CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

REIMAGINING PRIVACY IN THE AI ERA: PERSONAL DATA PRIVACY AS A PUBLIC GOOD

A call for shared responsibility and stronger protections to safeguard consumer privacy in the digital age.

ARTIFICIAL INTELLIGENCE IS MAKING INDIVIDUAL PRIVACY CHOICES INADEQUATE

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

Fifty years ago, personal data was largely private by default.[i] Today, it can be shared, sold, or traded instantly, with or without your consent. The global consumer movement calls for urgent action to protect privacy. Consumers need stronger collective protections to ensure personal data is used responsibly, transparently and fairly in the AI era.

Privacy can no longer be managed through individual choices alone. Protecting it should be a shared responsibility, not a private burden.

THE PROBLEM: CONSUMERS ARE BEING ASKED TO MANAGE SYSTEMIC PRIVACY RISKS

Privacy is treated as each individual's responsibility: read lengthy policy notices, manage complex settings, and exchange personal data for digital services.

That approach no longer reflects how artificial intelligence[ii] (AI) uses consumer data. AI systems can now predict information about us that we never explicitly shared,[iii] with unclear consequences driven by design choices and lack of governance. The harms could include being charged more, denied credit or insurance, steered toward less favourable options, or targeted based on inferred characteristics. Consumers in vulnerable circumstances are often the hardest hit and have the fewest avenues for recourse.

90% of consumer advocates worldwide identify privacy and safety as the leading consumer risks from AI.[iv]

OUR CALL: MAKE PRIVACY A SHARED PROTECTION

To treat privacy like a public good – such as clean air or road safety – with protections that work for everyone rather than placing the burden on individuals. Our call to action sets out six principles, developed with consumer organisations, to help advance consumer advocacy, guide responsible business practice and support stronger regulation.

The goal is simple: to ensure that nobody can use our data to charge us more, exclude us unfairly, or exploit our vulnerabilities. A public good approach does not mean using less data. It means managing data in a way that maximises public benefit while minimising harm.

THE PAY-OFF: STRONGER PRIVACY BUILDS TRUST IN THE DIGITAL ECONOMY

Privacy is an important factor in fostering trust and confidence in the digital economy. Transparent, responsible and accountable systems reduce risks, enable safe and fair use of data, and empower consumers to engage confidently with digital services. Strong privacy protections strengthen consumer confidence and help ensure that innovation delivers benefits for everyone.

As AI enables providers to collect, predict, and use ever more information, personal data privacy concerns continue to grow.

Providers that protect privacy can have a competitive advantage, but only where consumers have real opportunities to choose, switch, and take their data elsewhere.

Definition: Provider An organisation that develops or operates data systems at scale, using personal data to make decisions, personalise services, or influence consumer outcomes.

WHAT IS PRIVACY AND WHAT IS A PUBLIC GOOD?

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

PRIVACY means having control over how your personal information and data is collected, used and shared.[v]

A PUBLIC GOOD is a resource or condition whose benefits and harms are shared across society, requiring collective governance rather than individual management.

78% of consumers in the United States would support a law regulating how companies can collect, store, share, and use our personal data.[vi]

PUBLIC GOODS HAVE TWO KEY CHARACTERISTICS

NON-EXCLUDABLE: people cannot avoid being affected.
NON-RIVALROUS: one person's benefit does not reduce the benefit available to others.

	EXCLUDABLE	NON-EXCLUDABLE
RIVALROUS	PRIVATE GOODS food, clothes, cars	COMMON GOODS fish, timber, coal
NON-RIVALROUS	CLUB GOODS cinemas, gyms, private beaches	PUBLIC GOODS clean air, road safety

EXAMPLES OF PUBLIC GOODS

CLEAN AIR: no individual can opt out of air pollution, and one person's exposure to it does not reduce another's. Society relies on collective protections, such as emissions standards and air-quality regulations, rather than expecting individuals to manage the risk for themselves.

ROAD SAFETY: safe roads, safer vehicles, speed limits and seatbelt laws protect everyone, including those who personally choose to forgo such protections. Individual consent is not the governing principle for road safety.

PRIVACY is not a textbook public good, but it increasingly works in the same ways. AI creates risks that affect everyone making collective protections increasingly necessary.

