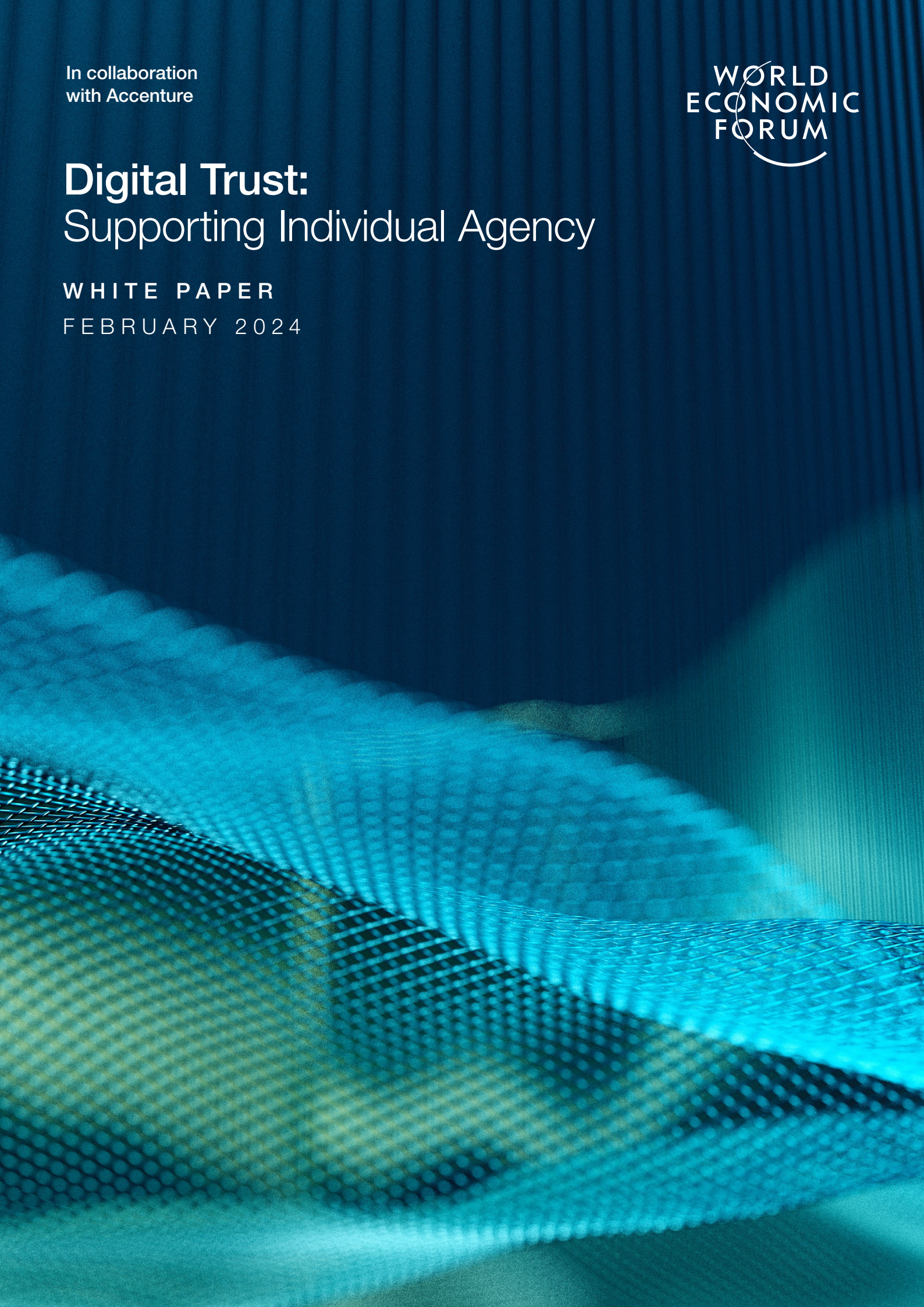
In collaboration
with Accenture

WORLD ECONOMIC FORUM

Digital Trust:
Supporting Individual Agency

WHITE PAPER

FEBRUARY 2024



Images: Getty Images, Unsplash

Contents

Foreword

Daniel Dobrygowski
Head, Governance and Trust, Centre for the Fourth Industrial Revolution, World Economic Forum

Kathryn White
Executive Fellow, Centre for the Fourth Industrial Revolution, World Economic Forum; Global Principal Director, Responsible Emerging Technology and Innovation, Accenture, USA

At the 2024 World Economic Forum Annual Meeting in Davos, stakeholders convened under the meeting's theme of Rebuilding Trust. At that meeting, participants continued to endorse the Forum's guidance that trust in technology – especially new and emerging technologies like artificial intelligence (AI) – must be earned through responsible decision-making while emphasizing that individuals and society have agency over the future of technology.[1]

At the Forum, the Centre for the Fourth Industrial Revolution helps stakeholders harness the full potential of technological progress for the equitable and human-centred transformation of industries, economies and societies. With thematic areas ranging from AI to immersive technologies and quantum technologies to space, improving governance is a top priority. To improve governance across technological domains, the Forum launched the Digital Trust initiative in 2021 to establish a global consensus among key stakeholders regarding what digital trust means and what measurable steps can be taken to improve the trustworthiness of digital technologies.

Specifically, the Forum's Digital Trust Initiative, through a multistakeholder approach, has defined Digital Trust as "individuals' expectation that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values."[2] This definition has informed the publication of a decision-making framework, high-level implementation roadmap[3] and guidance on pre-implementation steps[4] and how to measure digital trust[5] for organizations' leaders. This document builds on these groundbreaking publications, ensuring individuals are at the centre of technology. It further guides business and government leaders, as well as individuals, on how to better recognize the role of people as vital stakeholders in digital trust. With individuals increasingly interacting with new and rapidly developing technologies like generative AI, it has never been more relevant to support human-centric technology.

This report closely examines the digital trust dimensions of transparency, privacy and redressability according to the perspectives of organizations, governing bodies and individuals – all with the central lens of supporting individual agency. Business and government leaders are encouraged to prioritize the individual's perspective throughout the technology life cycle and take a by-design approach, especially to transparency and privacy. With all actors doing their part, we are hopeful that the benefits of emerging technologies can be fully realized while building trust among all stakeholders.

Executive summary

Trustworthy digital systems support and protect individual choice and agency.

Digital trust is a necessity in a world where digital technologies support and mediate virtually all economic transactions, social connections and institutions. However, trust in technology, innovation and science is eroding on a global scale. The World Economic Forum launched its Digital Trust Initiative to help reverse this trend by focusing on decision-making in support of trustworthy technologies. That work defines digital trust as "the expectation by individuals that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values."[6]

This paper describes how support for individual agency and human rights and respect for individual users' choices and values are crucial to rebuilding trust in digital technologies. The suggested method of trustworthy development – **individual agency by design** – must be a core component of any technology strategy or regulatory approach that seeks to earn the trust of users and individuals.

