certain contexts, but the final determination of what, in fact, is sensitive or high-risk should be left to contextual risk assessments. It is the particular use of data that creates risks and harms for people , and not the data itself.

A categorical approach may have the unintended effect of requiring organizations to treat information as sensitive even where the circumstances of the processing present a limited risk to affected individuals, thereby preventing a beneficial data use for no reason. Equally, where specific data elements do not appear in a prescribed list, there is a risk that certain processing—which in fact is sensitive and carries a high risk for data subjects—is not characterized as such, thereby increasing the possibility of risky data uses.

A pre-defined list of sensitive data elements fails to take into account the context of the processing, including the purposes for which the data is processed, the volume of data, who carries out the processing, what other information that organization has access to, and any privacy enhancing measures that are in place. Defining sensitive data by reference only to a list of pre-set data types and ignoring the context of the processing activity may result in worse outcomes for individuals and organizations, leading to either overly conservative or unduly permissive processing.

More generally, the Commission should review the scope of data as previously articulated in its 2012 Report, *Protecting Consumer Privacy in an Era of Rapid Change*.[46] As defined in that report, data is limited to "consumer data" that can be "reasonably linked to a specific consumer, computer, or other device." Furthermore, the report clarified that data is not "reasonably linkable" to the extent that a company: "(1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to reidentify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[47] Thus, personal data that has been effectively anonymized based on this test should be explicitly excluded from any potential law or regulation.

[45] ANPR, 87 FR at 51277.

[46] FTC Report: *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers*, March 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[47] *Id.*, at p. iv.

Q12. Lax data security measures and harmful commercial surveillance injure different kinds of consumers (*e.g.,* young people, workers, franchisees, small businesses, women, victims of stalking or domestic violence, racial minorities, the elderly) in different sectors (*e.g.,* health, finance, employment) or in different segments or "stacks" of the internet economy. For example, harms arising from data security breaches in finance or healthcare may be different from those concerning discriminatory advertising on social media which may be different from those involving education technology. How, if at all, should potential new trade regulation rules address harms to different consumers across different sectors? Which commercial surveillance practices, if any, are unlawful such that new trade regulation rules should set out clear limitations or prohibitions on them? To what extent, if any, is a comprehensive regulatory approach better than a sectoral one for any given harm?

As mentioned in the Executive Summary, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[48] our comments below will focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

An accountability-based solution that includes an obligation to conduct a proper risk assessment (i.e., a contextual risk assessment) will address the specific concerns raised in this question. Risk assessments help determine whether a particular use in a given context will adversely affect different groups of consumers, in different sectors, or in different segments of the economy. Risk assessments also determine whether certain uses are sensitive and high-risk for individuals and, therefore, in need of higher protections (e.g., enhanced security measures, limitations on processing purposes or secondary uses, enhanced transparency, etc.). Under the risk-based approach, organizations:

- build data protection into the design and strategy of their programs;
- assess privacy (and other) risks to individuals and devise appropriate risk mitigations on a continual and context-specific basis; and
- document their risk assessments and demonstrate them on request to relevant enforcement authorities, showing that appropriate risk criteria, frameworks, and methodologies are applied.

Any legal or regulatory approach to addressing the risks of harm associated with data processing should focus on enabling an effective risk-based approach to data protection, supplemented with regulatory guidance addressing relevant risk criteria and consequential harms, and suggesting appropriate risk-assessment methodologies to be used.

In general, CIPL does not believe that a sectoral approach is the right way to regulate the use, collection, sharing, and wider processing of data. Data is agnostic of sectors; it moves across sectors,

[48] ANPR, 87 FR at 51277.

technologies, borders, and entities, which makes it difficult to regulate on a sectoral basis. Instead, CIPL recommends a horizontal, sector-agnostic approach that includes:

a) a general, principle- and risk-based framework that is comprehensively applicable to all data;
b) flexible, co-regulatory mechanisms—such as codes of conduct, certifications, and accountability standards—that translate general rules into specific practices or requirements that can evolve over time; and
c) regulatory guidance, created in consultation with relevant stakeholders, that helps interpret general rules to different contexts and sectors.

B. Harm to children, including teenagers

Q13. The Commission here invites comment on commercial surveillance practices or lax data security measures that affect children, including teenagers. Are there practices or measures to which children or teenagers are particularly vulnerable or susceptible? For instance, are children and teenagers more likely than adults to be manipulated by practices designed to encourage the sharing of personal information?

Children's participation in the digital economy through child-specific (as well as general-audience) products and services can enhance their education, recreation, communication, and other activities, but it also creates unique risks given children's vulnerability.

CIPL recently published **a white paper on children's privacy** entitled "Protecting Children's Data Privacy, Policy Paper I, International Issues and Compliance Challenges."[49] This report explores key issues and compliance challenges as well as policy considerations that organizations and regulators face when addressing children's online data privacy. Our paper looks closely at the competing rights and interests associated with children's ability and need to participate in the digital society.

We ask the Commission to consider our white paper as CIPL's full response to the ANPR's questions relating to children's data and to incorporate it as part of the record.

In a nutshell, CIPL encourages the Commission, Congress, and other policymakers to focus on the best interests of the child as a guiding principle, taking into account the need and the importance of online participation, together with the potential risks.[50] As is the case with data processing in general, there are a number of important and beneficial purposes for processing children's data—including those

[49] CIPL White Paper: *Protecting Children's Data Privacy, Policy Paper I, International Issues and Compliance Challenges*, October 22, 2022, available at https://www.informationpolicycentre.com/policy-paper-i-international-issues--compliance-challenges.html; filed herewith as Exhibit 1.

This report will be followed by a second report in 2023, provisionally titled "Protecting Children's Data Privacy Policy Paper II: Practical Solutions to Protect Children and Enhance Compliance." That second report will highlight existing and potential policy, industry sector and technology solutions for the challenges identified in Policy Paper I.

[50] See CIPL White Paper: *GDPR Implementation in Respect of Children's Data and Consent*, March 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf; filed herewith as Exhibit 13.

that involve "profiling"[51]—along with a range of potential risks, which should be addressed in the same way as all data processing risks should be addressed: through context-specific risk assessments that enable organizations to identify the appropriate mitigations for a given context and a given use. A risk-based approach to regulating the privacy of children (including teenagers) is the best way to take into account multiple interests, rights, risks, and benefits for children, and it would enable companies to tailor protection and controls for different services and products based on such risk assessments.

Q14. What types of commercial surveillance practices involving children and teens' data are most concerning? For instance, given the reputational harms that teenagers may be characteristically less capable of anticipating than adults, to what extent should new trade regulation rules provide teenagers with an erasure mechanism in a similar way that COPPA provides for children under 13? Which measures beyond those required under COPPA would best protect children, including teenagers, from harmful commercial surveillance practices?

Please refer to our response to Question 13 and our recently published white paper on children's privacy.[52]

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

Q17. Do techniques that manipulate consumers into prolonging online activity (e.g., video autoplay, infinite or endless scroll, quantified public popularity) facilitate commercial surveillance of children and teenagers? If so, how? In which circumstances, if any, are a company's use of those techniques on children and teenagers an unfair practice? For example, is it an unfair or deceptive practice when a company uses these techniques despite evidence or research linking them to clinical depression, anxiety, eating disorders, or suicidal ideation among children and teenagers?

While again encouraging the Commission to re-evaluate its use of the term "commercial surveillance" (see our response to Question 7), CIPL agrees that the Commission raises valid concerns regarding certain practices related to children. That said, these sorts of concerns would naturally be addressed as part of a proper risk assessment, which is a foundational element of organizational accountability and which, in the children's context, would take into account the best interests of the child. It is important to note that risk assessments encompass periodic reviews of the organization's overall privacy program and information uses in light of changes in business models, law, technology, understandings of the involved risks, regulatory guidance and other relevant factors, followed by modifications to the program to account for those changes. Therefore, when evidence shows certain practices as being harmful to children, such evidence, if not available earlier, would be considered in

[51] For example, companies can create user profiles to facilitate and ensure a safe experience for young users.

[52] *Supra*, note 49.

a periodic risk assessment. For additional commentary, please see our response to Question 13 and our recently published white paper on children's privacy.[53]

As to the question of whether the use of certain techniques would constitute an unfair practice, CIPL again notes that the Commission's authority to stop "unfair … acts or practices in or affecting commerce"[54] requires a **risk assessment** by both industry and the Commission. The FTC's unfairness authority applies only to practices that cause "substantial" injury to consumers that are "not reasonably avoidable by consumers themselves" and are "not outweighed by countervailing benefits to consumers or to competition."[55] Thus, the **FTC Act itself requires a balancing** of both "injuries" and "benefits" in any assessment of unfairness, providing statutory support for a risk-based model. CIPL believes that the best way to promote such a balancing would be through **dialogue and engagement** not only with key stakeholders (consumers and industry), but also with other agencies and enforcement authorities that address privacy and data security issues. All affected parties need to come to a consensus about risks and harms in order to clarify consumer expectations and business responsibilities.

Q18. To what extent should trade regulation rules distinguish between different age groups among children (*e.g.,* 13 to 15, 16 to 17, etc.)?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR.

The age of consent in the context of data privacy varies widely across jurisdictions.[56] This disparity reflects the reality that any determination of a child's maturity to provide consent to the collection and processing of data does not lend itself to bright-line analysis.

The question of consent in children's data privacy is further complicated because children's awareness, maturity, and need to access resources and information change as they mature. The nature of the content and experiences appropriate for children evolves with their development – what is appropriate for a 15-year-old girl is not necessarily appropriate for her 8-year-old brother.

These contextual questions, however, could be addressed as part of a proper risk assessment. So, again, CIPL stresses the need for risk assessments to be included in any proposed action, be it

[53] *Supra*, note 49.

[54] 15 U.S.C. §45(a)(1).

[55] 15 U.S.C.§45(n).