SIX PRINCIPLES FOR PRIVACY AS A PUBLIC GOOD

If privacy is a shared condition rather than an individual responsibility, we need shared rules that protect everyone. Our framework is built around six principles:

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

1 DATA SERVES THE CONSUMER INTEREST FIRST

Providers should use personal data in ways that benefit consumers and are consistent with the purpose for which the data was collected.

2 SAFEGUARD AGAINST HARMFUL AI PROFILING

Protect people not only from excessive data collection, but also from harmful predictions and profiling.

3 ENSURE ACCOUNTABILITY AND EFFECTIVE ENFORCEMENT

Consumer protection should be built into AI systems, markets and regulatory frameworks, rather than relying on individuals to safeguard their own rights.

4 ENABLE EASY EXIT, PORTABILITY AND REAL CHOICE

Consumers should be able to move and delete their data without barriers.

5 MANDATE PRE-TESTING, MONITORING AND HUMAN INTERVENTION

AI systems should be tested, monitored and audited before and after deployment for privacy guardrails. Because systemic harms can be difficult to detect, oversight should focus on real-world outcomes as well as compliance with regulatory requirements.

6 ENSURE EFFECTIVE REMEDY AND REDRESS FOR PRIVACY HARMS EXPERIENCED

Consumers must be able to understand decisions, challenge outcomes and obtain timely redress when privacy harms occur.

PROTECTING PERSONAL DATA PRIVACY TOGETHER

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

WHY SHOULD PRIVACY BE TREATED LIKE A PUBLIC GOOD?

Consumers cannot protect themselves alone.

Even if you do not share your own data, providers can infer information about you from the data of your family, friends, or people like you. The reverse is also true: your data can reveal information about others who have shared nothing themselves. Privacy is therefore a shared condition. No individual can fully protect it – or consent it away – on their own.

AI has turned privacy into a collective issue.

Many of today's privacy risks are collective, rather than individual. That's because AI can learn things about you from information about other people who are similar to you, even if you never shared that information yourself. Treating privacy as a public good places governance responsibilities on the actors best able to manage these collective risks, rather than leaving consumers to address them alone.

Businesses cannot solve the problem alone.

Even companies committed to stronger privacy practice face a collective-action problem. Acting alone can create a competitive disadvantage if rivals continue to extract and monetise excessive consumer data. Shared rules let firms move together without any one of them paying the price of going first.

Privacy is about fairness, not secrecy.

Privacy is not about having something to hide. It is about ensuring personal information cannot be used to charge people more, exclude them unfairly from opportunities, manipulate their choices, or exploit their vulnerabilities. Even seemingly harmless data can be combined and analysed to affect people's lives in ways they may never see or understand.

The greatest harms fall on those least able to bear them.

AI can reinforce discrimination, manipulation, and unfair classification of consumers at a scale no individual can identify or contest. Consumers in vulnerable situations are often affected most, amplifying existing inequalities.[vii]

Self-management places a heavy burden on consumers.

Today's notice-and-consent models expect consumers to police their privacy across every service. In practice, many consumers feel they have little meaningful choice but to share their data to access digital services. Privacy protection should not depend on individual vigilance.

TODAY'S AI-DRIVEN DATA ECONOMY EXPOSES CONSUMERS TO HARM AT EVERY STAGE

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

STEP 1:

Data is collected for uses beyond serving the consumer.

A dominant business model treats consumer data as a raw material to be extracted, processed, and monetised beyond what benefits the consumer. Data sharing can deliver real benefits, in scams or fraud prevention[viii] – and consumers may value personalisation where it is appropriate. However, collecting more data than necessary creates opportunity for harm.

EXAMPLE: BANK USES DATA TO STOP SCAM

A bank detects an unusual payment and stops a scam before money leaves a customer's account. This protects consumers because the data is used for a clear purpose. By contrast, collecting, reusing and trading data without clear limits removes that protection. The consumer value requires a defined purpose.

STEP 2:

Unauthorised creation of new data and profiles of the consumer.

