Digital Trust and Why It Matters

CHEW HAN EI[1]

Senior Research Fellow

JEANNE TAN

Research Assistant

CAROL SOON[1]

Principal Research Fellow &

Head, Society & Culture

Institute of Policy Studies

Lee Kuan Yew School of Public Policy

National University of Singapore

[1]Principal Investigators

NUS Centre for Trusted Internet and Community

This report is funded by the NUS Centre for Trusted Internet and Community
[Research Grant CTIC-RP-20-04]

Table of Contents

Executive Summary 4
1 A Global Decline in Digital Trust 6
1.1 Methodology 8
1.2 Two plus one approaches for understanding digital trust 8
1.3 Digital trust definitions 10
2 Mechanical Digital Trust (Trustworthy Technology) 13
2.1 Cybersecurity 15
2.2 Safety 16w
2.3 Privacy 17
2.4 Auditability, transparency and accountability 18
2.5 Usability and ease of use 19
2.6 Reliability and predictability 20
2.7 Information and content quality 21
2.8 Interoperability 23
2.9 Fairness 23
2.10 Redressability 23
3 Digital Trust as Relational Trust 24
3.1 Individual traits that affect relational digital trust 26
3.1.1 Digital literacy and attitudes towards technology 26
3.1.2 Experiences in using technology 27
3.1.3 Propensity to trust 29
3.1.4 Age 30
3.1.5 Income 30
3.1.6 Education 30
3.2 Interpersonal factors that affect digital relational trust 30
3.2.1 Strength of ties in digital networks relationships 31
3.2.2 Perceived similarity and homophily 32
3.2.3 Shared community values 32
3.2.4 Increased trust from repeated interactions 33
3.2.5 Benevolence demonstrated through responsiveness 34
4 Digital Trust Ecosystem 34
5 Interrelation Between Offline and Digital Trust in Government 37
5.1 Dimensions of mechanical digital trust in e-government 37
5.1.1 Privacy and security in e-government 37
5.1.2 Transparency in governance through e-government 39

5.1.3 Functional attributes that drive trust in e-government 40
5.2 Dimensions of relational digital trust in e-government 40
5.2.1 Trust in technology 40
5.2.2 Digital literacy and experience 40
5.2.3 Propensity to trust 41
5.3 Bi-directional nature of trust and digital trust in e-government 41
5.3.1 Genesis of trust in e-government 41
5.3.2 Interaction with e-government 42
5.3.3 Cycle of use and trust in e-government services 43
6 Digital Trust in Singapore 43
6.1 Singapore's approach to building digital trust 46
6.1.1 Build resilient infrastructure 47
6.1.2 Enable a safer cyberspace 49
6.1.3 Enhance international cyber cooperation 53
6.1.4 Develop a vibrant cybersecurity ecosystem 54
6.1.5 Grow a robust cyber talent pipeline 54
7 Recommendations From an Ecosystem Perspective 56
7.1 Adhering to state-of-the-art data privacy practices 57
7.2 Defining the scope of cyber safety and online harms 58
7.3 Preparing for interruptions in digital services through collective capacity building 59
7.4 Improving redressability for end users 59
7.5 Building a whole-of-nation mindset for digital trust 60
7.6 Expanding the trust ecosystem for cybersecurity to the region 62
8 Conclusion 63
9 References 65
10 Appendix: Expert Interview Guide 80

Executive Summary

The digital revolution has increased quality of life in many aspects but has also exposed individuals to sophisticated and prolific cyber threats and online harms. The World Economic Forum (WEF) has warned that some organisations' technology usage has led to uneasiness, resulting in a decline in trust that could limit digitalisation benefits (n.d.-b).

This review focuses on unpacking the concept of digital trust. For this, we conducted a literature review that synthesised academic research, consultancy reports, policy research, intergovernmental research, press releases, and news publications. We also conducted four in-depth interviews with domain experts from around the world, on their thoughts about the components of digital trust. They are Tammy Lin (National Chengchi University), William Dutton (Michigan State University), Gregory Porumbescu (Rutgers University) and Jonathan Obar (York University).