[56] In the United States, for example, the Child Online Privacy Protection Act provides that children may provide consent at age 13. The GDPR sets that age at 16, but permits Member States to set the age as low as 13. Both South Korea and China establish the age of consent at 14. In some cases, privacy law establishes the age at which children may consent; in others, laws related to contract are relied on to make that determination, so that a child's ability consent to the collection and processing of data mirrors their ability to enter into a contract. Other jurisdictions take a more calibrated approach and provide that children can make certain decisions about data collection and processing at different stages in their development.

legislative or regulatory. For additional commentary, please see our response to Question 13 and our recently published white paper on children's privacy.[57]

Q19. Given the lack of clarity about the workings of commercial surveillance behind the screen or display, is parental consent an efficacious way of ensuring child online privacy? Which other protections or mechanisms, if any, should the Commission consider?

For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

Requiring the consent of a parent to the collection or processing of data when a child is not of age raises issues for organizations and families alike. For example, parents may be unfamiliar with various technologies and data protection laws and regulations. As a result, they may not understand how parental consent works or what consequences flow therefrom. Thus, a parental consent requirement may be limited in its effectiveness. Moreover, a parental consent requirement may envision a nuclear family, inadvertently discriminating against or sidelining children who do not live with both parents, whose parents are deceased or otherwise incapable of acting on their behalf, whose parents do not have the child's best interests at heart, or who live in other non-nuclear family structures. Furthermore, such a requirement may not sufficiently address situations where parents and children share devices.

If a law or regulation were to broaden the definition of "parent" to include other responsible adults who may act in their place, companies are faced with determining whether the individual who is consenting on a child's behalf may indeed act in that capacity. While this issue arises in many contexts–medical treatment, education, social care–it is a problem online especially because the relationship with the child is both limited and distant, so that normal mechanisms for assessing who may exercise a role of responsibility are not available. Making such a determination online requires an evaluation of documentation to determine whether the individual is in fact the parent or is legitimately acting as a guardian.

The parental consent conundrum also arises in the case of pre-teens or young adolescents, who may wish to share data necessary to access information or resources designed to help them deal with questions they may not choose—or be ready—to share with their parents, such as sexual orientation, sexual abuse, gender identity, issues of body image, and mental health. The availability of online resources may be particularly important to them at a critical moment in their lives. In such cases, it may be necessary to identify alternatives to traditional parental consent where no other legal basis for processing applies. For additional commentary, please see our response to Question 13 and our recently published white paper on children's privacy.[58]

[57] *Supra*, note 49.

[58] *Supra*, note 49.

Q20. How extensive is the business-to-business market for children and teens' data? In this vein, should new trade regulation rules set out clear limits on transferring, sharing, or monetizing children and teens' personal information?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. That said, any proposed action should recognize, protect, and enable legitimate and beneficial transfers of children's data (such as for the purpose of preventing child victimization or providing necessary products or services to children). For additional commentary, please see our response to Question 13 and our recently published white paper on children's privacy.[59]

Q22. Should new rules impose differing obligations to protect information collected from children depending on the risks of the particular collection practices?

As mentioned in the Executive Summary, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[60] our comments below will focus exclusively on the substance and nature of the issues raised in this question.

CIPL agrees that potential legislation or rules concerning children's data should account for the particular risks associated with both the collection and use of such data. This is why CIPL supports organizational accountability, which specifically includes risk assessments. Overall, CIPL believes that the processing of children's data should focus on the best interests of the child as a guiding principle, while also assessing the risks.[61] In these cases, particular attention should be paid to the purpose of the processing, the role that the processing plays in the provided service, and the safeguards put in place to address likely and serious harms. Given that there are beneficial uses of children's data, policymakers should recognize that the processing of personal data relating to children does not raise the same level of risk in all cases, so a proper risk assessment should be part of any proposed solution. For additional commentary, please see our response to Question 13 and our recently published white paper on children's privacy.[62]

[59] *Supra*, note 49.

[60] ANPR, 87 FR at 51277.

[61] *Supra*, note 50.

[62] *Supra*, note 49.

Q23. How would potential rules that block or otherwise help to stem the spread of child sexual abuse material, including content-matching techniques, otherwise affect consumer privacy?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

Artificial intelligence (AI) applications promise enormous benefits for society; one such application could support efforts to stem the spread of child sexual abuse material. While AI applications, at times, are in tension with traditional data protection principles, trade-offs are required in certain contexts, and the suppression of child sexual abuse material is undoubtedly one of those contexts. Data should therefore be made available to AI developers in order to train algorithms appropriately.[63] Of course, CIPL's endorsement of a risk-based approach would apply in this situation as well, with the benefits to society of training relevant algorithms possibly outweighing an infringement to privacy interests. For additional commentary, please see our response to Question 13 and our recently published white paper on children's privacy.[64]

C. Balancing costs and benefits.

Q24. The Commission invites comment on the relative costs and benefits of any current practice, as well as those for any responsive regulation. How should the Commission engage in this balancing in the context of commercial surveillance and data security? Which variables or outcomes should it consider in such an accounting? Which variables or outcomes are salient but hard to quantify as a material cost or benefit? How should the Commission ensure adequate weight is given to costs and benefits that are hard to quantify?

As mentioned in the Executive Summary and elsewhere, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[65] our comments below will focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

From the regulator's perspective, one of the benefits of an accountability-based model is that the **regulated entity—as opposed to the regulator—is the one responsible** for conducting the relevant risk assessments, including the necessary cost/benefit analyses. However, the regulated entity must then be able to **demonstrate** its risk assessments to the regulator upon request and be able to explain and defend its processing decisions based on those assessments.

[63] See, for example, *Building ML Models to Detect Malicious Behavior*, Jan. 23, 2020, available at https://h2o.ai/resources/video/building-ml-models-to-detect-malicious-behavior/.

[64] *Supra*, note 49.

[65] ANPR, 87 FR at 51277.

In such a scenario, a regulator's primary roles would be (1) to provide guidance to companies on the appropriate factors to consider and methodologies to use when assessing the severity and likelihood of risk, and (2) to evaluate—in the context of an investigation or enforcement action—the soundness of a given risk assessment and the processing decisions based thereupon. Thus, the regulator would not itself be tasked with conducting risk assessments for all possible processing scenarios; instead, it would establish appropriate risk assessment processes and frameworks, provide guidance on the desired outcomes, and enforce consequent compliance. Of course, the regulator may, at times, need to conduct *de novo* risk assessments for the purpose of determining the nature of its guidance on key issues or re-evaluating the assessments made by regulated entities.

In order to facilitate the standardization of risk assessments and to avoid unnecessary assessments, it would be useful for the regulator to facilitate **engagement and discussions** with stakeholders on appropriate risk taxonomy and methodologies.[66] The regulator should also consider producing **guidance** on the most common high-risk use cases and provide a standard set of mitigating measures that businesses could apply in certain routine situations without the need to conduct a separate or full-blown risk assessment. Of course, such guidance should be directional only; companies would be free to implement different mitigating measures on the basis of a formal risk assessment, in particular if they have reason to believe that in their given context a particular practice might be higher-risk or lower-risk compared to general expectations.

In any event, it is important to remember that the purpose of a risk assessment **is not to establish *whether* there is any risk** in the processing; indeed, almost all uses of personal data involve some kind of risk, and it is virtually impossible to eliminate all risks once they are identified. Instead, the purpose of a risk assessment is **to consider the *severity of risk* and to *reduce it* as much as is reasonable and practicable** in light of the intended benefits and the available mitigations and controls (e.g., state-of-the-art technology, cost of implementation, and best practices). In its 2015 report on Data-Driven Innovation,[67] the OECD stressed that, "a certain level of risk has always to be accepted for the value cycle to provide some benefit."

It is important to remember that risk may also have a **temporal element**: risk can be classified by taking into account the timing of the possible harms. From this viewpoint, risks have long-, medium- and short-term impacts, which must be considered in any risk assessment.

While risk assessments focus primarily on the likelihood and severity of harms that individuals may experience, assessments should also include **consideration of the benefits** to individuals, the organization, and third parties or society. This enables the preservation of the desired benefits when implementing any necessary mitigations to address the identified risks. Benefits should be considered at the outset of the risk assessment, as they are related to the purpose of the processing. They are also relevant in devising appropriate mitigation measures, which can affect the margin of benefits.

As with harms, the assessment of benefits should include both the magnitude of benefit and its likelihood of occurring. The range of benefits should include benefits to individuals (e.g., ability to

[66] See, for example, CIPL's Draft Risk Matrices, discussed in response to Question 7.

[67] *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD, available at https://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm.

complete a transaction, obtain a desired good or service, be protected from fraud, etc.) and to the organization (e.g., ability to attract customers, deliver goods or services more efficiently, reduce fraud and other losses, etc.). They should also include benefits likely to be enjoyed by society more broadly (e.g., use of data for social good, such as reducing the spread of infectious diseases, reducing environmental waste, delivering services with greater efficiency and fairness, etc.).

A risk-based approach provides organizations with a great deal of flexibility, but it also requires sound judgment and a thorough understanding of the potential impact of the organization's activities. Some businesses have difficulty operationalizing—in a consistent and repeatable manner—the identification of relevant risks, harms, and benefits; the balancing of those factors; and the likelihood and severity of anticipated harms.[68] To assist those businesses, the regulator should provide guidance on the **appropriate factors to consider and methodologies to use**.

In sum:

- Adoption of a risk-based approach delivers effective, appropriate, and proportionate protection for consumers and enables innovative and responsible data uses.
- Organizations are best placed to understand the risks raised by their own processing activities, and, therefore, are best placed to identify and implement appropriate mitigation measures.
- Risk is contextual. Regulatory guidance can provide examples and guardrails on risk and high-risk for individuals. However, organizations should be allowed to evaluate risks in light of the particular context of the proposed use and to implement appropriate safeguards to address any identified risks through internal accountability programs.
- The relevance of risk to compliance should permeate all aspects of any proposed legislation or regulation. Organizations must be able to prioritize compliance based on risk.
- Proposed laws or regulations should promote organizational assessments of the benefits and the risks to individuals and society from the organization's use of consumer data. A risk-based approach can maximize these goals.
- Providing categorical lists of scenarios, technologies, or processing activities that are "high risk" should be avoided; proposed laws or regulations will likely be more effective if they instead clarify specific harms to individuals that should be avoided.
- Proposed laws and regulations could provide presumptions as to what might be considered "high risk" processing, but such presumptions should be rebuttable through actual risk assessments. This approach combines useful regulatory and legal guidance with the ability of organizations to verify the actual level of risk for their specific processing activities.
- Risk mitigation should not be understood to mean the **elimination** of risk, but rather the **reduction** of risk to the extent practicable and acceptable, given the desired benefits and reasonable economic and technological parameters. Often there will be a residual risk.