AI takes the existing data from Step 1 to generate new behavioural profiles and predictions about people, including information they never explicitly shared. These predictions evolve at a speed and scale that outpace individual consent frameworks, and existing safeguards often do not adequately govern how these predictions are created or used.[ix]

EXAMPLE: LOYALTY SCHEME DATA USED BEYOND CONSENT

A consumer joins a supermarket loyalty scheme and agrees to receive personalised offers. Years later, the same shopping data is used by an AI system to predict sensitive characteristics, such as health risks, financial stress or major life changes. The resulting profile is shared with third parties the consumer never expected to interact with. Their original consent did not extend to creating or sharing this behavioural profile.

STEP 3:

Opaque AI decisions impact the consumer's access to products and services, with unclear redress.

Predictions made in Step 2 can influence prices, products and opportunities, often without people knowing or being able to challenge the outcome.[x]

EXAMPLE: MORTGAGE RATE CALCULATION WITH NO EXPLANATION

A consumer renews their mortgage and is quoted a higher rate than expected. Rather than relying on traditional factors –such as age, postcode, claims history – the lender's AI pricing system analyses a broad range of data to predict risk and profitability, potentially drawing conclusions about the consumer from personal data that they never disclosed. The consumer receives no clear explanation for the higher rate and has little opportunity to understand, question or challenge the outcome.

BUILDING A DIGITAL ECONOMY THAT PROTECTS CONSUMERS AND DELIVERS WIDER BENEFITS

A public good approach does not mean we need less data. It means managing data in ways that maximise benefits for consumers while minimising harm.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

TRUST AND DIGITAL PARTICIPATION

Consumers should be able to use digital services without feeling they must give up their privacy in return. Strong baseline protections reduce uncertainty about how personal data is collected, used and shared. When privacy is protected by default, consumers can participate in the digital economy with greater confidence.

EXAMPLE

A consumer can attend a public event or use an essential service without their presence being tracked, profiled or targeted for unrelated commercial purposes.

MORE EFFICIENT MARKETS

Today's privacy framework often relies on individuals identifying problems after harm has already occurred. A public good approach shifts responsibility to providers and regulators to prevent harm in the first place. Clear rules and accountability create greater certainty for consumers and businesses alike.

EXAMPLE

Food safety protects everyone who buys food, not just those who read labels. Data privacy should work the same way, with protections built into the system rather than relying on consumers to manage every risk themselves.

GREATER CHOICE AND INNOVATION

Today, services with the most users often have the greatest data advantage: more data can strengthen products, improve targeting and reinforce market power. Strong privacy protections, combined with effective portability and switching rights, can create opportunities for new services to compete on quality, trust and innovation rather than on the volume of data they have accumulated.

EXAMPLE

A provider that offers privacy-protective services can compete by earning consumer trust, rather than by collecting ever more personal information.

ECONOMIC GROWTH THROUGH TRUST

Trust is a foundation of the digital economy. We contend that when consumers believe their data will be used responsibly, they are more willing to engage with new technologies and services. Businesses benefit from stronger customer relationships, while innovators can develop products that create value without relying on increasingly intrusive data practices. Shared privacy protections also help ensure businesses compete on trust and innovation, rather than on how much consumer data they can extract.[xi]

HOW WE CAN ACHIEVE THIS: CORE PRINCIPLES OF PRIVACY AS A PUBLIC GOOD

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

If privacy is a collective condition rather than an individual responsibility, governance should shift from managing consumer choices to shaping the behaviour of providers and systems. These six principles provide a framework for doing so.[xii]

PRINCIPLE 1: DATA SERVES THE CONSUMER INTEREST FIRST

Providers should use personal data in ways that benefit consumers and are consistent with the purpose for which the data was collected.

- **Heightened standards for people at greater risk.** AI systems should apply stronger protections – such as disabling profiling and targeting and applying protective settings by default – when processing data relating to children, older consumers or others who may be more vulnerable to harm.
- **Fair treatment of data, regardless of consent.** All data collection and use should be fair and proportionate, whether or not a consumer has given consent. Consent cannot authorise unfair processing that creates harm or unreasonable risk, and one person's consent cannot authorise processing of another's data.
- **Use privacy-preserving technologies.** Providers should prioritise approaches that deliver utility, including personalisation where relevant, without requiring mass collection of personal data. Technology already makes this possible.[xiii]
- **Maintain strong security standards.** Providers should maintain security standards proportionate to the sensitivity of the data they hold and the scale at which they operate. A privacy framework that can be undermined by a preventable breach is not functioning in the public interest. Security obligations should be continuous and auditable.