Individual agency by design is a crucial responsible design principle for digital technologies and focuses on the digital trust dimensions of **transparency**, **privacy** and **redressability**. The design principles described here ensure that technologies can be developed in a human-centred way that supports individuals' expectations and values. Specifically, individual agency by design is realized in the following ways:

Transparency

A hallmark of trustworthy design, transparency ensures that digital technologies do no more and no less than the user expects. Transparency is incorporated into digital technologies when developers:

- Build transparency into their products and services
- Offer effective digital literacy programmes
- Make transparency tools more accessible, available and intuitive

Privacy

Default protections for privacy assure users that their interactions online will be safe and that their personal data is protected. Privacy is integrated into digital technologies when:

- Technologies adhere to the spirit and letter of comprehensive privacy regulations
- Developers incorporate effective consent mechanisms and supporting tools and resources

Redressability

Preparation and prevention are not always sufficient to eliminate the chance of harm from digital technologies. Therefore, effective redressability mechanisms must be put in place to ensure that individuals who are harmed can be made whole. These mechanisms fall into the following categories:

- Harm prevention tools used to enforce individual or consumer rights
- Redress procedures that allow for interaction between harmed individuals and technology developers and owners
- Third-party oversight mechanisms to ensure individual harms are fairly rectified.

By recognizing the primacy of individual agency in human-digital interactions, this report aims to support a human-centric and trustworthy approach to the development of new technologies. Ultimately, developing and incentivizing technology that respects human agency is a shared public-private responsibility, one that – if adequately executed by all stakeholders – will serve to rebuild trust in digital technology and innovation.

Introduction

A trustworthy digital landscape requires technology to protect, inform and enable individuals.

Protecting individual choice and agency is essential to any trustworthy system. The world is navigating the complexities of modern technology roughly a decade into the Fourth Industrial Revolution. People are experiencing a social, political and economic shift from the digital age of the late 1990s and early 2000s to an era of embedded connectivity – a fusion of the digital, biological and physical worlds,[7] where an individual's digital experience can be more embodied, immersive and ever-present.[8] In this context, individual agency, which enables individuals to navigate their digital lives in an informed, self-sufficient and protected manner, is vital. Supporting individual agency includes activities and decisions related to the deployment and development of digital systems. Support for individual agency requires upholding human rights and, as such, is a necessary component for durable trust – and durable digital trust is critical to a fairer, safer and more sustainable digital economy. People deserve to be able to make choices for themselves and on their behalf. Enabling individual agency further supports responsible innovation, which is the only sustainable and fair way to ensure the adoption of Fourth Industrial Revolution technologies such as artificial intelligence and spatial computing.

Digital trust is *the expectation by individuals that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values.*[9] Pursuing this objective, the World Economic Forum created the Digital Trust Initiative[10] and published its foundational work on the subject, *Earning Digital Trust*, which focuses on how organizations can make more trustworthy decisions regarding technology. This paper – *Digital Trust: Supporting Individual Agency* – discusses the much larger group of stakeholders who use or otherwise interact with digital technologies. For digital trust to be effectively established and maintained, these individuals must be able to recognize themselves as stakeholders with the agency to self-navigate digital technologies.

This paper raises examples from the data management space, a sector at the forefront of navigating digital trust considerations, to explore how organizations can make decisions that enable individual agency and foster digital trust. The paper applies by-design principles to transparency, digital literacy and privacy, offering suggestions for how these concepts can be embedded into the user's experience of a digital product or service. Among the various dimensions of digital trust, three of the most relevant are highlighted due to their direct relationship with individual agency: transparency, privacy and redressability (this order is not meant to suggest an order of importance). This exploration covers important considerations, including the responsibility of organizations to ensure clarity and trust and detail how privacy mechanisms can support individual agency and the tiers of mechanisms available for redress when harm does occur. The efforts summarized in this paper supporting individual agency are not a cure-all. Instead, they are a piece of a larger puzzle of organizational protection and support. Likewise, the ordering of interventions in this paper does not represent an order of preference or application. Rather, the concepts here are described in order of most cooperative and preventative approaches first, with post-hoc resolution mechanisms at the end.

Individual agency by design

Digital trust requires a by-design approach to technology that emphasizes the need for principles that protect and support individuals from inception, putting their needs and values at the earliest possible stage of development. First popularized through the "secure-by-design" concept, the by-design concept has influenced several other approaches to designing and developing technologies, including privacy by design, accessibility by design and sustainability by design.[11]

This methodology, wherein user protection and online harm prevention are baked into the technology, translates into a digital product or service that supports individual agency and is more trustworthy.[12] The idea is not to take choices away from individuals or increase the burden of responsibility on everyday people but to ensure they are presented with fair options within a safe, secure and trustworthy environment that other organizational safeguards enable.

Ensure people are presented with fair options within a safe, secure and trustworthy environment.

Applying responsible innovation design principles

Technology companies and developers can avail themselves of an existing library of guidelines, principles and standards developed by international organizations, governments and non-governmental organizations.

- International organizations have defined safeguards, such as the United Nations (UN) *Guidelines for Consumer Protection*[13] and the UN's proposed Global Digital Compact.[14]
- Governments promote cybersecurity, privacy and responsible technology use across jurisdictions, such as the US *Blueprint for an AI Bill of Rights*,[15] the US National Institute of Standards and Technology *AI Risk Management Framework*,[16] Singapore's Online Safety Code,[17] Japan's laws promoting a digital society,[18] the European Union (EU) Artificial Intelligence (AI) Act[19] and the European Declaration on Digital Rights and Principles for the Digital Decade[20] as well as the EU Digital Markets Act and Digital Service Act.[21]
- Resources from non-governmental organizations such as Consumers International,[22] a consumer advocacy organization whose resources include recommendations for Digital Finance Consumer Protections,[23] and strategic frameworks like the Forum's Presidio Recommendations on Responsible Generative AI[24] and the Global Network Initiative (GNI) Framework on Freedom of Expression and Privacy.[25]

1

Transparency by design: The responsibility to illuminate choices

Just as a well-lit room enables clear vision and understanding, a transparent digital environment illuminates interaction bounds and opportunities, ensuring clarity and trust.

Building and maintaining trust is an ongoing endeavour.

As a crucial first step in recognizing individual agency, organizations seeking to cultivate digital trust must provide sufficient "light" for individuals to feel empowered to make their own choices and act in their own best interests in the digital environment. Building and maintaining trust is an ongoing endeavour requiring organizations to consistently demonstrate a commitment to consumer protection across their policies, products and services. Specifically, organizations aim to ensure that users maintain control by building transparency into their products and services, offering effective digital literacy programmes and making transparency tools more accessible, available and intuitive. Having consumers represented in the design process bolsters the decision-making that goes into achieving such transparent ends. Consumer advocates seek to work with organizations and regulators to ensure transparency efforts are pervasive and beneficial for consumers. Such efforts result in appropriate choices in the marketplace, consumer-friendly online choice architecture and corresponding default settings.

Digital literacy and transparency, crucial elements in the design and use of technology, work in harmony to support individual agency and earn digital trust. Their interplay forms the baseline for accountability for a given technology and an organization's accountability culture while providing a more reliable and secure digital environment for the individual.