The review comprises two parts. The first half of the review explores the two key types of digital trust and their corresponding dimensions, followed by a discussion on a digital trust ecosystem that synthesises both types of digital trust. The complexities and the bi-directional nature of offline and online trust are then explored in the case of e-government. The latter section of the review focuses on the gaps in digital trust through an analysis of global indices for digital trust as well as local policies that have contributed to the development of digital trust. Here, we offer suggestions on how policies and programmes can evolve to enhance digital trust in Singapore. Recommendations in this review are intended for practitioners and policymakers.

What is digital trust?

Digital trust can be distinguished into two core types — mechanical and relational trust (Dobrygowsky & Hoffman, 2018). Mechanical digital trust refers to the "means and mechanisms that deliver predefined outputs reliably and predictably" (Dobrygowsky & Hoffman, 2018). This includes applications of technology such as generative AI, Internet of Things and blockchain processes, as well as website infrastructure, such as functionality and usability. In our review, we operationalise and evaluate mechanical digital trust through the following 10 dimensions: cybersecurity; safety; privacy; auditability, transparency and accountability; usability; reliability; information and content quality; interoperability; and fairness and redressability.

Relational digital trust is related to traditional trust between people, which influences the adoption of digital tools. It can also be understood as the social norms and expectations of using digital tools (Dobrygowsky & Hoffman, 2018). Relational digital trust is influenced by individual traits, which include one's level of digital literacy, experience in using digital technology, propensity to trust and demographic variables, as well interpersonal factors such as the strength of ties in digital networks relationships, homophily and more.

A synthesis of both mechanical digital trust and relationship digital would result in an **"ecosystem approach"** towards understanding digital trust. This integrated approach recognises the importance of digital connections in different aspects of people's lives and that it takes both mechanical digital trust and relationship digital trust for the benefits of technology to be fully realised.

Another complexity of digital trust is that it can also be both a cause and an effect simultaneously. This review also examines the various dimensions of relational and mechanical digital trust in the context of e-government to illustrate this. The adoption of e-government services first requires offline relational trust in government. Therefore, trust is seen as a cause. Once adopted, digital users' trust in e-government services is reinforced as they acquire greater awareness of government policies. Digital trust increases relational trust in government. Hence, trust can also be an effect.

Singapore has been actively cultivating and reinforcing digital trust in the country and region. The Digital Trust scorecard developed by the Fletcher School at Tufts University ranks Singapore highly for its performance in terms of digital users' engagement with e-commerce, use of technology for daily services, reliance on digital or mobile wallet, accountability and security, institutional credibility, and digital hygiene. However, Singapore's trust-building mechanisms related to privacy, security and accountability were not as well-regarded. In particular, scores on privacy concerns and trust in science and technology were especially low.

Gaps and recommendations

Our review of Singapore's approach to building digital trust sheds light on the ways in which existing initiatives bolster the key dimensions of mechanical digital trust in terms of cybersecurity, safety and privacy, as well as relational digital trust, and through improving digital literacy and technology experiences for individuals. However, more work needs to be done to increase transparency in e-government and privacy protection. Bearing in mind that developing a trustworthy digital ecosystem is a challenge due to the constant evolution of digital technologies and the changing landscape, we offer recommendations on how to enhance and leverage the dimensions of digital trust through collaboration with public agencies, private entities, the community, and also between countries. Some of these recommendations include adhering to best practices in data privacy, defining the scope of cyber safety and online harms, improving redressability for digital end users, and building a whole-of-nation mindset for digital trust.