PRINCIPLE 2: SAFEGUARD AGAINST HARMFUL AI PROFILING

Protect people not only from excessive data collection, but also from harmful predictions and profiling.

- **No automatic data reuse for AI training.** Data collected for one purpose should not be repurposed to train AI systems in ways that conflict with applicable law, privacy obligations, contractual commitments, or reasonable consumer expectations. Such uses should be governed from the point of collection and subject to transparency, proportionality, and oversight.
- **Limits on predicted data and profiles.** Obligations should extend to what AI systems are permitted to predict and act on – including health status, financial vulnerability, and values or beliefs predicted from other information – not just the data collected. Limits should be proportionate: the greater the potential impact on consumer's access to services, jobs, or other consequential outcomes, the stronger the controls should be.
- **Prohibited and restricted uses.** Certain data uses should be prohibited regardless of consent, including predicting protected characteristics in ways that enable unlawful discrimination, unfair treatment, exploitation, or manipulation; targeting based on vulnerability; or using behavioural profiles to manipulate decision-making.

PRINCIPLE 3: ENSURE ACCOUNTABILITY AND EFFECTIVE ENFORCEMENT

Consumer protection should be built into AI systems, markets and regulatory frameworks, rather than relying on individuals to safeguard their own rights.

- **Enforceability requires investment.** Regulatory bodies should have the technical expertise, legal mandate, and resources needed to govern AI systems effectively.
- **Consumer choice and privacy protection should be regulatory priorities.** Regulatory frameworks should ensure market power is not used to make it hard for consumers to switch or to weaken privacy and choice, so that scale benefits consumers rather than entrenching control over their data.
- **Cross-border governance.** Binding minimum standards for data collection and processing should apply regardless of where a company is headquartered or where data is processed. Cross-jurisdictional enforcement and information sharing should support consistent protections.

HOW WE CAN ACHIEVE THIS: CORE PRINCIPLES OF PRIVACY AS A PUBLIC GOOD

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

PRINCIPLE 4: ENABLE EASY EXIT, PORTABILITY AND REAL CHOICE

Consumers should be able to move and delete their data without barriers.

- **Portability and compatibility between services.** Data portability and, where appropriate, interoperability can support consumer choice, innovation, and trust when implemented in a secure, privacy-protective, and proportionate manner.[xiv] Consumers should be able to choose the services that best protect their privacy without being locked in.
- **Simple account deletion.** Consumers should be able to close an account and have their personal data erased through a process no more difficult than the one used to sign up.
- **Withdrawal of consent.** Where processing relies on consent, consumers should be able to withdraw it as easily as they gave it, at any time and without penalty.

PRINCIPLE 5: MANDATE PRE-TESTING, MONITORING AND HUMAN INTERVENTION

AI systems should be tested, monitored and audited before and after deployment for privacy guardrails. Because systemic harms can be difficult to detect, oversight should focus on real-world outcomes as well as compliance with regulatory requirements.

- **Pre-deployment assessments.** AI systems used in high-impact areas, such as healthcare or financial services, should undergo risk-based assessments before deployment. The assessment should be proportionate to the use case, the sensitivity of the data involved, and the severity and likelihood of potential harm.[xv]
- **Human intervention.** Human oversight should allow providers to identify, challenge and correct harmful outcomes.
- **Continuous auditing.** Providers should actively monitor and audit AI systems throughout their lifecycle. Auditing and testing should identify discriminatory outcomes, system drift, disproportionate impacts on specific groups, and emerging harms.
- **Transparency reporting.** Regulated entities should report on their systems' performance against required standards, making outcomes visible to regulators and the public.

PRINCIPLE 6: ENSURE EFFECTIVE REMEDY AND REDRESS FOR PRIVACY HARMS EXPERIENCED

Consumers must be able to understand decisions, challenge outcomes and obtain timely redress when privacy harms occur.