Visibility into data flow

The use and movement of individuals' data offers a helpful example of digital literacy and transparency at work. Data underpins a person's interactions with digital technologies. As the digital economy has expanded, with several applications collecting data for some corporations, advertising has become a way to offer digital products and services without erecting paywalls. In exchange for the use of technology services, consumers are incentivized to share their personal data. As this dynamic has increased, consumer data has become more valuable and collection methods more thorough. This has amplified the scale of the opportunities and the potential harms for both users and organizations.[26]

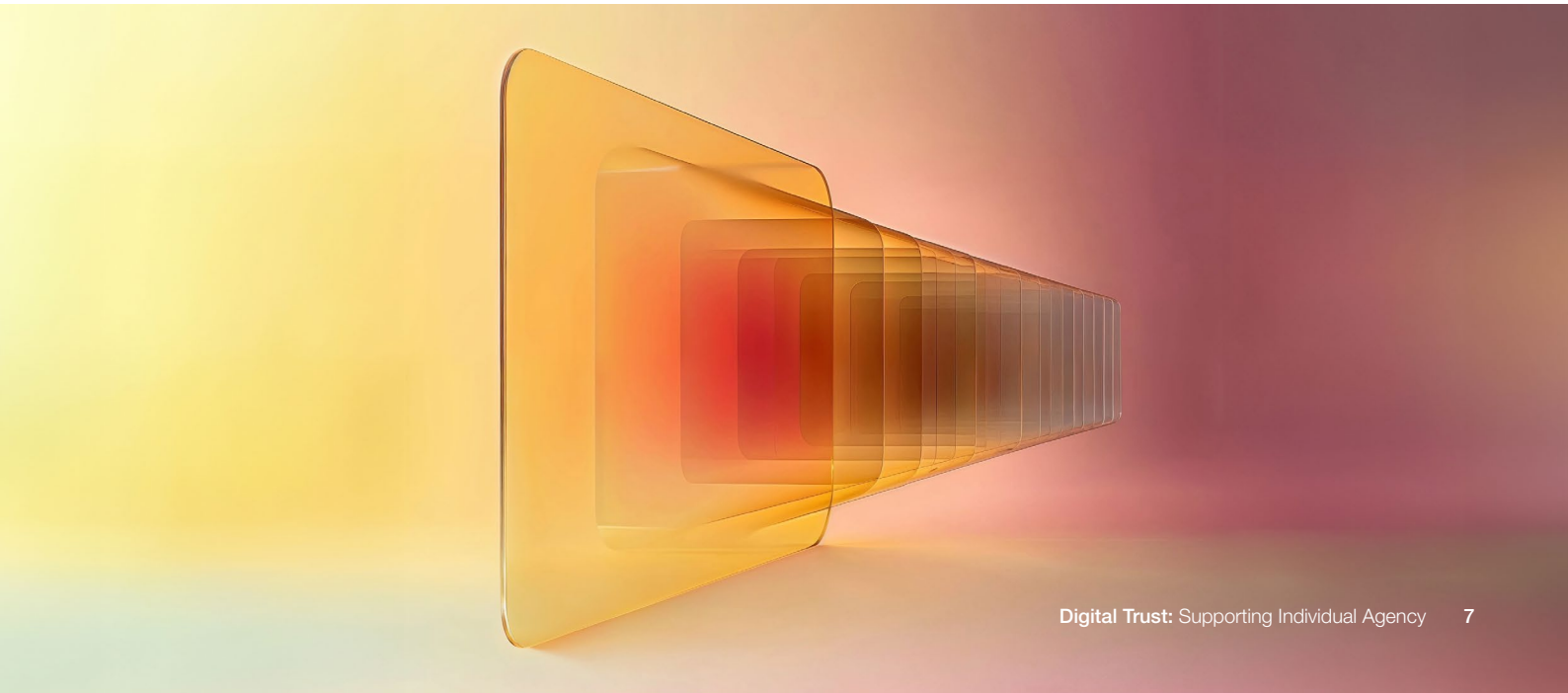


TABLE 1 **Opportunities and harms for users regarding consumer data**

Opportunities (for users)	Harms (for users)
– **Improved services:** With insights from data collected, companies can refine their services, leading to better user satisfaction. – **Personalized experiences:** Users can receive recommendations and content tailored to their preferences, enhancing the user experience. – **Access to subscription-free services:** Access to services that would otherwise be behind a paywall may be granted to users in exchange for sharing their data. – **Enhanced product development:** Companies can develop or refine products based on user feedback and data insights.	– **Privacy and data breaches:** Data collection without consent infringes on individual privacy. Furthermore, there's the ever-present risk of data being accessed unlawfully, whether through cyber-attacks, inadequate security or internal malpractice. – **Over-personalization:** Overly personalized marketing can feel invasive, giving users the impression that their online (and offline) actions are constantly monitored and exploited. – **Data misuse:** Even with initial consent, a risk remains that data might be sold, shared or accessed by third parties without the user's knowledge. – **Default settings:** Users may be unaware of functionality that is programmed by default. Because defaults are set by the product and service providers, they may skew in favour of the interests of those providers.

TABLE 2 **Opportunities and harms for organizations regarding consumer data**

Opportunities (for organizations)	Harms (for organizations)
– **Strategic decision-making:** Analysing user data can lead to more informed decisions regarding product development, marketing strategies and user experience enhancements. – **Predictive analytics:** By understanding patterns in data, organizations can predict future trends, user behaviours and market demand. – **Personalized marketing:** Organizations can tailor advertisements and promotions to specific user preferences, leading to increased sales and user engagement.	– **Security breaches:** Holding vast amounts of data increases the risk of data breaches and the scale of the resulting harms, which can be financial, reputational and legal in nature. – **Regulatory penalties:** Non-compliance with data protection regulations can lead to significant fines and sanctions. – **Market perception:** Inappropriate data use can erode brand loyalty and reputation. – **Misinterpretation:** Incorrect analysis of data can lead to flawed strategic decisions.

The profound amount of data that companies possess about users and their engagement with digital technologies may risk misaligned incentives. Individuals are increasingly cognizant of this potential risk. A study has revealed that, as transparency and digital literacy have increased, 86% of consumers care about data privacy, signalling a significant shift in consumer sentiment and a burgeoning demand for enhanced protection and control over personal data, all of which underscore the urgent need for organizations to adapt and address these concerns.[27] In this environment, better transparency lays the groundwork for effective adherence to individuals' choices and expectations. As consumer awareness and expectations have shifted, so have the capabilities of organizations, including ethics and compliance programmes and the like.

Transparency in digital interfaces refers to providing clear visibility into the technology's characteristics, including what data it collects, how it processes the information and the purposes for which the data is used. Such transparency supports individual agency by respecting the individual's right to understand and control their interactions with technology. It is about ensuring that technology operates as the user expects, doing only what the user has granted permission for. For example, in artificial intelligence, resources like the Foundation Model Transparency Index can provide information that may help users understand the ramifications of their activities as they increasingly engage with generative AI.[28] This comprehensive assessment of the transparency of foundation model developers uses 100 transparency indicators.[29] They report on the transparency of foundation models, the resources required to build them and their role in the ecosystem.[30] Such transparency regarding responsible AI seeks to promote trustworthiness and engender trust.

Effective transparency requires that digital products and services be both well-explained and easily understandable. Regarding data collection and management, a variety of methods are employed today, each with its own advantages and disadvantages (see the table on the advantages and disadvantages of common methods of transparency in data collection and management in the appendix). Drawing from current best practices in data collection transparency, helpful practices include:

> The synergy of transparency and digital literacy fosters a culture of accountability that holds promise for a more trustworthy future.