[68] For a detailed discussion of the role of risk assessments, see *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, CIPL, June 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf (filed herewith as Exhibit 18); and *The Role of Risk Management in Data Protection*, CIPL, December 2014, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_2-the_role_of_risk_management_in_data_protection-c.pdf (filed herewith as Exhibit 17).

Organizations will have to make a reasoned and evidence-based decision on whether to proceed with processing in light of any residual risks, taking into account "proportionality" vis-à-vis purpose, interest, and/or benefits.

- Where an organization cannot resolve or reach a decision regarding the residual risk of a given processing, proposed laws or regulations could offer an opportunity for ex-ante consultation with the regulator, which could approve, disapprove, or recommend modifications to the organization's proposed processing.

Q26. To what extent would any given new trade regulation rule on data security or commercial surveillance impede or enhance innovation? To what extent would such rules enhance or impede the development of certain kinds of products, services, and applications over others?

For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7. Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

A **risk-based regulatory approach** would promote innovation by enabling organizations to identify potential harms to individuals and adopt appropriate protective measures to minimize the risks associated with new uses of consumer data. It would also identify areas where the potential negative impact on individuals is limited.

In addition, **innovation depends on trust**: the more individuals can trust organizations to take their privacy obligations seriously and implement appropriate measures, the more comfortable they will be with organizations using their data.

Moreover, to encourage innovation, any proposed legislative or regulatory regime must provide businesses with **robust, flexible, and future-proof legal bases** for processing consumer data. If a law or regulation were to adopt a restrictive approach—i.e., limiting or narrowly defining legal bases for processing and placing excessive emphasis on consent—it would risk excluding legitimate and beneficial uses of data. Data protection frameworks that adopt a consent-based approach subject to a list of exemptions can become quickly outdated, with innovative data uses oftentimes falling outside the scope of what the law permits.

A **legitimate interest basis**[69] that explicitly requires a demonstrable weighing of interests is increasingly regarded as an essential legal basis for data processing in the modern information age. It enables ongoing delivery and improvement of products and services—as well as new and innovative uses of data—while ensuring organizational accountability and respecting the privacy concerns of individuals. It is useful in the context of rapidly advancing technologies and constantly evolving business models where processing activities are increasingly digitized.

[69] See, for example, the EU General Data Protection Regulation (GDPR) and Brazil's *Lei Geral de Proteção de Dados* (LGPD).

In any proposed action, policymakers should thus consider recognizing innovative and flexible legal bases (including legitimate interests) that could be used to support a wide range of data uses—including innovative data uses—where consent or other more prescriptive bases would be impracticable or inappropriate.

Good regulation doesn't inhibit good innovation. Any proposed action should not regulate good practices out of existence.

One way to encourage innovative uses in a more tightly regulated context is through the creation of **regulatory sandboxes**, which allow businesses to safely explore new uses of data, including data sharing practices, within a safe environment and in consultation with the regulator.[70]

"**Policy prototyping**" is another approach where possible policy positions and proposed regulations are tested on a cohort of willing entities—including small and medium-sized enterprises (SMEs) or start-ups—to provide concrete, experience-based input from those implementing the rules. This ultimately helps create more viable and effective rules.[71]

"**Design Thinking**" is another method whereby data privacy requirements and compliance challenges can be addressed, made scalable, and developed bottom-up by multifunctional teams. The concept of "design thinking" may also provide opportunities for regulatory participation and engagement with regulated organizations and experts from other areas (e.g., behavioral economists, user-centric designers, technology engineers, marketing and customer relationship experts).[72]

It is also helpful when the regulator, together with regulated entities, views compliance as an iterative, dynamic, and ongoing process, as opposed to a one-off event. Any proposed legal or regulatory initiative should reflect and enable such an approach. **Dynamic compliance** is particularly suited for data protection, given the speed of technological developments and adoption of digital solutions. Just like technology deployment, compliance should be agile and subject to continual feedback. This approach enables improvements, based on user feedback, internal and external developments, and

[70] See, for example, the U.K. Information Commissioner's Office (ICO) development of a Regulatory Sandbox service, accessible at https://ico.org.uk/for-organisations/regulatory-sandbox/, which supports organizations that are "creating products and services [that use] personal data in innovative and safe ways."

See also, CIPL's Regulatory Sandbox White Paper: *Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice*, March 8, 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf; filed herewith as Exhibit 10.

[71] See Policy Prototyping, Infocomm Media Development Authority (IMDA), Singapore, available at https://www.imda.gov.sg/programme-listing/Data-Innovation/Policy-Prototyping. See also, Andrade, Norberto Nuno Gomes de and Kontschieder, Verena, AI Impact Assessment: A Policy Prototyping Experiment (January 1, 2021). Available at SSRN: https://ssrn.com/abstract=3772500 or http://dx.doi.org/10.2139/ssrn.3772500.

[72] See, Why Design Thinking Works, Jeanne Liedtka, Harvard Business Review, Sept.-Oct., 2018, available at https://hbr.org/2018/09/why-design-thinking-works.

lessons from industry and regulators. Organizations should be encouraged to adopt dynamic compliance, and the regulator should not punish those that actively try to get it right over time.[73]

Prof. Christopher Hodges suggests an **Outcome-Based Cooperation Regulation (OBCR)** model for regulators to “co-create” with industry leaders and other stakeholders by agreeing on common purposes and desired outcomes. According to Hodges, scientific research has shown that this model is superior to the traditional “rule-breach-enforcement” model that banks on deterrence. Reserving “hard enforcement” only “as a last resort,” OBCR encourages ex ante constructive engagement between regulators and regulated entities, as well as guidance on best practices and other supportive measures; it seeks to account for the goals of business (commercial success and profit) and the goals of governments, regulators, and societies (economic growth and protection from harm) with acceptable risk. OBCR is based on **trust**, requiring all stakeholders (including regulators) to show that they are trustworthy. OBCR aims to create a framework that supports cooperation rather than conflict in regulation.[74]

Q28. Should the analysis of cost and benefits differ in the context of information about children? If so, how?

CIPL recognizes that children’s data presents unique risks, which is why risk assessments are needed and useful. Each risk assessment, by nature, considers the relevant risks and benefits of data use in a particular context. For additional commentary, please see our response to Question 13 and our recently published white paper on children’s privacy.[75]

Q29. What are the benefits or costs of refraining from promulgating new rules on commercial surveillance or data security?

CIPL has been and continues to be a strong supporter of federal privacy legislation, which ideally would provide organizations with a single federal standard. The currently quite advanced stage of developing

[73] *Supra*, note 7. See also, CIPL White Paper: *Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions*, October 6, 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021___3_.pdf; filed herewith as Exhibit 3.

[74] See Christopher Hodges, *Supporting Cooperative Behavior*, July 20, 2022, available at https://www.indr.org.uk/_files/ugd/6b9149_c7e339a0f5dd4999a220d609573d6352.pdf; Christopher Hodges, *An Introduction to Outcome Based Cooperative Regulation (OBCR)*, available at https://55c366d1-05de-46e1-a383-a8f804514d8a.filesusr.com/ugd/6b9149_9424aee004ff4051bd67025c867f1f79.docx?dn=2202%20An%20Introduction%20to%20OBCR.docx; Christopher Hodges, *Outcome-Based Cooperation - In Communities, Business, Regulation, and Dispute Resolution*, 2022, Bloomsbury Publishing, available at https://www.bloomsbury.com/us/outcomebased-cooperation-9781509962495/; Christopher Hodges, *Ethical Business Regulation; Growing Empirical Evidence*, 2016, available at https://www.fljs.org/sites/default/files/migrated/publications/Ethical%20Business%20Regulation.pdf.

[75] *Supra*, note 49.

a federal privacy law raises the legitimate question of whether regulatory action by the FTC at this stage is appropriate, necessary, or advisable. We believe that any rulemaking at this stage might add to the already complex patchwork of comprehensive state and sector-specific federal laws and regulations without significant corresponding benefits. That said, businesses would certainly benefit from additional guidance on best practices for responsible and accountable data privacy practices, and the Commission is well-placed to play a leading role in that regard.

D. Regulation of practices

Q30. Should the Commission pursue a Section 18 rulemaking on commercial surveillance and data security? To what extent are existing legal authorities and extra-legal measures, including self-regulation, sufficient? To what extent, if at all, are self-regulatory principles effective?

As mentioned above, CIPL has been and continues to be a strong supporter of federal privacy legislation, which we view as a superior solution for a U.S. federal privacy framework. There are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR.

That said, the Commission should continue to promote and encourage—through consent orders, industry guidance, and other non-rulemaking actions—the principles of organizational accountability, the use of risk assessments, and the implementation of comprehensive data privacy management programs.

CIPL also encourages the Commission's support of enforceable co-regulatory accountability and compliance mechanisms, such as the Global Cross-Border Privacy Rules (CBPR) initiative (in whose development and enforcement the Commission has been significantly involved),[76] privacy codes of conduct, and certifications. It would be particularly helpful if the Commission were to articulate more clearly that it will consider participation in such accountability and compliance schemes as a mitigating factor in the enforcement context. That would go a long way towards incentivizing and encouraging the uptake of proactive organizational accountability and translate into tangible privacy benefits for consumers.[77]

[76] See *Global Cross-Border Privacy Rules Declaration*, https://www.commerce.gov/global-cross-border-privacy-rules-declaration. See also, *FTC becomes first enforcement authority in APEC Cross-Border Privacy Rules System*, July 26, 2012 available at https://www.ftc.gov/news-events/news/press-releases/2012/07/ftc-becomes-first-enforcement-authority-apec-cross-border-privacy-rules-system; and *FTC Joins New Asia-Pacific Multinational Network of Privacy Enforcement Authorities*, July 19, 2010, available at https://www.ftc.gov/news-events/news/press-releases/2010/07/ftc-joins-new-asia-pacific-multinational-network-privacy-enforcement-authorities.