- **A clear point of contact for consumers.** Every jurisdiction should have a designated body with the mandate and resources to provide human support on complaints, investigations, and enforcement. Consumers need to know where to go for help.
- **Decisions people can understand and challenge.** Where AI influences consequential decisions, consumers should receive explanations in terms consumers and regulators can understand and act on.
- **Redress should match the scale of harm.** When AI harms large groups of consumers, redress should also operate at scale. Consumer organisations and regulators should be able to bring collective actions on behalf of everyone affected, rather than leaving individuals to seek remedy alone.[xvi]

DELIVERING BETTER OUTCOMES FOR STAKEHOLDERS

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

FOR CONSUMERS

A public good approach means privacy protection no longer depends on individual consumer knowledge, time, or resources. People are safeguarded by the system itself. This:

- removes the burden on individuals to manage systemic privacy risks;
- protects against exploitation regardless of capability or digital literacy;
- creates meaningful routes to challenge AI-driven decisions;
- promotes choice and interoperability across services;
- strengthens accountability systems for consumers.

FOR THE PRIVATE SECTOR

Clear rules benefit businesses. This:

- distinguishes between data use that creates genuine value and practices that are simply extractive;
- creates consistent competitive conditions that apply across the market;
- builds consumer trust as a competitive market asset rather than treating privacy as a compliance cost.[xvii]

FOR GOVERNMENTS

A public good framework gives governments the tools to govern proactively, rather than responding after harm has occurred. This:

- shifts the focus from reactive enforcement to system-level safeguards;
- strengthens public trust in digital systems and the institutions that oversee them;
- provides a foundation for cross-border cooperation on an issue that does not respect national boundaries.

A COLLECTIVE CALL TO RECOGNISE PERSONAL DATA PRIVACY AS A PUBLIC GOOD

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

ACIM
ASSOCIATION DES CONSOMMATEURS DE L'ILE MAURICE

45 AÑOS
ADELCO Acción del Consumidor
1980 - 2025

AMBIO
ALERTA AMBIENTAL

ADECO
Associação para Defesa do Consumidor

ADEC
ASSOCIATION POUR LA DEFENSE DE L'ENVIRONNEMENT ET DES CONSOMMATEURS

ACTIVE CONSUMERS

consumer.

BENIN SANTE ET SURVIE DU CONSOMMATEUR (BSSC)

ক্রেতা আন্দোলন গড়ে তুলুন
CAB
Consumers Association of Bangladesh

消費者委員會
CONSUMER COUNCIL
香港・HONG KONG

CR Consumer Reports

CONSUMERS COUNCIL OF CANADA

CADEF
CONSUMER ADVOCACY AND EMPOWERMENT FOUNDATION

CPRC
Fairer markets for Australians

CERC
CONSUMER EDUCATION AND RESEARCH CENTRE
HAR GRAHAK KA SATHI

一般社団法人
全国消費者団体連絡会
CONSUMERS.JAPAN

FEDERACIÓN DE CONSUMIDORES Y USUARIOS
CECU

CUTS International
Since 1983

CONSUMER COUNCIL OF FIJI

جمعية حماية المستهلك
Consumer Protection Association

A COLLECTIVE CALL TO RECOGNISE PERSONAL DATA PRIVACY AS A PUBLIC GOOD

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

CONSUMER VOICE

empowering communities 35 YEARS 1991 - 2026 EMPOWER INDIA

epic.org ELECTRONIC PRIVACY INFORMATION CENTER

FIJIAN COMPETITION & CONSUMER COMMISSION

idec instituto de defesa de consumidores

FORBRUKERRÅDET

KCO SERVICE TO CONSUMERS

koodos

LEMBAGA KONSUMEN YOGYAKARTA
YOGYAKARTA CONSUMER INSTITUTE

မြန်မာစားသုံးသူများသမဂ္ဂ
MYANMAR CONSUMERS UNION
Rights and Responsibilities thru Education