- **Plain language** – Use everyday words and minimize technical jargon to make transparency efforts intelligible and provide appropriate disclosures
- **Segmented information** – Provide a brief summary upfront, then delve into detailed explanations
- **User-centric design** – Prioritize intuitive interfaces and streamlined user experience
- **Multichannel engagement** – Communicate through emails, in-app notifications and other relevant platforms
- **Real-time indicators** – Highlight active data collection or processing through immediate cues
- **Algorithm transparency** – Clearly explain how data influences algorithmically-driven system processes and decisions
- **Educational tools** – Offer concise tutorials or FAQs to clarify data practices
- **Feedback-driven updates** – Continuously adapt strategies based on user feedback and comprehension studies
- **Third-party audits** – Periodically validate data practices through external reviews

Digital literacy

In an age of information overload, digital literacy acts as the individual's compass, providing insight as they seek to understand how digital technologies and services work so they can make informed decisions.[31] Literacy makes transparency action-oriented – without an understanding of what is being shared, transparency is merely theatre. Alongside transparency, digital literacy enables individuals to effectively navigate these interfaces and comprehend the technological controls in place. As users enhance their digital literacy, they can make more informed decisions about their technology use and more clearly express their expectations to technology developers, reflecting their genuine agency through these critical elements:

- Informed expectations via terms of service and community guidelines
- Assurance that technology in use was designed in accordance with consumer rights[32]
- Ability to compare products on the dimensions of trustworthiness (e.g. the World Economic Forum's Digital Trust Framework[33])
- Access to tools that allow individuals to evaluate and enhance their personal digital safety
- Clear action steps when an individual's experience is out of alignment with their expectations of trustworthiness

The synergy of transparency and digital literacy fosters a culture of accountability that promises a more trustworthy future. With transparency providing clear insight into a technology's operations and digital literacy enabling an understanding of these insights, users can maintain a healthy dialogue about their end-user needs with technology providers. This accountability is mutually beneficial and ensures that digital tools respect consumer rights and expectations and work in the users' best interests. This accountability aspect becomes pivotal in maintaining digital trust, as technology developers, being the "least cost avoiders",[34] can effectively prevent and remediate online harms.[35] Well-defined and clearly assigned responsibilities, paired with feedback mechanisms, significantly enhance the trustworthiness of digital technologies.

Taken together, digital literacy and transparency guide technology to be more user-centred, shaping a digital landscape that is understandable, explainable, controllable and accountable – supporting individual agency and building digital trust. Box 1 provides an example of a transparency tool in support of individual agency.

BOX 1 **Example of a transparency tool in support of individual agency**

Salesforce trust site[36]

Salesforce provides a dashboard where users can view real-time information on service availability and performance. The transparency of this resource instils customer trust and confidence in the company's services.

2 Privacy by design: Safeguarding user privacy

Default protections help reduce users' concerns about whether they will be safe or their privacy will be protected.

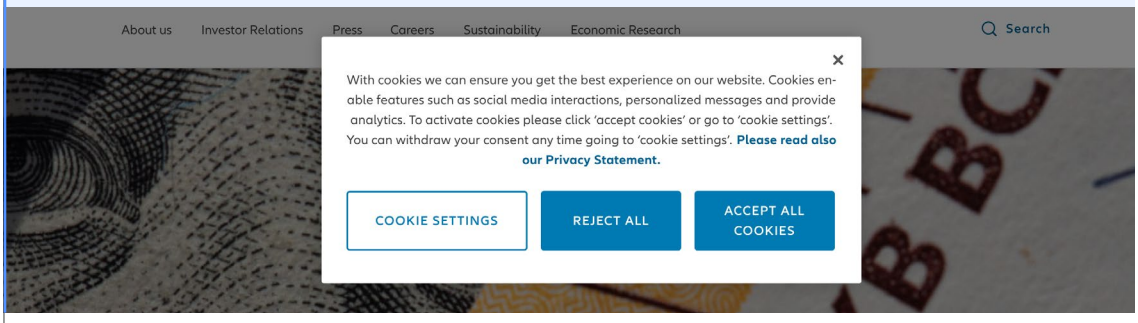
Privacy by design appears in a wide variety of regulations, such as the EU's General Data Protection Regulation (GDPR)[37,38] and India's Digital Personal Data Protection Bill.[39] Major technology developers use similar approaches (Google's Privacy and Security Principles,[40] Microsoft's Responsible AI Standard,[41] IBM on Operationalizing Trustworthy AI[42]). These concepts aim to proactively incorporate principles into a product or service in a manner that ensures they will be prioritized in the development of the integral components that shape the user's experience and interaction with technology.

As trust- and confidence-building measures, these protections enable users to interact with technologies more confidently and engage more authentically.

BOX 2 **Offering fair choice options**

Allianz trust-by-design approach

Allianz, a multinational insurance and asset management firm, is committed to a privacy-by-design approach that offers consumers a fair choice. Evident simply in its website's prompt about cookie preferences, consumers have three options: accept all cookies, reject all, cookie settings. Cookies, data collected while a user engages with a website, support session management (for example, allowing items in a shopping cart to persist) and help enable personalization such as custom advertisements. Allianz provides the opportunity to express cookie preferences thanks to the European Union's General Data Protection Requirement (GDPR). While "accept all" is typically readily available on organizational websites in accordance with this requirement, there is variation in the number of times a user has to click to select to reject all. Allianz's provision of a "reject all" option next to the accept all option is a prime example of providing a fair choice and enacting it with a privacy-by-design approach.



Default protections underscore the organization's focus on a human-centric approach that prioritizes respect for the individual, which in turn strengthens digital trust. They send a message that the user's safety, privacy and rights are a priority, regardless of the user's ability to set up these protections themselves. Examples of a privacy-by-design approach include:

- Making significant investments in privacy settings and controls
- Managing trust-enhancing features over time by monitoring users' engagement with them, testing to confirm understanding and adoption, and adjusting and improving these features over time
- Implementing organization-wide digital trust programmes (see the World Economic Forum's Digital Trust guidance[43] and briefing on implementation[44])
- Creating internal guidelines, principles and standards (e.g. Microsoft's comprehensive Responsible AI Standard[45])

User consent

As consent mechanisms and their supporting tools and resources become more transparent and understandable, the process becomes more consumer-friendly and users can better determine the purposes for which their data is processed. When organizations provide greater clarity and individuals can increase their understanding, such efforts serve individual agency. It is important to note that this can be challenging depending on the extent to which an organization's contracts and agreements are digitalized.

Transparent organizations that support privacy decision-making accrue benefits – the potential future risks decrease and trust with the user is strengthened. Table 3 presents examples of transparent user consent notices.

TABLE 3 **Transparent user consent notices**

Google Privacy Dashboard[46]	Google provides a dashboard where users can understand, track and control permissions and data access across Google applications (apps). Such interactive visuals and transparency tools allow users to understand data use and tailor their privacy settings.
Apple's app "Privacy Nutrition Labels"[47]	Apple introduced mandatory labels in all App Stores that provide a summary of the app's privacy policies, similar to food nutrition facts. This mechanism offers users a clear understanding of the app's data processing (i.e. collection, analysis, secondary use). Such a concise transparency mechanism enables easy comparison between different apps regarding how they process data. Additionally, Apple offers users an App Privacy Report[48] that provides visibility into how apps use the privacy permissions users have granted them and the corresponding network activity.

3 Redressability: Prevention, engagement, oversight

When digital technologies harm individuals, they deserve to be made whole.

Redressability, the possibility of obtaining recourse where technological processes, systems or data uses have negatively affected individuals, groups or entities,[49] can take many forms. Organizational leaders can take steps to support redressability by making decisions regarding prevention, engagement and how to address. Firstly, a by-design approach allows for the implementation of solutions such that the risk of the need for redress is minimized (for example, regulatory tech, supervisory tech, enforcement tech). Secondly, allowing individuals to directly engage with an organization and its representatives can support simple resolutions to redress scenarios (such as fair credit reporting). However, prevention and engagement activities may not be sufficient in all cases, so opportunities should exist for a specific individual or broad consumer groups to take action to seek redress.