[77] *Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions,* CIPL, October 6, 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_organizational_accountability_in_data_protection_enforcement_-_how_regulators_consider_accountability_in_their_enforcement_decisions__6_oct_2021__3_.pdf (filed herewith as Exhibit 3); *CIPL Accountability Discussion Paper 2 - Incentivising Accountability: How Data*

Q31. Should the Commission commence a Section 18 rulemaking on data security? The Commission specifically seeks comment on how potential new trade regulation rules could require or help incentivize reasonable data security.

As mentioned in the Executive Summary and elsewhere, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[78] our comments below will focus exclusively on the substance and nature of the issues raised in this question.

CIPL supports a risk-based and flexible framework for privacy protections and data security that includes appropriate incentives for organizations to implement effective accountability measures. Such incentives should include the regulator's explicit reliance on demonstrated accountability practices as a **mitigating factor in an enforcement context**. CIPL has published two papers on this topic.[79]

CIPL notes that data security is difficult to regulate in a detailed and prescriptive manner, as the appropriate data security practices, tools, and technologies are constantly evolving and changing. Moreover, "appropriate" security depends on the context of the processing, the relevant risks and harms, the available technology, and the cost of implementation. Hence, detailed security rules are best left to standards bodies, certifications, and industry-developed solutions.

Policymakers should also avoid duplicating existing data security regulations and standards in an already crowded field. Numerous risk-based frameworks are already established or are in the process of being finalized, such as Executive Order 14028 on Improving the Nation's Cybersecurity,[80] many state data security laws and regulations,[81] the NIST Cybersecurity Framework,[82] the NIST Cybersecurity Framework 2.0,[83] the Cyber Incident Reporting for Critical Infrastructure Act

Protection Authorities and Law Makers Can Encourage Accountability, CIPL, July 23, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf (filed herewith as Exhibit 12).

[78] ANPR, 87 FR at 51277.

[79] *Supra*, note 77.

[80] Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity, 86 FR 26633, available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[81] See, for example, 201 Mass. Code of Regs. 17.00-17.04, available at https://www.mass.gov/regulations/201-CMR-1700-standards-for-the-protection-of-personal-information-of-residents-of-the-commonwealth, and 23 NYCRR Part 500, available at https://dfs.ny.gov/industry_guidance/cybersecurity.

[82] NIST Cybersecurity Framework, available at https://www.nist.gov/cyberframework.

[83] NIST Cybersecurity Framework – Journey To CSF 2.0, available at https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

rulemaking,[84] NIST Security and Privacy Controls for Information Systems and Organizations SP 800-53,[85] and ISO/IEC Standard 27001.[86] Policymakers should acknowledge, assess, leverage, and promote these existing and proposed regulations and frameworks.

Q35. Should the Commission take into account other laws at the state and federal level (e.g., COPPA) that already include data security requirements. If so, how? Should the Commission take into account other governments' requirements as to data security (e.g., GDPR). If so, how?

The Commission should follow developments in data security laws and regulations both domestically and abroad, especially in light of our previous recommendation[87] that it is not really possible, or advisable, to stipulate concrete security measures.[88]

CIPL supports **dialogue and cooperation** with other regulators, and it encourages the Commission to understand the current regulatory landscape both within the U.S. and beyond to improve consistency across jurisdictions and to minimize potentially conflicting regulatory overlap for businesses.

Q38. Should the Commission consider limiting commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies? If so, how?

As mentioned in the Executive Summary and elsewhere, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[89] our comments below will focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

[84] See the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) webpage, available at https://www.cisa.gov/circia, and the related Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022, 87 FR 55833, available at https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022.

[85] Security and Privacy Controls for Information Systems and Organizations, SP 800-53 Rev. 5, available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[86] ISO/IEC 27001 and related standards, Information security management, available at https://www.iso.org/isoiec-27001-information-security.html.

[87] See our response to Question 31.

[88] Indeed, the GDPR adopts a general, principles- and outcomes-based data security requirement, enabling companies to determine the appropriate measures in a particular context to achieve data security and avoid unauthorized and unlawful access to, use of, and sharing of data.

[89] ANPR, 87 FR at 51277.

Biometric data is already being used in different sectors (such as transportation, health, and retail), but there is no consensus on what it covers.[90] It often includes facial templates, fingerprint scans, palm prints, iris and retina scans, and voiceprints, but it can sometimes include behavioral characteristics, including gait and motion patterns[91] as well as handwriting.[92]

While the benefits and efficiencies of biometric technologies are obvious, there is increasing concern globally relating to the collection and storage of biometric data:

- Biometric data is usually unalterable. If it is the subject of a breach, it may be difficult to mitigate potential harms resulting from the use of the data by bad actors.
- Biometric data is an inherent part of a person's identity and physical body; there are heightened sensitivities around sharing such information, just as there are with personal health information.
- Biometric data can enable the profiling and monitoring of individuals with extreme precision and without the subject's knowledge, which can be quite alarming in certain contexts.
- Biometric data can be used to discriminate against individuals, for example, by charging them higher prices for services or insurance, or denying them access to certain services.

CIPL acknowledges the legitimate concerns raised by individuals, regulators, and policymakers regarding the collection and use of biometric data. While implementation of specific risk-based protections and heightened requirements for this type of data could alleviate those concerns, any laws or rules applicable to biometrics should be careful not to prevent legitimate uses, such as authentication. (CIPL is currently working on a white paper about beneficial and essential uses of biometric data and will share this paper with the Commission in the coming months.) Nor should any laws or rules permit biometric processing only on the basis of consent, since consent could foreclose legitimate uses, such as airport security.

Facial recognition technology (FRT) applies artificial intelligence to digitized images of individuals. Common functions of FRT include determining the location of a face in a picture; estimating demographic characteristics (e.g., age, gender, race); and identifying specific individuals from a

[90] Texas law, for example, defines a "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry," without further elaboration. Tex. Bus. & Com. Code § 503.001. The law in Illinois is similar, but it goes on to provide examples of what a biometric identifier does not include, such as writing samples, written signatures, and photographs. 740 Ill. Comp. Stat. § 14/10. In contrast, Washington defines a "biometric identifier" more broadly, as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual." Wash. Rev. Code 19.375.010.

[91] "The term 'biometric identifier information' means a physiological, biological or behavioral characteristic that is used to identify, or assist in identifying, an individual, including, but not limited to ... gait or movement patterns …." N.Y.C. Admin. Code § 26-3001.

[92] Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting. 34 CFR § 99.3.

database of facial images.[93] A major debate is currently taking place globally regarding how and in what contexts FRT should be deployed. The debate concerns both private and public sector uses of FRT.[94]

If policymakers choose to regulate the use of FRT specifically, CIPL encourages them to consider:

- adopting a risk-based approach that enables beneficial, low-risk uses of FRT while flagging high-risk applications that would be subject to heightened protections;
- identifying specific contexts where FRT would be prohibited outright in light of available safeguards or lack thereof (e.g., use of FRT by law enforcement).

Q43. To what extent, if at all, should new trade regulation rules impose limitations on companies' collection, use, and retention of consumer data? Should they, for example, institute data minimization requirements or purpose limitations, *i.e.,* limit companies from collecting, retaining, using, or transferring consumer data beyond a certain predefined point? Or, similarly, should they require companies to collect, retain, use, or transfer consumer data only to the extent necessary to deliver the specific service that a given individual consumer explicitly seeks or those that are compatible with that specific service? If so, how? How should it determine or define which uses are compatible? How, moreover, could the Commission discern which data are relevant to achieving certain purposes and no more?

As mentioned in the Executive Summary and elsewhere, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[95] our comments below will focus exclusively on the substance and nature of the issues raised in this question.

While traditional data protection principles of data minimization and purpose limitation are clearly aimed at providing better privacy protections, these principles are increasingly in tension with modern technologies such as AI and blockchain. Continued adherence to these principles without careful consideration of their application to new technologies may undermine substantial benefits and innovations, negatively impacting the digital economy and society.

Access to large amounts of data potentially collected for a different purpose is critical to building analytics models, AI systems, and machine learning algorithms. AI systems in particular need diverse data sets, including sensitive data, to understand and subsequently limit biased and discriminatory outputs. Notwithstanding the data minimization and purpose limitation principles, it can be difficult

[93] FRT: Commercial Uses, Privacy Issues, and Applicable Federal Law, U.S. Government Accountability Office, July 2015, available at https://www.gao.gov/products/gao-15-621.

[94] Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance, June 2021, available at https://www.amnesty.org/fr/documents/doc10/4254/2021/en/.

[95] ANPR, 87 FR at 51277.

to know ahead of time what is "necessary" in the AI context, since the processing of more and more data may lead to new discoveries and correlations, may maximize the accuracy of results, and may improve bias detection and prevention. Moreover, AI technology has the capability of finding new and beneficial uses for old data (e.g., in the financial industry, old data can reveal patterns and identify trends that were unknown at the time of collection, which can be helpful for fraud prevention).

Again, CIPL recommends the adoption of strong accountability- and risk-based safeguards. A risk-based approach is well-suited to evaluating uses that rely on large volumes of data. It would identify unwarranted risks and adverse impacts, while at the same time permitting legitimate and low-risk processing, without creating automatic barriers for certain forms of data collection and storage that may never raise such risks in the first instance (as may be the case under strict data minimization and use limitation rules).