المنظمة التونسية للإرشاد المستهلك
OTIC

ONPECO OBSERVATORIO NACIONAL PARA LA PROTECCIÓN DEL CONSUMIDOR

PARADIGM INITIATIVE

Privacy Foundation NZ

Proconsumer

REDECOMA

SOUTH SUDAN CONSUMER PROTECTION ORGANIZATION

SK SVERIGES KONSUMENTER
THE SWEDISH CONSUMERS' ASSOCIATION

สภาองค์กรของผู้บริโภค
Thailand Consumers Council

TheNetwork for Consumer Protection

TRIBUNA ECUATORIANA DE CONSUMIDORES Y USUARIOS

VOICES OF PRIVACY

Yemen Association For Consumer Protection

YLKI

SIGNATORIES

Reclaiming Privacy in the AI Era: Personal Data Privacy as a Public Good is endorsed by the following organisations:

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

ORGANISATION	COUNTRY
Acción del Consumidor (ADELCO)	Argentina
Association for the Defence of Consumers and the Environment (ADEC - Association pour la Défense de l'Environnement et des Consommateurs)	Senegal
Benin Health and Consumers' Survival (BSSC - Bénin Sante et Survie du Consommateur)	Benin
Brazilian Institute of Consumer Protection (IDEC -Instituto Brasileiro de Defesa do Consumidor)	Brazil
Bulgarian National Association Active Consumers (BNAAC)	Bulgaria
Consumer Advocacy and Empowerment Foundation of Nigeria (CADEF)	Nigeria
Consumer Association of Mauritius (ACIM - Association des Consommateurs de l'Ile Maurice)	Mauritius
Consumer Council of Fiji	Fiji
Consumer Defence Association (ADECO - Associação para Defesa do Consumidor)	Republic of Cape Verde
Consumer Defence Group of Mali (REDECOMA - Regroupement pour la défense des consommateurs du Mali)	Mali
Consumer Education and Research Centre (CERC)	India
Consumer NZ	New Zealand
Consumer Policy Research Centre (CPRC)	Australia
Consumer Protection Association of Mercosur (PROCONSUMER - Asociación de Protección de los Consumidores del Mercosur)	Argentina
Consumer Protection Association	Kuwait
Consumer Reports	United States
Consumer Unity and Trust Society (CUTS)	India
Consumer VOICE	India
Consumers Association of Bangladesh	Bangladesh
Consumers Council of Canada	Canada
Consumers Japan	Japan
Electronic Privacy Information Center (EPIC)	United States

ORGANISATION	COUNTRY
Empower India	India
Federation of Consumers and Users (CECU - Federación de Consumidores y Usuarios)	Spain
Fijian Competition & Consumer Commission (FCCC)	Fiji
Fundación Ambio	Costa Rica
Hong Kong Consumer Council	Hong Kong
Kenya Consumers Organisation	Kenya
Koodos Labs	United States
Myanmar Consumers Union	Myanmar
National Observatory for Consumer Protection (ONPECO)	Dominican Republic
Norwegian Consumer Council (Forbrukerrådet)	Norway
Privacy Foundation NZ	New Zealand
Paradigm Initiative	Nigeria
South Sudan Consumer Protection Organisation (SSCPO)	South Sudan
Swedish Consumers' Association (Sveriges Konsumenter)	Sweden
Thailand Consumer Council	Thailand
TheNetwork for Consumer Protection	Pakistan
Tribune of Consumers and Users of Ecuador (Tribuna Ecuatoriana de Consumidores y Usuarios)	Ecuador
Tunisian Organisation to Inform the Consumer (OTIC - l'Organisation Tunisienne pour Informer le Consommateur)	Tunisia
Voices of Privacy	United States
Yayasan Lembaga Konsumen Indonesia	Indonesia
Yemen Association for Consumer Protection	Yemen
Yogyakarta Consumer Institute (Lembaga Konsumen Yogyakarta)	Indonesia

ACKNOWLEDGEMENTS

We are grateful to colleagues from Consumers International who led the drafting and development of this document, including: Erin Parsons, Nandini Harihareswara, Alexandra Straessle, Stefan Hall and Brooke Kingsland.

This document was developed by Consumers International with guidance and input from a multistakeholder AI Advisory Group, and several external partners. Participating organisations are listed below. We thank all contributors for their valuable insight and feedback, while noting that the principles presented here do not necessarily reflect the individual views of all organisations involved.