Enabling harm prevention

Technology crafted under a redressability-by-design approach will automate regulatory compliance (RegTech), regulatory supervision (SupTech) or, in certain instances, seek to enforce consumer protections (EnforceTech). Together, these technologies fortify the architecture of individual agency and enhance transparency. Supporting individuals in understanding that, if harms occur, redress is possible is important in cultivating an environment of digital trust.

Specifically, RegTech can aid firms in adhering to compliance requirements, ensuring organizations efficiently and effectively align their digital practices with legal regulations thanks to risk management, monitoring and reporting functionalities.[50] SupTech can help an organization ensure its digital systems are compliant, namely with respect to data collection and analytics.[51] Related to SupTech, EnforceTech encompasses innovative technologies that can support consumer advocate agencies in fulfilling their objectives of protecting consumers.[52] These types of technologies, while still emerging, promise to play an increasingly pivotal role in preserving individual agency in the digital domain.

However, automated regulation, supervision and enforcement will likely be insufficient to fully offer appropriate redress and will always require a human in the loop. Nevertheless, these technologies are useful tools in the broader toolkit to support individual agency and digital trust.

Enabling redress procedures

Regulatory regimes relating to new and emerging technologies are a patchwork of existing and proposed policies, so there is room for consideration of how to apply the best practices of and principles behind consumer protections to the digital realm.

Redress, however, is not merely an issue facing technology. Existing means of redress – including those related to the misuse of individuals' data – may provide useful illustrations of how redress can work in digital technologies. In the US, Title VI of the Fair Credit Reporting Act[53] embodies several important protections, including a user's right to request their credit score, be informed if information in their file has been used against them, access the contents of their file, and request information in their file be corrected. Moreover, consumer reporting agencies are mandated to rectify or remove inaccurate, incomplete or unverifiable data. Through these provisions, the regulation improves transparency by ensuring users can access and understand their data. It also provides an avenue for companies to prioritize and support individual rights, fostering a proactive culture of user-centricity. Importantly, in situations where discrepancies arise, these regulations also offer a clear redress mechanism for consumers, solidifying their trust in the system. These regulations hold credit reporting agencies to a high standard of promoting individual agency, which goes a significant way towards cultivating trust in the system as a whole.

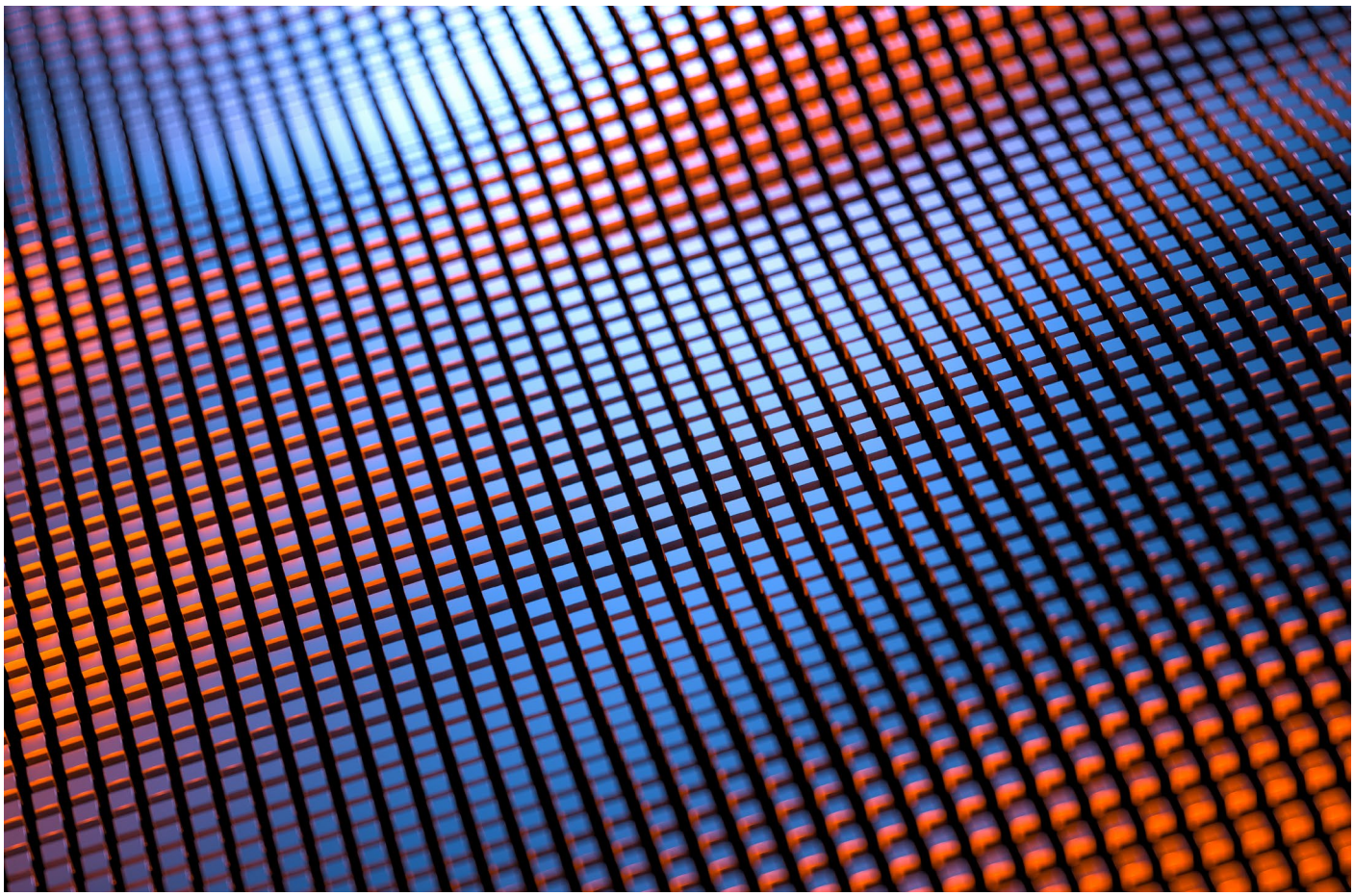
Additionally, in the financial sector, the European Commission has proposed regulations to improve consumer protection in a way that empowers consumers to share their data to enable better and cheaper financial products and services.[54] Such examples from the financial sector may be relevant for digital economies globally.

Third-party oversight

If digital harms occur and are not prevented or resolved directly with the responsible organizations or through regulatory oversight, this implicates the trustworthiness of digital systems. To re-establish trust, individuals may require further protection supported by consumer protection or advocacy groups. Generally, third-party oversight methods of redress can be costly in terms of time and money. Yet, this form of external oversight may be both useful and essential, especially in instances of applications of emerging technologies where there may be uncertainty about how to apply existing regulations and consumer protections. In these instances, for the sake of ensuring trust, additional safeguards are necessary.

Consumer protection groups may help to support individual technology users or subjects where business-to-consumer redress mechanisms break down. Two prime examples of consumer advocates providing third-party oversight protections include the Digital Security Helpline from Access Now and the Permission Slip app from Consumer Reports. Access Now's Digital Security Helpline[55] works with individuals and organizations in civil society globally to enhance their digital security, assisting those facing digital threats. The helpline ensures rights are upheld when organizations or systems fall short of safeguarding them. Consumer Reports offers a smartphone application, Permission Slip,[56] that enables users to take control of their data and manage their various accounts, including filing requests to stop selling personal information, in a single interface.