1 A Global Decline in Digital Trust

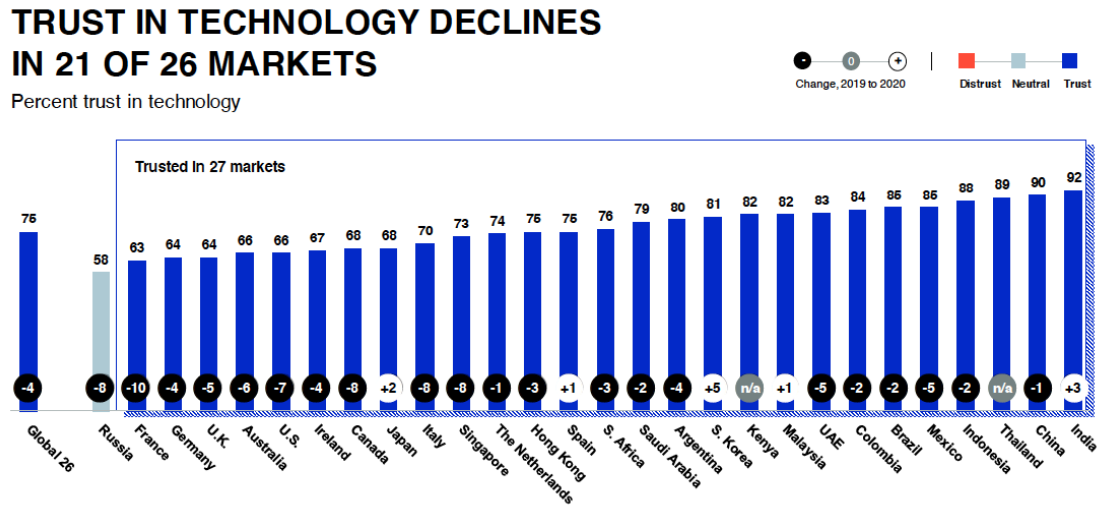
The digital revolution has accelerated in recent years, catalysed by the COVID-19 pandemic, which necessitated widespread adoption of digital technologies like contact-tracing apps, telecommuting, e-learning and telemedicine (Kumaran & Lugani, 2020). Widespread digitalisation has no doubt increased quality of life in some aspects but has also exposed individuals to sophisticated and prolific cyber threats and online harms. In April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 in just one week (Kumaran & Lugani, 2020). The number of cyberattacks has also increased, with the 2021 State of Cybersecurity Report by Accenture noting that an average company experienced 270 attacks in the year (Bissell et al., 2021). Additionally, 2021 witnessed a record number of data breaches, totalling 1,862 breaches, or a 68 per cent increase from the previous year (Identity Theft Resource Center, 2022).

Despite technology's affordances and benefits during the pandemic, misinformation spread through digital platforms have also amplified discontent and mistrust in societies. These developments that erode trust in the digital realm run diametrically opposite to the global trend of technology becoming increasingly integrated with essential societal functions, such as e-governance and e-payments. The World Economic Forum (WEF) has warned that some organisations' technology usage has led to uneasiness, resulting in a decline in trust that could limit digitalisation benefits (WEF, n.d.-b)

International studies provide evidence of the eroding trust. The Centre for International Governance Innovation (CIGI) and Ipsos have conducted large international user surveys since 2014 and in 2019 reported that 75 per cent of users who distrust the internet agreed that social media platforms contributed to their lack of trust (CIGI-Ipsos, 2019).

The 2020 Edelman *Trust Barometer Special Report: Trust in Technology* revealed that trust in technology decreased by an average of 4 percentage points between 2010 to 2020 in 21 out of 26 markets (Edelman, 2020). The largest declines were reported in France (10 percentage points), Canada, Italy, Russia and Singapore (8 percentage points), the United States (7 percentage points), and Australia (6 percentage points). Singapore ranked 18th out of the 26 markets studied (see Figure 1).

Figure 1. Decline in trust in technology



The Edelman study highlighted concerns regarding technology being out of control, with 61 per cent of respondents feeling that the pace of technological change is too fast. Additionally, 66 per cent of respondents agreed that their governments lack an adequate understanding of emerging technologies to effectively regulate them. There is also distrust in emerging technologies, including artificial intelligence (AI), the Internet of Things, virtual reality, and 5G cellular technology.

Locally, Singapore has seen an increase in security and privacy breaches in recent years. In 2022, a phishing scam targeting OCBC Bank customers led to at least 469 victims, with losses totalling at least S$8.5 million (Raguraman, 2021). This incident prompted many senior citizens to terminate their bank accounts (Chew & Soon, 2022). The total number of scam and cybercrime cases rose from about 27,000 cases in 2021 to about 34,000 cases in 2022. Victims lost nearly S$661 million in 2022 (Singapore Police Force, 2023).