ORGANISATION
Amazon.com, Inc.
Consumentenbond NL
Consumer Policy Research Centre (CPRC)
Consumer Reports
Danish Consumer Council
DuckDuckGo
Javier Ruiz Diaz
Jeannie Paterson, PhD
Koodos Labs
Que Choisir Ensemble
Visa, Inc.

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

Consumers International brings together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly.

Consumers International is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.

consumersinternational.org
@consumers_int
/consumersinternational

i Rule, J, *Private Lives and Public Surveillance: Social Control in the Computer Age* (1974). London: Schocken Books.

ii For the purposes of this report, artificial intelligence (AI) refers to the cognitive ability of machine agents that mimics human cognition in processing information and executing tasks for which the machine agent is trained. World Bank, *GovTech Glossary*. Available at: https://www.worldbank.org/en/programs/govtech/gtmi/gtmi-glossary

iii The digital advertising industry maintains standardised taxonomies to classify people and the content they engage with, published by Interactive Advertising Bureau (IAB) Tech Lab. The Content Taxonomy defines roughly 700 categories describing the subject matter of a page or app, while the Audience Taxonomy sorts consumers into more than 1,500 targetable segments across demographic, interest, and purchase-intent attributes, including sensitive data that can be shared, traded, and synced across digital services. These categories can also be used to infer more niche characteristics. IAB Tech Lab, *Audience Taxonomy and Content Taxonomy*. Available at: https://iabtechlab.com/standards/#taxonomies

iv Consumers International, *Global AI Survey* (2025).

v Alan Westin's 1967 seminal work defined privacy as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated." Westin, A, *Privacy and Freedom* (1967). New York: Atheneum.

vi Consumer Reports, *American experiences survey: a nationally representative multi-mode survey* (2024). Available at: https://article.images.consumerreports.org/image/upload/v1728423752/prod/content/dam/surveys/Consumer_Reports_AES_September_2024.pdf

vii United Nations Educational, Scientific and Cultural Organization (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (2022). Available at: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

viii Consumers International, *Stopping Online Scams: Building Consistency and Coordination for Consumers* (2026). Available at: https://www.consumersinternational.org/media/699948/consumers-international-stopping-online-scams-building-consistency-and-coordination-for-consumers.pdf

ix UN Human Rights Office (OHCHR), *The right to privacy in the digital age: report* (2021). Available at: https://www.ohchr.org/en/calls-for-input/2021/right-privacy-digital-age-report-2021

x UN Conference on Trade and Development (UNCTAD), *Artificial Intelligence and Consumer Protection* (2024), p.12-13. Available at: https://unctad.org/system/files/information-document/ccpb_artificial_intelligence_consumer_protection_en.pdf

xi Organisation for Economic Co-operation and Development (OECD), *The intersection between competition and data privacy* (2024). Available at: https://www.oecd.org/en/publications/2024/06/the-intersection-between-competition-and-data-privacy_b5ac1ae6.html

xii These principles scale with size, risk, and impact: the principles applied to a dominant provider processing sensitive data at scale is not the same as those applied to a small provider or low-risk use.

xiii Systems can be built to learn patterns without collecting each person's data centrally, to answer useful questions without exposing any individual, and to keep sensitive information on a consumer's own device. For example, federated learning trains a model across many devices or organisations so that only the lessons learned travel back to the developer, not the underlying personal data. Differential privacy adds a calibrated amount of noise to results, so that useful patterns remain visible while no single person can be picked out from them. On-device processing keeps the analysis on a consumer's own phone or computer, so sensitive information never reaches a company's servers. Information Commissioner's Office (ICO), *Privacy-Enhancing Technologies Guidance* (2023). Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

xiv Data Transfer Initiative, *A Path Forward for AI Portability* (2025). Available at: https://dtinit.org/blog/2025/08/26/path-forward-AI-portability

xv A note that several of the themes explored in this principle are covered under current EU regulation.

xvi Consumer redress includes having clearly communicated rights and responsibilities and accessible complaint channels. Prompt resolution through mandatory redress schemes that place responsibility on those best positioned to manage a given risk should be ensured.

xvii CGAP, *Is data privacy good for business?* (2023). Available at: https://www.cgap.org/research/publication/is-data-privacy-good-for-business