In some situations, individuals or groups of individuals may not be able to rely on the actions of regulators to protect or judicial authorities to represent their interests and vindicate their agency and rights. Providing a mechanism (such as private right of action, private cause of action or class action) for individuals to seek redress for technology-related harms they experience, without the mediation of regulators or other actors, may help democratize the redress process and may support individuals as digital trust stakeholders. It also serves as a method of recourse for individuals in situations where regulators are under-resourced or otherwise unable to ensure that harmed individuals are allowed adequate redress. Such rights recognize the agency of individuals as stakeholders who can vindicate their rights, expectations and values where new technologies cause unanticipated (or expected but unmitigated) harm. Private rights of action often feature in consumer protection safeguards (such as the US Fair Credit Reporting Act) and privacy protection regulations (like the EU's GDPR, China's Personal Information Protection Law (PIPL) and the California Consumer Privacy Act (CCPA)) all provide private rights of action. Broader applications of a private right of action may help bolster trustworthy systems by guaranteeing a redressability mechanism of last resort.[57]



Conclusion

Using a unified approach to advance individual agency.

To meaningfully advance digital trust, a collaborative approach between the public and private sectors is vital. This collaboration should prioritize individual agency and establish universally accepted best practices.

BOX 3 **Public-private collaboration in support of safety and digital trust**

Illustrating the potential for such collaborations, Singapore has pioneered the Sunlight Alliance for Action, a public-private collaboration initiative launched in 2021 to bridge the digital safety gap. The initiative operates through workstreams including research, victim support and public education, as mentioned in the Forum's *Earning Digital Trust: Decision-Making for Trustworthy Technologies insight report.*[58]

Furthermore, Singapore has implemented a four-star system for rating the security of smart devices across different providers, giving people an easy-to-understand framework for selecting products and offering a marketing incentive for tech companies to elevate their security standards. This system has earned bilateral recognition with countries like Germany and Finland and may potentially gain future recognition from international bodies like the International Organization for Standardization (ISO).[59]

Upholding digital trust and individual agency is a shared responsibility that requires effective collaboration across the public and private sectors. As the world advances into the digital future, globally recognized, shared and verified standards can serve as powerful tools to bolster digital trust. They will enhance consumer protection and promote consensus between the public and private sectors, demonstrating the inherent value in collaborative efforts to reinforce individual agency.

The critical interplay between individual agency and digital trust anchors the digital ecosystem in a human-first approach. Organizations aiming to cultivate this trust have crucial areas of best practice to focus on – design methodologies that actively protect, inform and enable individuals. This commitment to individual agency requires broad-based collaboration across both the public and private sectors, anchoring the digital future on globally recognized standards that promote respect for individual autonomy and create a trusted digital ecosystem.

Appendix

Alignment of the UN Consumer Protection Principles for Good Business Practices and the Forum's Digital Trust Framework along with key considerations for organizations building digital trust

TABLE A1 **Transparent user consent notices**

United Nations Consumer Protection Principles for Good Business Practices (All)[60]	Digital trust goal	Alignment title	Digital consumer protections (summarized & paraphrased)
Education and awareness-raising	Accountability and oversight	**Digital literacy and education**	– Assistance to consumers to understand the choices available to them and the consequences of those choices – Supporting consumers to develop skills and confidence to manage risks and opportunities
Protection of privacy	Security and reliability Inclusive, ethical and responsible use	**User privacy and consent**	– Consumer understanding and control of the collection and use of personal data
Consumer complaints and disputes	Accountability and oversight	**Recourse and redress**	– Consumer access to simple and effective recourse – Consumer access to fair redress
Fair and equitable treatment	Inclusive, ethical and responsible use	**Inclusion and protection from harm**	– Consumer access to an affordable, good quality and reliable internet connection and essential digital services – Secure online interactions and safe digital environments/ protection from harm – Protection for vulnerable and disadvantaged customers
Commercial behaviour	Accountability and oversight Inclusive, ethical and responsible use	**Responsible business conduct**	– Effective governance and accountability, including consumer representation in relevant processes. – Consumer choice of digital providers, products and services in a competitive market
Disclosure and transparency	Accountability and oversight	**Access to information**	– Consumer access to accurate and meaningful information about digital products and services

FIGURE | **The Digital Trust Framework**

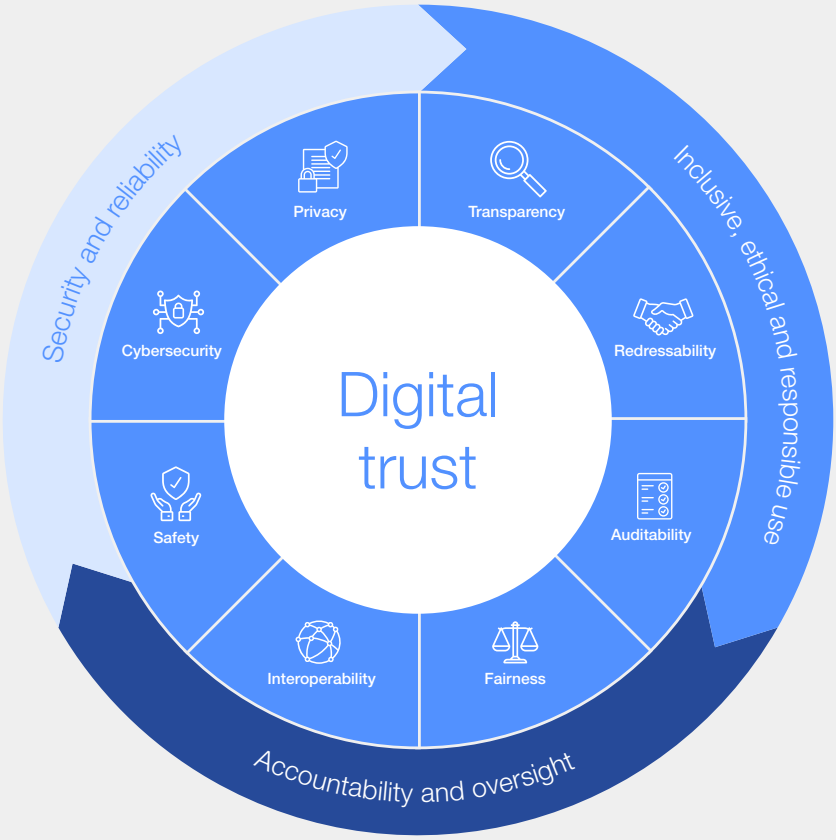


TABLE A2 **Advantages and disadvantages of common methods of transparency in data collection & management**

Method	Advantages	Disadvantages
Privacy policies and terms of service agreements	– **Standardized:** Universally accepted format – **Comprehensive:** Covers all aspects, clauses and potential scenarios related to data usage; optimized for regulatory compliance	– **Lengthy:** Most users don't read them due to their length and complexity – **Complex language:** Often written in legalese, making it hard for an average user to understand
Interactive privacy dashboards	– **User-friendly:** Interactive visuals and tools allow users to understand and control data use – **Customizable:** Users can often tailor their privacy settings here	– **Overwhelming:** Too many options or poorly designed interfaces can confuse users
Just-in-time notifications	– **Contextual:** Offers information when it's most relevant (e.g. asking for location data when a relevant feature is activated) – **Concise:** Provides bite-sized, understandable information	– **Interruptive:** Can disrupt the user experience if not appropriately timed; often ignored or rapidly dismissed by users
Privacy "nutrition" labels	– **Simplified overview:** Gives users a quick snapshot of how an app uses data, similar to nutrition labels on food – **Standardized comparisons:** Allows for easy comparison between how different apps handle data	– **Limited detail:** Might not convey the depth of data interactions
Regular data usage reports	– **Transparency:** Shows users exactly how their data has been used over time	– **Might not be seen:** Relies on regular user engagement – **Might be ignored:** Users might overlook these reports if they receive too many notifications