In addition, the notion of "compatible" further uses should be carefully considered so as not to unnecessarily preclude new uses of data that do not raise substantial risks of harm to consumers and that do not interfere with or negate the "original" purpose for which the data was collected. The key consideration of any privacy principle is whether it contains or limits the risk of harm to individuals, but a closely related consideration seeks to enable legitimate and beneficial uses of data. Both considerations can be addressed through comprehensive, risk-based data privacy management programs, particularly in contexts where the traditional principles of data minimization and purpose limitation are in tension with the demands of the digital economy and society.

Q45. Pursuant to a purpose limitation rule, how, if at all, should the Commission discern whether data that consumers give for one purpose has been only used for that specified purpose? To what extent, moreover, should the Commission permit use of consumer data that is compatible with, but distinct from, the purpose for which consumers explicitly give their data?

As mentioned in response to Question 43 (which we incorporate here by reference), the tension between traditional data protection principles and modern technologies such as AI stems from technology's ability to discover unexpected correlations and draw unforeseen inferences from large datasets. Such power may uncover new uses or purposes for old data, such as in the reuse of clinical data to improve healthcare management and reduce healthcare costs.[96] If the purpose limitation principle is interpreted too narrowly, it could stifle further research and innovation, and preclude individuals and society from recognizing the full potential of AI. Nevertheless, the expectations underlying the purpose limitation principle could still be achieved in the AI context by mandating strong accountability-based safeguards, including risk assessments. The key consideration should be whether the processing for the new purpose increases the risk of harm to consumers and whether and how this harm can be minimized or avoided through appropriate accountability measures.

Also, companies seeking to use data for a new purpose should treat new uses of existing data as a collection and use in the first instance, with all the attendant responsibilities, including risk

[96] See Clinical Data Reuse or Secondary Use: Current Status and Potential Future Progress, S. M. Meystre, et al., Aug. 26, 2017, available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6239225/.

assessments. In that light, purpose limitation seems a bit out of place, especially where the new purposes have gone through a risk assessment and risk mitigation steps.

Q46. Or should new rules impose data minimization or purpose limitations only for certain designated practices or services? Should, for example, the Commission impose limits on data use for essential services such as finance, healthcare, or search—that is, should it restrict companies that provide these services from using, retaining, or transferring consumer data for any other service or commercial endeavor? If so, how?

As explained above in response to Questions 43 and 45 (which we incorporate here by reference), CIPL believes that the principles of purpose specification and use limitation must be balanced with the need to allow organizations the flexibility to react to new inferences from old or different data sets and to generally use data for new and beneficial purposes that do not increase the risk of harm to individuals. One way of doing this is by enabling further processing where the new use is "compatible" or "not-incompatible" with the original purpose,[97] which would include all uses that are consistent with, can co-exist with, and do not undermine, conflict with, or negate the original purpose, and where any new risk of harm can be appropriately addressed through targeted mitigations and controls based on risk assessments.

Imposing heightened limits on data use in the context of essential services such as finance, health, or search could have the unintended consequence of preventing beneficial uses of data in exactly the areas where it is most socially beneficial. For example, healthcare delivery networks have deployed AI models to analyse medical insurance data for the purpose of predicting high-risk diseases. Policymakers should seek to promote, rather than inhibit, socially beneficial uses of data such as this.

Q47. To what extent would data minimization requirements or purpose limitations protect consumer data security?

While data minimization and purpose limitation principles are designed to enhance data security as well as consumer privacy, these principles (as noted above) are increasingly in tension with modern technologies such as AI, blockchain, and cloud computing.[98] Limiting data collection, data storage, and data uses may undermine innovation, raise consumer costs, and limit future societal benefits. In that regard, CIPL encourages policymakers to adopt a flexible, risk-based approach that enables contextual collection, processing, storage, and future use decisions based on the actual risk of the

[97] See, for example, the GDPR Art. 5(1)(b), which permits the processing of data for purposes other than those for which the personal data was initially collected where the processing is compatible with the purposes for which the personal data was initially collected. See also GDPR Recital 50.

[98] See CIPL AI First Report: Artificial Intelligence and Data Protection in Tension, October 10, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf; filed herewith as Exhibit 11. See also CIPL AI Second Report: Hard Issues and Practical Solutions, February 27, 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf; filed herewith as Exhibit 7.

proposed processing. Please refer to our responses to Questions 43, 45, and 46—as well as our responses to Questions 2, 24, and 26—for additional information.

Moreover, to the extent that companies seeking to use data for a new purpose would treat the new use as a use in the first instance, thereby satisfying attendant responsibilities, any concerns related to data minimization and purpose limitation principles would be allayed.

Q48. To what extent would data minimization requirements or purpose limitations unduly hamper algorithmic decision-making or other algorithmic learning-based processes or techniques? To what extent would the benefits of a data minimization or purpose limitation rule be out of proportion to the potential harms to consumers and companies of such a rule?

As mentioned in our response to Question 43, access to large amounts of data potentially collected for a different purpose is critical to building analytics models, AI systems, and machine learning algorithms. AI systems in particular need diverse data sets, including (and especially!) sensitive data, to understand and subsequently limit biased and discriminatory outputs. Notwithstanding the data minimization and purpose limitation principles, it can be difficult to know ahead of time what is "necessary" in the AI context, since the processing of more and more data may lead to new discoveries and correlations, may maximize the accuracy of results, and may improve bias detection and prevention. Moreover, AI technology has the capability of finding new and beneficial uses for old data (e.g., in the financial industry, old data can reveal patterns and identify trends that were unknown at the time of collection, which can be helpful for fraud prevention).

Again, CIPL recommends the adoption of strong accountability- and risk-based safeguards. A risk-based approach is well-suited to evaluating uses that rely on large volumes of data. It would identify unwarranted risks and adverse impacts, while at the same time permitting legitimate and low-risk processing, without creating automatic barriers for certain forms of data collection and storage that may never raise such risks in the first instance (as may be the case under strict data minimization and use limitation rules).

In addition, the notion of "compatible" further uses should be carefully considered so as not to unnecessarily preclude new uses of data that do not raise substantial risks of harm to consumers and that do not interfere with or negate the "original" purpose for which the data was collected. The key consideration of any privacy principle is whether it contains or limits the risk of harm to individuals, but a closely related consideration seeks to enable legitimate and beneficial uses of data. Both considerations can be addressed through comprehensive, risk-based data privacy management programs, particularly in contexts where the traditional principles of data minimization and purpose limitation are in tension with the demands of the digital economy and society.

Please also refer to our responses to Questions 45-47.

Q51. To what extent, if at all, should the Commission require firms to certify that their commercial surveillance practices meet clear standards concerning collection, use, retention, transfer, or monetization of consumer data? If promulgated, who should set those standards: the FTC, a third-party organization, or some other entity?

For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7. Again, we note that there are legitimate questions about whether the

Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

Given the Commission's considerable demands in relation to its limited resources, co-regulatory schemes such as certifications or codes of conduct can provide some relief to regulatory and enforcement pressures. CIPL recognizes the Commission's critical role in helping to develop appropriate standards for co-regulatory models and in being the backstop enforcer of these schemes when necessary. For example, the Commission played a significant role in the development of the APEC Cross-Border Privacy Rules (CBPR) requirements and now serves as one of the official backstop enforcement authorities for the CBPR under the APEC Cross-Border Privacy Enforcement Arrangement (CPEA). Now that the CBPR is a global system and in the process of being updated, the FTC should take an active role in that process, in addition to continuing to serve as one of the backstop enforcement authorities for the CBPR.

Certification schemes and codes of conduct involve the use of third-party certifiers, monitoring bodies, and dispute resolution providers. These entities can play important front-line enforcement and oversight roles and remediate many issues before the regulator needs to step in. They review organizations' compliance and accountability programs and ensure that companies comply with the relevant standard to which each was certified. When necessary, they can suspend certifications and take other remedial actions against non-compliant organizations. Dispute resolution functions can relieve the regulator from the burden of dealing with large numbers of "easy" cases, allowing the regulator to focus on more important and strategic matters.

The benefits of such schemes to regulators are numerous:

- **Reduce oversight workload**: Where certification bodies take on and share the burdens of supervision and oversight with the regulator, the regulator's workload is reduced.
- **Improve compliance**: Certifications may result in improved outcomes and more effective on-the-ground compliance due to mandatory periodic re-certification processes and ongoing monitoring requirements, thereby reducing enforcement burdens of the regulator.
- **Reduce complaint handling**: Because certifications may include complaint handling and dispute resolution mechanisms, they can address large numbers of individual complaints. To the extent the regulator does not need to get involved, formal co-regulatory schemes make enforcement easier, freeing the regulator to investigate compliance against specific sets of detailed requirements established by certifications and codes of conduct.
- **Transparency**: Certification requires organizations to disclose their data practices in a transparent and organized fashion vis-à-vis the certification bodies and ultimately the regulator in the event of enforcement. This makes it easier for the regulator to properly assess these practices as well as possible violations of the relevant requirements. This, in turn, may drive down the costs and burdens of enforcement actions, both for the regulator and organizations.

Co-regulatory schemes can also help companies—particularly small and medium-sized enterprises (SMEs)—to meet relevant legal and accountability requirements by relying on existing standards, without having to devise a custom-made program themselves. They enable organizations to readily demonstrate accountability and their program to regulators, business partners, clients, and individuals, creating administrative efficiency and building trust.

However, to encourage uptake of certifications by industry, it is crucial for the certification process to be efficient and scalable. Moreover, it is essential that certifications are effectively incentivized, i.e., clearly accompanied by benefits for certified organizations, such as considering certification as a mitigating factor in enforcement.[99] Otherwise, organizations will be reluctant to invest time and money in obtaining and maintaining certifications on top of the many other requirements to which they are already subject.

In short, such co-regulatory schemes benefit all stakeholders because they augment the capabilities and reach of the regulator and raise the level of overall privacy protections and compliance.[100] See also our response to Question 30.