To address these issues, Singapore has redoubled its efforts to build and rebuild digital trust. In June 2022, the Infocomm Media Development Authority (IMDA) and the National Research Foundation launched the Digital Trust Centre (DTC). According to IMDA (2019b), digital trust requires technology to be secure and used responsibly, and the DTC aims to deepen research on trust technologies that help build and uphold digital trust, such as privacy protection solutions. The call to action to backstop declining digital trust was also echoed by the private sector. At a 2022 global forum on Digital Trust, SGTech Chair Mr Wong Wai Meng said,

> "Digital Trust will be a game-changer for Singapore to secure its place as a global digital and data node. To fully capitalise on this opportunity will require an acceleration in our capabilities building and skills development that demands the collective will and vision of our government, businesses, and individuals." (SGTech, 2022b)

The contrasting milieu of widespread adoption and growing distrust is the backdrop of the fourth and final review in our series of four policy reviews on the digital landscape in Singapore. **The singular goal of this policy review is to clarify the concept of "digital trust" and why it matters for our Smart Nation goals.** The review aims to define digital trust, identify

factors that increase and decrease digital trust, and explore how Singapore can build digital trust.

1.1 Methodology

For this report, we conducted a literature review that synthesised about 223 secondary sources comprising academic research, consultancy reports, policy research, intergovernmental research, press releases, and news publications. Key search terms included “online trust”, “digital trust”, “trust in technology”, “trust in digital media”, and other related terms specific to each section. This review was conducted online from August to December 2022. Current, Singapore-based and diverse sources were included wherever possible.

As part of this review, we also conducted in-depth interviews with domain experts from around the world on their thoughts about improving digital inclusion. The four domain experts are professors who are thought leaders in the field — from Taiwan, the United Kingdom, and the United States. They are:

Tammy Lin

Distinguished Professor, College of Communication, National ChengChi University

William Dutton

Quello Professor of Media and Information Policy, Michigan State University

Gregory Porumbescu
Associate Professor, School of Public Affairs and Administration, Rutgers University

Jonathan Obar

Associate Professor, Department of Communication & Media Studies, York University

The interviews were conducted online in December 2022 and January 2023. Each interview was recorded with consent and lasted an hour on average. The interview guide can be found in the appendix. Direct quotes from the interviews can be found throughout the review where we thought they were most relevant. As we had done for the first three reviews, we begin our final review with approaches to define digital trust.

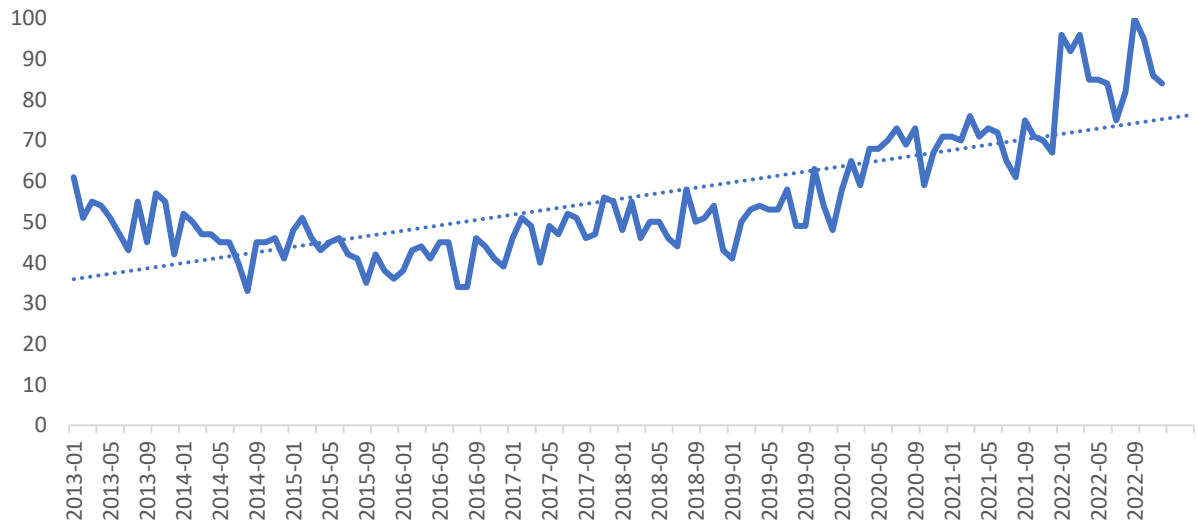
1.2 Two plus one approaches for understanding digital trust

Efforts to define digital trust are nascent, and there is no one definition of online trust or digital trust. Trust itself is a highly complex concept even in the offline world, often misunderstood and taken for granted (Connolly, 2007). There is also a lack of evidence-based assessments

that provide insights on the drivers of digital trust and a dearth of proper guidelines for various stakeholders to work together to build digital trust. Without a clear consensus on digital trust, understanding how it functions in the online world and how to improve it becomes even more challenging.