TABLE A2 **Advantages and disadvantages of common methods of transparency in data collection & management (continued)**

Method	Advantages	Disadvantages
Data access & portability requests	– **Data access:** Individual has direct access to data – **Agency:** Gives the individual ability to take direct action	– **Security:** Potential for security breaches – **Knowledge constraint:** Utility depends on the level of user expertise and contextual understanding of the data
Embedded device indicators (e.g. internet of things (IoT) devices)	– **Real-time indicators:** Immediate data activity notifications – **On-device:** Direct transparency available on the device itself	– **Space constraints:** Limited screen may restrict comprehensive info. – **Misinterpretation:** Users may misinterpret indicator meanings – **Coverage gap:** Indicators might not reflect all data collection types
User experience surveys (e.g. research initiatives)	– **Scope clarity:** Explicit boundaries of data collection – **Consent:** Achieves explicit user consent	– **Dynamic limitations:** Limited utility in continually changing context – **User dependence:** Relies heavily on user willingness

Sources: Cranor, L.F. (2023, 6 May). Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. Harvard University Privacy Tools Project. https://privacytools.seas.harvard.edu/presentations/necessary-not-sufficient-standardized-mechanisms-privacy-notice-and.

Gage Kelley, P. et al. (2009). A 'Nutrition Label' for Privacy. *SOUPS '09: Proceedings of the Symposium on Usable Privacy and Security*, pp. 1-12.

Genaro Motti, V. and Caine, K. (2015). Users' Privacy Concerns About Wearables. In *Financial Cryptography and Data Security*. Edited by M. Brenner, N. Christin, B. Johnson, K. Rohloff, pp. 231-244, Springer.

Hay Newman, L. (2020, 14 December). Apple's App 'Privacy Labels' Are Here—and They're a Big Step Forward. *Wired.* https://www.wired.com/story/apple-app-privacy-labels/.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Dædalus*. https://www.amacad.org/publication/contextual-approach-privacy-online.

Porter Felt, A. et al. (2012). Android permissions: user attention, comprehension, and behavior. *SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security*, no. 3, pp. 1-14.

Schaub, F. et al. (2015). A Design Space for Effective Privacy Notices. *SOUPS '15: Proceedings of the Symposium on Usable Privacy and Security*, pp.1-17.

Tiell, S. and Pesce Ares, L., (2022, 28 June). Principles to practice: Using ethical spectrums to guide decision-making. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/principles-to-practice-using-ethical-spectrums-to-guide-decision-making/.

Van Alstyne, M. and Paul, S. (2016, 10 November). Platform Strategy and the Internet of Things. *MIT Sloan Management Review*. https://sloanreview.mit.edu/article/platform-strategy-and-the-internet-of-things/.

Wang, N. et al. (2014). Designing the default privacy settings for Facebook applications. CSCW Companion '14: Proceedings of the companion publication of the 17th ACM conference on Computer supported cooperative work & social computing, pp. 249-252.

World Economic Forum. (2018). *Data Policy in the Fourth Industrial Revolution: Insights on personal data*. https://www.weforum.org/publications/data-policy-in-the-fourth-industrial-revolution-insights-on-personal-data.

Contributors

Lead authors

Daniel Dobrygowski
Head, Governance and Trust, Centre for the Fourth Industrial Revolution, World Economic Forum

Amanda Stanhaus
Executive Fellow, Digital Trust Initiative, World Economic Forum; Senior Manager, Responsible Emerging Technology and Innovation, Accenture, USA

Kathryn White
Executive Fellow, Centre for the Fourth Industrial Revolution, World Economic Forum; Global Principal Director, Responsible Emerging Technology and Innovation, Accenture, USA

World Economic Forum

Cathy Li
Head, Artificial Intelligence, Data and Metaverse; Member of the Executive Committee

Hesham Zafar
Lead, Digital Trust Initiative

Acknowledgements

The Digital Trust Initiative is a multistakeholder collaboration led by the World Economic Forum, with contributions from the entire Digital Trust Community.

Justiin Ang
Director, Security and Resilience Division, Ministry of Communications and Information of Singapore

Keith Enright
Vice-President and Chief Privacy Officer, Google

Stefan Hall
Director, Digital Innovation and Impact, Consumers International

Thibaut Kleiner
Director, Policy, Strategy and Outreach, DG Connect, European Commission

Helena Leurent
Director-General, Consumers International

Peter Micek
General Counsel and United Nations Policy Manager, Access Now

Phillip Raether
Group Chief Privacy Officer, Allianz

Indre Raviv
Senior Vice-President, Marketing, Cujo AI

Dan Rice
Vice-President, Digital Governance, Walmart

Kim Scardino
Senior Partnership Manager, Trust & Safety, Apple

Lynn Simons
Senior Director, Security Engagement, Salesforce

David Treat
Senior Managing Director, Innovation Incubation Lead, Accenture

The initiative team would also like to thank Lara Pesce Ares (Accenture) for her diligent research, writing and editing that made this report possible.

Production

Danielle Carpenter Sprüngli
Editor, Eagle Eye Communications

Laurence Denmark
Creative Director, Studio Miko

Oliver Turner
Designer, Studio Miko

Endnotes

1. World Economic Forum. (2024). Technology in a Turbulent World session. Annual Meeting 2024. https://www.weforum.org/events/world-economic-forum-annual-meeting-2024/sessions/technology-in-a-turbulent-world/.
2. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
3. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
4. World Economic Forum. (2023). *Implementation Workstream: Pre-Implementation Briefing Paper.* https://www3.weforum.org/docs/WEF_World_Economic_Forum_Digital_Trust_Initiative_2023.pdf.
5. World Economic Forum. (2023). *Measuring Digital Trust: Supporting Decision-Making for Trustworthy Technologies.* https://www.weforum.org/publications/measuring-digital-trust-supporting-decision-making-for-trustworthy-technologies.
6. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
7. Schwab, K. (2016). *The Fourth Industrial Revolution. Portfolio Penguin.*
8. Philbeck, T. and Davies, N. (2019). The Fourth Industrial Revolution: Shaping a New Era. *Journal of International Affairs,* vol. 72, no. 1, Fall 2018/Winter 2019, pp. 17-22.
9. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
10. World Economic Forum. Digital Trust Initiative. https://initiatives.weforum.org/digital-trust/about.
11. Cavoukian, A. (2012). Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era. In *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*. Edited by G.O.M. Yee (pp. 170-208). IGI Global.
12. World Economic Forum. (2023). *Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms.* https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf.
13. United Nations Conference on Trade and Development. (2016). *United Nations Guidelines for Consumer Protection.* https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf.
14. United Nations. (2023). *Our Common Agenda Policy Brief 5: A Global Digital Compact — an Open, Free and Secure Digital Future for All.* https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf.
15. The White House. *Blueprint for an AI Bill of Rights.* https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
16. National Institute of Standards and Technology. *AI Risk Management Framework.* https://www.nist.gov/itl/ai-risk-management-framework.
17. Infocomm Media Development Authority. (2023, 17 July). *IMDA's Online Safety Code comes into effect [Press release].* https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/imdas-online-safety-code-comes-into-effect.
18. Library of Congress. (2021, 19 May). Japan: Diet Passes Three New Laws to Promote a "Digital Society". https://www.loc.gov/item/global-legal-monitor/2021-07-23/japan-diet-passes-three-new-laws-to-promote-a-digital-society/.
19. European Parliament. (2023, 9 December). *Artificial Intelligence Act: deal on comprehensive rules for trustworthy artificial intelligence (AI) [Press release].* https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.
20. European Commission (2022, 19 December). European Declaration on Digital Rights and Principles. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles.
21. European Parliament. (2021, 14 December). EU Digital Markets Act and Digital Services Act explained. *News* https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained.
22. Consumers International. Digital Index. https://www.consumersinternational.org/what-we-do/digital-rights/digital-index/.
23. Consumers International. (2023). *Digital Finance: The Consumer Experience.* http://www.consumersinternational.org/media/451453/digital-finance-the-consumer-experience-2023-final.pdf.
24. World Economic Forum. (2023). *The Presidio Recommendations on Responsible Generative AI.* https://www3.weforum.org/docs/WEF_Presidio_Recommendations_on_Responsible_Generative_AI_2023.pdf.
25. Global Network Initiative. Framework on Freedom of Expression and Privacy. https://globalnetworkinitiative.org/gni-principles/.
26. World Economic Forum. (2023). *Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms.* https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf.