Q56. To what extent, if at all, should new rules require companies to take specific steps to prevent algorithmic errors? If so, which steps? To what extent, if at all, should the Commission require firms to evaluate and certify that their reliance on automated decision-making meets clear standards concerning accuracy, validity, reliability, or error? If so, how? Who should set those standards, the FTC or a third-party entity? Or should new rules require businesses to evaluate and certify that the accuracy, validity, or reliability of their commercial surveillance practices are in accordance with their own published business policies?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

In general, CIPL opposes highly detailed regulatory requirements. Any proposed laws or regulations should identify expected outcomes and refrain from specifying particular steps. Given the speed at which technology advances, any requirements imposed today may be obsolete within a year. Indeed, AI applications may find new ways of processing personal data that have not been anticipated by regulators or policymakers as yet.

Preventing, detecting, and mitigating bias will be critical to ensure fair outcomes and a trusted AI ecosystem. Adopting a risk-based approach focusing on the use of high-risk data, including more sensitive forms of data, can enable a balancing test to determine whether the benefits of using such data to avoid bias outweigh the risks of processing the data.

When considering proposed laws or regulations on automated decision-making (ADM) systems, policymakers should take the following into account:

- The outcomes intended by some data protection principles (especially data minimization, retention limitation, and purpose specification) could be achieved by mandating strong accountability-based safeguards, including risk assessments, by organizations collecting,

[99] *Supra*, note 77.

[100] See CIPL White Paper: *Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanism*, April 12, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_certifications_discussion_paper_12_april_2017.pdf; filed herewith as Exhibit 16.

using, and storing the data to enable both modern AI processing and a high level of privacy protection for individuals.

- Any laws or regulations should be crafted in consultation with industry, with all stakeholders represented.
- Any laws or regulations should recognize the need to process more data in some AI contexts (e.g., processing of sensitive data to prevent, detect, and mitigate bias).
- Any transparency requirements should be high-level and principles-based to enable the delivery of appropriate and different forms of transparency for a variety of AI contexts.
- Any rules on ADM should not restrict the ability to engage in ADM, but rather focus on ensuring appropriate redress, including through rights of review of automated decisions. This approach provides for an ex post remedy rather than a potentially quickly obsolete ex ante micromanagement of ADM.

For additional information, see CIPL's *Top Ten Recommendations for Regulating AI in Brazil*,[101] as well as CIPL's *Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU*.[102]

Q57. To what extent, if at all, do consumers benefit from automated decision-making systems? Who is most likely to benefit? Who is most likely to be harmed or disadvantaged? To what extent do such practices violate Section 5 of the FTC Act?

Automated decision-making (ADM) systems are everywhere in the digital economy and are fundamental to its proper functioning. To provide just a few examples:[103]

- Banks utilize AI-powered solutions to provide home buyers with real-time digital mortgage support, in turn enabling bank staff to focus on more complex problems.
- Natural language processing models empower universities to engage with a broader pool of prospective students. Digital assistants can provide key admissions information in different languages and around the clock, thereby making the information accessible to a more diverse applicant pool.

[101] *CIPL's Top Ten Recommendations for Regulating AI in Brazil*, October 4, 2022, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipls_top_ten_recommendations_for_regulating_ai_in_brazil__4_october_2022_.pdf; filed herewith as Exhibit 2.

[102] *CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU*, March 22, 2021, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_risk-based_approach_to_regulating_ai__22_march_2021_.pdf; filed herewith as Exhibit 5.

[103] For additional examples and further reading, see *CIPL Comments on WP29's Profiling and ADM Guidelines*, December 1, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf; filed herewith as Exhibit 14.

- Digital farming platforms powered by farm and field data enable farmers to improve food production efficiency, transparency, and sustainability.[104]

Any laws or regulations concerning ADM systems must have dual goals of enabling these systems and making them more reliable and safe. Organizations developing and using these technologies should be encouraged to build best practices and tools that maximize the accuracy and safety of these technologies. Rather than restricting organizations' ability to develop and deploy these new technologies, the focus should be on developing appropriate redress mechanisms (including human review) for decisions with legal impact or similarly significant impact on consumers to ensure a quick resolution for any harms when a possible error in the automated decision has been identified. This approach emphasizes ex post remedies without undermining the development and use of ADM applications where they are needed.

As to whether the use of ADM systems would violate the FTC Act, CIPL again notes that the Commission's authority to stop "unfair … acts or practices in or affecting commerce"[105] requires a **risk assessment** by both industry and the Commission. The FTC's unfairness authority applies only to practices that cause "substantial" injury to consumers that are "not reasonably avoidable by consumers themselves" and are "not outweighed by countervailing benefits to consumers or to competition."[106] Thus, the **FTC Act itself requires a balancing** of both "injuries" and "benefits" in any assessment of unfairness, providing statutory support for a risk-based model.

Q58. Could new rules help ensure that firms' automated decision-making practices better protect non-English speaking communities from fraud and abusive data practices? If so, how?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

As stated above, specific concerns (including those involving vulnerable communities) can and should be included in any risk assessment of ADM practices. See also our response to Question 12.

Q59. If new rules restrict certain automated decision-making practices, which alternatives, if any, would take their place? Would these alternative techniques be less prone to error than the automated decision-making they replace?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

[104] See *10 Ways AI Has The Potential To Improve Agriculture In 2021*, Forbes, February 17, 2021, available at https://www.forbes.com/sites/louiscolumbus/2021/02/17/10-ways-ai-has-the-potential-to-improve-agriculture-in-2021/.

[105] 15 U.S.C. §45(a)(1).

[106] 15 U.S.C.§45(n).

Without specific details on which practices the Commission (or other policymakers) may choose to restrict, CIPL encourages policymakers to familiarize themselves with the contents of two CIPL white papers on artificial intelligence, which we incorporate by reference and make part of the record:

- CIPL AI First Report: Artificial Intelligence and Data Protection in Tension[107]
- CIPL AI Second Report: Hard Issues and Practical Solutions[108]

CIPL's first paper examined some of the tensions that exist between AI technologies and traditional data protection principles. The report concluded that ensuring the protection of personal data will require forward-thinking practices by companies and reasonable interpretation of existing laws by regulators, if individuals are to be protected effectively and society is to enjoy the benefits of advanced AI tools.

The second report takes a deeper dive into examining some of the hardest challenges surrounding AI. It focuses on critical issues for ensuring the responsible use of AI in the context of data protection laws that were often enacted prior to the explosion in AI technologies. The report put forward concrete approaches to resolving the tensions outlined in the first report and provides some key examples of creative approaches and tools that enable human-centric AI, privacy, and the protection of personal data in the AI context.

CIPL also encourages policymakers to review our comments to the Article 29 Data Protection Working Party's Guidelines on Automated Individual Decision-Making and Profiling.[109]

Q73. The Commission invites comment on the effectiveness and administrability of consumer consent to companies' commercial surveillance and data security practices. Given the reported scale, opacity, and pervasiveness of existing commercial surveillance today, to what extent is consumer consent an effective way of evaluating whether a practice is unfair or deceptive? How should the Commission evaluate its effectiveness?

For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7. Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

[107] CIPL AI First Report: *Artificial Intelligence and Data Protection in Tension*, October 10, 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf; filed herewith as Exhibit 11.

[108] CIPL AI Second Report: *Hard Issues and Practical Solutions*, February 27, 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_second_report_-_artificial_intelligence_and_data_protection_-_hard_issues_and_practical_solutions__27_february_2020_.pdf; filed herewith as Exhibit 7.

[109] *CIPL Comments on WP29's Profiling and ADM Guidelines*, December 1, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_automated_individual_decision-making_and_profiling.pdf; filed herewith as Exhibit 14.

Consent is often regarded as a desirable, easy-to-use ground for processing personal data that gives choice to individuals. In practice, however, consent can be cumbersome, transient, and both overwhelming and meaningless for individuals who face a barrage of requests without the time, inclination, or capacity to review them to the level required for informed decision making. Consent can also be difficult to collect, as it must often meet certain standards to be considered valid. Opt-in consent, which requires an affirmative or explicit action from the individual, is often the norm, while opt-out consent (or implied consent that can be inferred from the individual's behavior) remains the exception.

As noted above, opt-in consent results in consent fatigue, which will only increase as activities are digitalized and data is collected, used, and shared by default in the digital economy. Thus, opt-in consent often undermines and devalues effective privacy protection by discouraging individuals from reviewing privacy notices that purport to provide meaningful notice.

In light of these constraints, CIPL encourages policymakers to consider moving away from the traditional consent model and instead establish an accountability-based model, which places the burden on organizations, not individuals, to prevent harms. This will help deliver far stronger protections for individuals.

Of course, consent should still be enabled where it is appropriate and meaningful, but where not appropriate or effective, consumers should be protected through other elements of organizational accountability, such as risk/benefit assessments and rights of redress, as discussed in our responses to earlier questions. See, in particular, our responses to Questions 18-19, 24, 26, and 57.

Moreover, as discussed more fully in our response to Question 2, the Commission should also consider the use of Privacy Enhancing Technologies (PETs) and Privacy Preserving Technologies (PPTs) as a means to protect consumer data.

Q74. In which circumstances, if any, is consumer consent likely to be effective? Which factors, if any, determine whether consumer consent is effective?

As noted in our response to Question 73, consent often undermines, rather than advances, effective privacy protection. Overreliance on consent can undermine the quality of the consents obtained, and it oftentimes fails to achieve the desired purpose of putting individuals in control.

There are many contexts and circumstances in the modern information age where obtaining consent can be impractical, impossible, ineffective or not meaningful, including:

- where there is no direct interaction with individuals;
- where the data use is common and carries little risk;
- where large and repeated volumes of data are processed;
- where consent is considered invalid because it is obtained from a vulnerable individual (such as a child) or one who lacks true bargaining power (such as an employee granting consent to an employer);
- where obtaining consent would be counterproductive, such as where data is processed to prevent fraud or crime, or to ensure information and system security; or
- where consent requests are too frequent.