27. Goswami, S. (2021, 23 November). What The Future Of Consumer Data Ownership Looks Like. *Forbes.* https://www.forbes.com/sites/forbestechcouncil/2021/11/23/what-the-future-of-consumer-data-ownership-looks-like/?sh=43dc6fd749e9.
28. Center for Research on Foundation Models. The Foundation Model Transparency Index. https://crfm.stanford.edu/fmti/.
29. Center for Research on Foundation Models. The Foundation Model Transparency Index. https://crfm.stanford.edu/fmti/.
30. Center for Research on Foundation Models. The Foundation Model Transparency Index. https://crfm.stanford.edu/fmti/.
31. Akman, P. (2021, 3 June). We can't tackle platform competition issues without increasing digital literacy. *Agenda.* https://www.weforum.org/agenda/2021/06/platform-competition-digital-literacy/.
32. Consumers International. What are Consumer Rights? https://www.consumersinternational.org/who-we-are/consumer-rights/.
33. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
34. Rosenzweig, P. (2013, 5 November). Cybersecurity and the Least Cost Avoider. *Lawfare.* https://www.lawfareblog.com/cybersecurity-and-least-cost-avoider.
35. World Economic Forum. (2023). *Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms.* https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf.
36. Salesforce. Trust site. https://trust.salesforce.com/.
37. European Commission. (2016). General Data Protection Regulation. https://gdpr-info.eu/.
38. European Commission. Data protections: Rules for the protection of personal data inside and outside of the EU. https://commission.europa.eu/law/law-topic/data-protection_en.
39. Ministry of Electronics and Information Technology. (2022). The Digital Personal Data Protection Bill. https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf.
40. Google. Our privacy principles. Safety Center. https://safety.google/principles/.
41. Microsoft. (2022). *Responsible AI Standard, v2.* https://www.microsoft.com/en-us/ai/principles-and-approach/.
42. Thomas, J. (2021, 17 June). Foundations of trustworthy AI: Operationalizing trustworthy artificial intelligence (AI). IBM. https://www.ibm.com/blog/operationalizing-trustworthy-ai/?mhsrc=ibmsearch_a&mhq=trustworthy%20ai.
43. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
44. World Economic Forum. (2023). *Implementation Workstream: Pre-Implementation Briefing Paper.* https://www3.weforum.org/docs/WEF_World_Economic_Forum_Digital_Trust_Initiative_2023.pdf.
45. Microsoft. (2022). *Responsible AI Standard, v2.* https://www.microsoft.com/en-us/ai/principles-and-approach/.
46. Google. Data and Privacy. https://myaccount.google.com/intro/data-and-privacy.
47. Hay Newman, L. (2020, 14 December). Apple's App 'Privacy Labels' Are Here—and They're a Big Step Forward. *Wired.* https://www.wired.com/story/apple-app-privacy-labels/.
48. Apple. About App Privacy Report. https://support.apple.com/en-us/HT212958.
49. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.
50. Adrian, T. (2021, 29 October). AI and Regtech. International Monetary Fund https://www.imf.org/en/News/Articles/2021/10/29/sp102921-ai-and-regtech.
Warren, Z. (2023, 7 February) Financial institutions are increasingly eyeing fintech & regtech tools, but so are regulators. *Thomson Reuters.* https://www.thomsonreuters.com/en-us/posts/legal/fintech-regtech-tools-regulation/
Vereckey, B. (2022, 8 March). Compliance demands spur firms to invest in 'regtech' — and more. MIT Sloan. https://mitsloan.mit.edu/ideas-made-to-matter/compliance-demands-spur-firms-to-invest-regtech-and-more.
Markovitz, G. (2023, 20 March). Could regulation technology - or 'reg-tech' - avert banking failures? This entrepreneur thinks so. *Agenda.* https://www.weforum.org/agenda/2023/03/banking-crisis-regulation-technology-regtech-financial-turmoil/.
51. Adrian, T. (2021, 29 October). AI and Regtech. International Monetary Fund https://www.imf.org/en/News/Articles/2021/10/29/sp102921-ai-and-regtech.
Broeders, D. and Prenio, J. (2018). *FSI Insights on policy implementation No 9: Innovative technology in financial supervision (suptech) – the experience of early users.* Bank for International Settlements. https://www.bis.org/fsi/publ/insights9.pdf.
52. EnfTech Project. EnfTech: maximising the potential of technology in consumer law enforcement. https://www.enftech.org/.
United Nations Conference on Trade and Development. (2023). Introducing EnfTech: A technological approach to consumer law enforcement. https://unctad.org/meeting/introducing-enftech-technological-approach-consumer-law-enforcement.
53. U.S. Federal Trade Commission. Fair Credit Reporting Act. https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

54. European Commission. (2023, 28 June). *Financial data access and payments package.* https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en.

55. Access Now. Digital Security Helpline. https://www.accessnow.org/help/.

56. Consumer Reports. Permission Slip. https://permissionslipcr.com/.

57. Chao, B., Null, E. and Park, C. (2019, 20 November). Enforcing a New Privacy Law. New America. https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/.
Tang, A. (2022, 3 June). Demystifying China's Personal Information Protection Law: PIPL vs. GDPR. ISACA. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/demystifying-chinas-personal-information-protection-law.
Kerry, C.F. and Morris, J.B. (2020, 7 July). In privacy legislation, a private right of action is not an all-or-nothing proposition. Brookings Institution. https://www.brookings.edu/articles/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition/.
U.S. Federal Trade Commission. Fair Credit Reporting Act. https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.
European Parliament (2016, 27 April). Regulation (EU) 2016/679 of the European Parliament and of the Council. National People's Congress (2021). Personal Information Protection Law of the People's Republic of China (Chairman's Order No. 91). State of California. California Consumer Privacy Act, CCPA, through Cal. Civ. Code § 1798.150 read with Cal. Civ. Code § 1798.82.

58. World Economic Forum. (2022). *Earning Digital Trust: Decision-Making for Trustworthy Technologies.* https://www.weforum.org/reports/earning-digital-trust-decision-making-for-trustworthy-technologies.

59. Cyber Security Agency of Singapore. Cybersecurity Labelling Scheme. https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.

60. United Nations Conference on Trade and Development. (2016). *United Nations Guidelines for Consumer Protection.* https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org