To counter consent fatigue, organizations should be encouraged to consider using consent only where it is a meaningful basis for processing individuals' data. In cases where this is not so, there are an array of accountability-based measures organizations can implement that can effectively protect individuals while also enabling data processing.

However, there are situations where requiring consent is appropriate, such as deciding with whom to share social media posts, or responding to a market research survey or to an employee engagement survey that seeks data in protected categories. Moreover, in cases where consent could be effective, it may not have to be affirmative or express consent; consent may be deemed or implied in situations where processing is low risk and within the reasonable expectations of individuals.

A practical use of "**deemed consent**" can be observed in Singapore, where the Personal Data Protection Act (PDPA) introduces the concept of "deemed consent." Accordingly, individuals can be deemed to have given consent when they voluntarily provide their personal data for a specific purpose, and it is reasonable that they would voluntarily provide such data. There are three forms of "deemed consent":

- **Deemed consent by conduct** applies where individuals voluntarily provide data to the organization and the purposes are limited to what is objectively obvious and reasonably appropriate based on the circumstances. Consent is deemed to be given to the extent that individuals intended to provide their data and have taken the actions required for the data to be collected by the organization. The organization must inform individuals about the processing and its purposes.
- **Deemed consent by contractual necessity** is where the disclosure of personal data by one organization to another is necessary for the conclusion or performance of a contract or transaction between the individual and the first organization.
- **Deemed consent by notification** applies where individuals are deemed to have consented to a particular processing of which they had notice and chose not to opt out. This is particularly relevant where an organization wants to use existing data for secondary purposes. Relying on deemed consent by notification is subject to a prior assessment to ensure that the processing is not likely to have an adverse effect on the individual and that the individual has been provided with the opportunity to opt-out of the processing.

Thus, it is possible to enable data processing without creating consent fatigue by (1) establishing an accountability-based model that provides for a range of accountability measures that protect and empower individuals even in the absence of consent; (2) permitting legal bases for processing other than consent; and (3) recognizing the concept of "deemed consent."

CIPL also stresses that consent is not the best or only way to empower individuals, even in cases where consent may be practicable.[110] Other ways to empower individuals include providing user-centric transparency about relevant data practices and providing access and correction rights with respect to consumers' personal data. Access and correction and related individual rights are common in global privacy laws, and they should be considered in the U.S. as well. Most importantly, as we have stressed

[110] See *Empowering Individuals Beyond Consent*, by Bojana Bellamy and Markus Heyder, July 2, 2015, available at https://iapp.org/news/a/empowering-individuals-beyond-consent/.

throughout this response, placing the onus on organizations to be accountable in their data privacy management practices—especially through the use of risk assessments and risk mitigation measures—is key to protecting individuals from substantial harms.

Q76. To what extent should new trade regulation rules prohibit certain specific commercial surveillance practices, irrespective of whether consumers consent to them?

As mentioned in the Executive Summary and elsewhere, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[111] our comments below will focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

As discussed above (see, in particular, our responses to Questions 24 and 26), CIPL believes that most data uses can be vetted by **contextual risk assessments**, which enable organizations to implement targeted risk mitigations and controls, or, where risk mitigation is questionable, to seek advice from the regulator. Such risk assessments should be conducted on the basis of regulatory guidance that describes the relevant cognizable harms to be considered, the categories of data and data uses that are more likely to be high risk, and the appropriate methodologies for any assessment. This approach could include a list of presumptively prohibited high-risk practices, but the presumption should be rebuttable through specific risk assessments in specific processing contexts or in consultation with the regulator. Equally, there could be regulatory guidance on routine, low-risk processing operations that typically would require no formal risk assessments. But there, too, the burden should be on organizations to determine if, in particular contexts, these "low-risk" practices warrant a more in-depth privacy risk assessment.

Q77. To what extent should new trade regulation rules require firms to give consumers the choice of whether to be subject to commercial surveillance? To what extent should new trade regulation rules give consumers the choice of withdrawing their duly given prior consent? How demonstrable or substantial must consumer consent be if it is to remain a useful way of evaluating whether a commercial surveillance practice is unfair or deceptive? How should the Commission evaluate whether consumer consent is meaningful enough?

As mentioned in our response to the previous question, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[112] our comments below will focus exclusively on the substance and nature of the issues raised in this

[111] ANPR, 87 FR at 51277.

[112] ANPR, 87 FR at 51277.

question. For CIPL’s comments on the Commission’s use of the term “commercial surveillance,” please refer to our response to Question 7.

As highlighted in our responses to Questions 73 and 74, policymakers should consider establishing an accountability-based model, which places the burden on companies, not individuals, to prevent potential harms. Under that approach, organizations would use risk assessments to consider whether a proposed data use is appropriate and respectful of consumers’ privacy (for example, a consideration of whether anonymization or aggregation of data would sufficiently allay consumers’ privacy concerns). The risk assessment would also consider whether consent would be appropriate and, if so, in what way it should be obtained.

Whether and how to enable revocation of consent would depend on context. For example, if the consented-to use involves research, then revoking consent for that purpose may not be possible given its potential impact on the integrity of the data set. Thus, consent may either not be the best basis for processing in that context, or revocation may not be possible. Where revoking consent is possible, it should be enabled in multiple ways, depending on the circumstances.

Q78. What would be the effects on consumers of a rule that required firms to give consumers the choice of being subject to commercial surveillance or withdrawing that consent? When or how often should any given company offer consumers the choice? And for which practices should companies provide these options, if not all?

First, any answer to this question would require consideration of the specific “surveillance” activity at hand. (For CIPL’s comments on the Commission’s use of the term “commercial surveillance,” please refer to our response to Question 7.)

Second, whenever the question arises whether an organization should obtain consent from consumers, the relevant questions to ask include:

- Will consent protect the consumer from a potential harm? If so, how?
- Can the organization protect the consumer from this harm through accountability- and risk-based measures that obviate the need to involve the consumer in the decision?
- If the proposed data use is beneficial to society (e.g., medical research or a wide range of data-for-good projects) and if it can be conducted without exposing consumers to inappropriate risks, should individual consumers be able to opt out, thereby undermining the larger good? Why or why not?
- What would be the aggregate impact on data security, innovation, scientific progress, and data use for societal good at large be if individual consumers opted-out or refused to consent, particularly in cases that do not involve substantial risks to them?

These are complex questions that go to the validity of the consent model. Any future laws or regulations on this subject should be based on careful consideration of these questions.

Q81. Should new trade regulation rules require companies to give consumers the choice of opting out of all or certain limited commercial surveillance practices? If so, for which practices or purposes should the provision of an opt-out choice be required? For example, to what extent should new rules require that consumers have the choice of opting out of all personalized or targeted advertising?

For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7. Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

See our response to Question 78. Further, CIPL believes that any implementation of consent must be adapted to the modern information age, where individuals interact with technology in nearly every aspect of their lives. Individuals will not and should not expect to have to legitimize every single use of data or every single processing operation. In fact, individuals will expect organizations to use their data responsibly when developing products, offering services, and conducting research. That said, a contextual risk assessment would help companies identify when an option to opt out would be appropriate.

Q82. How, if at all, should the Commission require companies to recognize or abide by each consumer's respective choice about opting out of commercial surveillance practices—whether it be for all commercial surveillance practices or just some? How would any such rule affect consumers, given that they do not all have the same preference for the amount or kinds of personal information that they share?

Please see our responses to Question 76 and Question 81.

Q83. To what extent should the Commission consider rules that require companies to make information available about their commercial surveillance practices? What kinds of information should new trade regulation rules require companies to make available and in what form?

As mentioned in the Executive Summary and elsewhere, there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. However, since the Commission has invited comments to generate a public record for purposes of informing not only its potential actions, but also those of Congress and other policymakers,[113] our comments below will focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

Transparency is critical for enabling consumer trust and goes beyond pure legal compliance. By effectively informing individuals about the protection and use of their personal data, including benefits of data processing, and by addressing the concerns of regulators, transparency will have the

[113] ANPR, 87 FR at 51277.

effect of raising the level of digital education, broadening individuals' expectations, increasing their acceptance of and support for certain data uses, and generally deepening individuals' and regulator trust. This in turn will enable organizations to use data for wider and more beneficial purposes, and also encourage competition around the most effective transparency.

There is obvious tension between a requirement to provide detailed notices to individuals for each data processing activity and a requirement that notices be "clear and concise." Where the goal is to provide understandable and actionable information to individuals, it is challenging to systematically communicate every complex detail. There needs to be an effort to find a balance between clarity and completeness—and to resolve this balance in favor of clarity through innovative ways of delivering required information.

In many jurisdictions, "transparency" means that organizations need to provide the following "key" information in a "concise and intelligible" manner:

- all purposes of processing;
- reliance on the legitimate interest processing ground;
- the logic in automated decision making;
- use of third parties to process data;
- cross-border data transfers;
- data retention period; and
- individuals' rights (access, rectification, objection, etc.).

CIPL believes that satisfaction of the transparency principle must be **contextual** and must allow appropriate discretion to organizations. Transparency must take into account the nature of the services being provided and the relationship between the organization and its customers/individuals. It must give individuals understanding and clarity about the products and services they are obtaining and the use of their personal data in that context. Of course, some information must always be provided, but that should be the most important information to enable choices or deliver user-centric transparency. The rest should be made available to individuals in an accessible location or manner. This approach is also in line with the layered notices approach.[114]

Additionally, organizations should be encouraged to develop transparency technology that understands and reacts to the user. Examples are user-friendly chat boxes or chatbots. Machine-learning should play a role, as should human interfaces.

Furthermore, it is important to highlight that transparency cannot be absolute. Transparency is an essential element of effective data protection, but it is subject to limitations imposed by the complexities of the modern digital economy and other rights and freedoms. This must be recognized. There should be a number of factors that define the limits. For instance, transparency may be limited by trade secrets, commercial, and competitive considerations, other intellectual property rights, as well as by rights of other individuals. Equally, there may be cases where full transparency to individuals

[114] CIPL White Paper: *Recommendations for Implementing Transparency, Consent and Legitimate Interest Under the GDPR*, May 19, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf; filed herewith as Exhibit 15.

may be inconsistent with public interest considerations, or may prejudice organizations' ability to conduct essential and common data processing (such as for fraud prevention, corporate investigations, or network security).

Q84. In which contexts are transparency or disclosure requirements effective? In which contexts are they less effective?

Transparency is related to the fair processing principle. Processing can be fair only if it takes place in a transparent manner. However, transparency can serve its purpose only if it is meaningful. There currently is a growing gap between legal transparency and user-centric transparency. Concise and intelligible privacy notices focusing on truly informing users by providing meaningful information are at the heart of user-centric transparency.

Transparency should be context-specific, flexible, and dynamic. It should be adaptable to constantly evolving and changing uses. It must provide clear and understandable information to enable a genuine choice where possible. User-centric transparency is about delivering relevant information as part of the customer relationship and digital trust. It should explain the benefits of data use and the value of the product or service, along with organizational accountability and available choices. However, even where choices are not available, transparency is still necessary to provide relevant information about processing activities, risk mitigation measures, individuals' rights, and other accountability-based practices.

Transparency must be provided by appropriate methods and at appropriate times throughout the lifecycle of the data and the individual's use of the underlying products or services. Transparency should make it possible to understand the processing of personal data *ex ante* and *ex post,* enabling individuals to exercise their rights at the appropriate time. One way to provide ongoing transparency and control would be periodic reminders about data and privacy settings, while also retaining the organization's flexibility to adjust to the specificities of a given service, circumstance, or user expectation.

Transparency should be designed to provide relevant, timely, and digestible information to individuals when and where it is most meaningful to them. This can be done both based on the "push" model (proactively providing just-in-time transparency) and the "pull" model (making information available to individuals at their convenience, e.g. permission management, transparency dashboards, and "learn more" tutorials). Such mechanisms can be delivered via a combination of tools, such as privacy policies, layered notices, just-in-time notices, dashboards, control panels, custom-built apps, tutorials, user guides, interfaces, etc.

Moreover, transparency should be driven not only by the legal requirements but also by the real needs, interests, and concerns of individuals with respect to data processing. These can be determined by researching and testing how people actually interact with services and discovering their concerns about the use of data.

Finally, algorithmic transparency vis-à-vis individuals and the general public must be achieved in a manner that is realistic and effective in practice. Algorithmic transparency should be focused on the broad logic involved and not the detailed workings of algorithms. Significantly, organizations should be transparent about the specific sets of input and output values and should ensure that the sets are both accurate and correctible.

As mentioned in response to Question 83, there is obvious tension between a requirement to provide detailed notices to individuals for each data processing activity and a requirement that notices be "clear and concise." Where the goal is to provide understandable and actionable information to individuals, it is challenging to systematically communicate every complex detail. There needs to be an effort to find a balance between clarity and completeness—and to resolve this balance in favor of clarity through innovative ways of delivering required information. Indeed, laws that require detailed notices are often less effective, as individuals will not read long notices. CIPL supports an accountability-based approach, which would allow organizations to determine what and how much individuals would want to know in a given circumstance.

Q89. To what extent should trade regulation rules, if at all, require companies to explain (1) the data they use, (2) how they collect, retain, disclose, or transfer that data, (3) how they choose to implement any given automated decision-making system or process to analyze or process the data, including the consideration of alternative methods, (4) how they process or use that data to reach a decision, (5) whether they rely on a third-party vendor to make such decisions, (6) the impacts of their commercial surveillance practices, including disparities or other distributional outcomes among consumers, and (7) risk mitigation measures to address potential consumer harms?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

All of the elements listed in Question 89 are relevant and important categories for transparency purposes. However, the level of detail organizations provide on each of these issues depends on the context; the level of detail should be left to organizations' judgment based on a reasonable assessment of what is important to consumers in connection with the business and data practices at hand.

Q90. Disclosures such as these might not be comprehensible to many audiences. Should new rules, if promulgated, require plain-spoken explanations? How effective could such explanations be, no matter how plain? To what extent, if at all, should new rules detail such requirements?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

CIPL believes that transparency is only effective if the disclosure is comprehensible. Presenting all of the information listed in Question 89 at the time of collection will undermine the very transparency the Commission is seeking to achieve; it would overwhelm users with information that in many cases they simply do not wish to actively consume. Thus, specific or just-in-time privacy notices should be reserved for actionable information and should be limited to cases where the provision of such information is warranted, such as where there is a higher risk associated with the processing, or where there are unexpected uses of data, or in cases of sharing with third parties that is outside the normal provision of the services. Again, a layered-notice approach should remain an option.

Q91. Disclosure requirements could vary depending on the nature of the service or potential for harm. A potential new trade regulation rule could, for example, require different kinds of disclosure tools depending on the nature of the data or practices at issue (*e.g.,* collection, retention, or transfer) or the sector (*e.g.,* consumer credit, housing, or work). Or the agency could impose transparency measures that require in-depth accounting (*e.g.,* impact assessments) or evaluation against externally developed standards (*e.g.,* third-party auditing). How, if at all, should the Commission implement and enforce such rules?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question.

Ideally, organizations implement accountability measures via comprehensive organizational data privacy management programs addressing all aspects of data governance, privacy law compliance, and the data cycle, including transparency and disclosure matters. Thus, as explained in our responses to Questions 83, 84, 89, and 90, CIPL believes that the means of delivering transparency and its content must be contextual and allow for appropriate discretion to organizations. Because a key element of accountability is risk assessment, accountability with respect to transparency should include information on how potential risks will be mitigated.

Q92. To what extent should the Commission, if at all, make regular self-reporting, third-party audits or assessments, or self-administered impact assessments about commercial surveillance practices a standing obligation? How frequently, if at all, should the Commission require companies to disclose such materials publicly? If it is not a standing obligation, what should trigger the publication of such materials?

Again, we note that there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR. Our comments below focus exclusively on the substance and nature of the issues raised in this question. For CIPL's comments on the Commission's use of the term "commercial surveillance," please refer to our response to Question 7.

Organizational accountability frameworks such as the CIPL Accountability Framework require organizations to implement comprehensive privacy management programs and to be able to demonstrate the existence and effectiveness of these programs and all their component parts on request, both internally (to their boards and senior management) and externally (to privacy enforcement authorities, business partners, and increasingly, shareholders and investors). This includes being able to demonstrate the risk assessments that the organization has conducted with respect to its data practices. Given the demonstrability requirement, we do not believe it is necessary to impose additional and routine self-reporting requirements or audits. However, we do believe that external audits may be a helpful tool for organizations to use in building and assessing effective privacy management programs.

III. Conclusion

In sum, while there are legitimate questions about whether the Commission can or should undertake broad-based regulatory action of the type envisioned in the ANPR, we offer the following bullets to help frame the discussion on the substance and nature of the issues raised. Any potential action addressing comprehensive privacy measures should strive for an **outcomes-based approach** that:

- promotes effective, targeted protections for consumers;
- enables innovative and responsible data uses;
- provides businesses with robust, flexible, and future-proof legal bases for processing consumer data, including legitimate interests;
- incorporates accountability-based practices that include **risk assessments**;
- acknowledges that risk is inherent in any use of consumer data;
- recognizes that risk mitigation does not mean the elimination of risk, but rather the reduction of risk to the extent practicable;
- indicates that companies are best placed to understand the risks raised by their own processing activities, and, therefore, are best placed to identify and implement appropriate mitigation measures;
- endorses **contextual** risk assessments so that companies may:
    - tailor their compliance measures to their unique risks and use cases;
    - evaluate the sensitivity of data and the attendant level of risk in context;
    - identify and prioritize high-risk processing;
    - identify legitimate and beneficial uses of data;
    - evaluate individual, organizational, and societal benefits;
    - identify appropriate mitigations for a given context and a given use;
    - document their compliance and be able to explain and defend their processing decisions under relevant legal standards, such as “unfairness”;
- does not unnecessarily encumber legitimate business practices or thwart data-driven innovation;
- supports Privacy Enhancing Technologies (PETs) and Privacy Preserving Technologies (PPTs);
- provides guidance on appropriate risk criteria, frameworks, and methodologies; and
- is drafted after engagement and discussions with stakeholders.

IV. APPENDIX

CIPL has uploaded the following documents in support of our comments and requests that these documents be made part of the public record:

1. CIPL White Paper: Protecting Children's Data Privacy, Policy Paper I, International Issues and Compliance Challenges, October 22, 2022.
2. CIPL's Top Ten Recommendations for Regulating AI in Brazil, October 4, 2022.
3. CIPL White Paper: Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions, October 6, 2021.
4. CIPL White Paper: How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation, July 1, 2021.
5. CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU, March 22, 2021.
6. CIPL Report: What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, Report of the CIPL Accountability Mapping Project, May 2020.
7. CIPL AI Second Report: Hard Issues and Practical Solutions, February 27, 2020.
8. CIPL Discussion Paper: Organizational Accountability in Light of FTC Consent Orders, November 13, 2019.
9. CIPL White Paper: The Concept of "Organizational Accountability" Existence in US Regulatory Compliance and its Relevance for a Federal Data Privacy Law, July 3, 2019.
10. CIPL White Paper: Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice, March 8, 2019.
11. CIPL AI First Report: Artificial Intelligence and Data Protection in Tension, October 10, 2018.
12. CIPL Accountability Discussion Paper 2 - Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability, July 23, 2018.
13. CIPL White Paper: GDPR Implementation in Respect of Children's Data and Consent, March 2018.
14. CIPL Comments on WP29's Profiling and ADM Guidelines, December 1, 2017.
15. CIPL White Paper: Recommendations for Implementing Transparency, Consent and Legitimate Interest Under the GDPR, May 19, 2017.
16. CIPL White Paper: Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanism, April 12, 2017.
17. CIPL White Paper: The Role of Risk Management in Data Protection, November 23, 2014.
18. CIPL White Paper: A Risk-based Approach to Privacy: Improving Effectiveness in Practice, June 19, 2014.