In our review of studies and reports on the topic, interest in digital trust has clearly been increasing. Google trends for the search term “digital trust” worldwide has seen a gradual increase from 2013 to 2022 (see Figure 2). In the references that we have consulted, digital trust was more commonly discussed in commercial and consultancy reports and less by academics. More work on the topic seems to be done by practitioners than academics and the definitions are consequently adapted to the business domain.

Figure 2. Monthly Google trends for “digital trust” (worldwide) from 2013 to 2022[1]



Among the literature we consulted, the terms “trust in the digital era” and “digital trust” are often used interchangeably. However, several works point out that digital trust encompasses trusting not only people and abstract systems, but also technical and technological systems (Kożuch, 2021).

Dobrygowsky and Hoffman (2018) distinguished digital trust into two core types: mechanical and relational trust. The authors refer to **mechanical digital trust** as the “means and mechanisms that deliver predefined outputs reliably and predictably.” Applications of technology, such as generative AI, Internet of Things and blockchain processes, can be considered “mechanical”. Other scholars such as Corritore et al. (2003) have also studied how website infrastructure, such as functionality and usability, affects digital users’ degree of trust in a website. When these technological systems perform reliably, individuals have greater mechanical digital trust.

[1] The numbers on the graph do not represent absolute search volume numbers, because the data is normalised and presented on a scale from 0 to 100, where each point on the graph is divided by the highest point, or 100. A line trending downward means that a search term's relative popularity is decreasing — not necessarily that the total number of searches for that term is decreasing, but that its popularity compared to other searches is shrinking.

Relational digital trust can be considered an extension of traditional trust adapted to the digital age. Relational trust is examined in terms of trust between people and how it drives the adoption of digital tools. For example, researchers such as Kim (2008) and McKnight et al. (2002) have examined how trust in another actor, such as another person or web vendor, drives digital users' decision to use technology.

For Dobrygowski and Hoffman (2018), relational trust refers to the norms and expectations in society and in the context of digital trust, a "shared agreement on when, where, why and how technologies are used." For digital trust to be built, individuals, organisations and policymakers need to have a common set of rules and understanding for the use of technology so that their different interests are aligned. Without these common sets of rules, trust and digital trust between these stakeholders would continue to erode.

The third approach in the literature that we have reviewed is the **"ecosystem approach"** that synthesises the first two approaches, and accounts for both relational and mechanical digital trust (although the distinctions may not always be clear and consistent).

For instance, Shankar et al. (2002) pointed out that the first two approaches have different objects of trust. The object of traditional (relational) trust is generally a person or an entity. In the context of digital spaces, the object of trust typically refers to the technology and *the organisation that supports it*. In the context of commerce, customers place their trust in sellers or organisations they purchase from in a traditional offline context (Doney & Cannon, 1997) while customers of e-commerce must be able to trust the website they are purchasing from, as well as *the company that own the website* (Boyd, 2003). It is unclear from the above studies if trust in an organisation is wholly relational or wholly mechanical, but we posit that organisations are purveyors and stewards for both. This integrated approach seems to be most promising, as it recognises the importance of digital connections in different aspects of people's lives and that it takes both mechanical digital trust and relational digital trust for the benefits of technology to be fully realised.

1.3 Digital trust definitions

We categorised the different definitions of digital trust from our review in Table 1, according to the approach that each of the source takes. Digital trust is categorised three ways: as **mechanical trust**, as **relational trust,** and as an integrated concept that accounts for both relational and mechanical trust, and usually referred to as a **trust ecosystem**. This integrated approach typically describes confidence in the digital ecosystem or in societal norms and structures.

Table 1. Selected definitions of digital trust

Definition	Actors	Source
Digital trust as mechanical trust		
Individuals' expectation that digital technologies and services — and the organisations providing them — will protect	Consumers and businesses	WEF (n.d.-a)

all stakeholders' interests and uphold societal expectations and values.		
Consumer faith in cybersecurity, data privacy, and responsible AI.	Consumers and businesses	McKinsey & Company (2022)
Level of confidence that consumers enjoy while interacting digitally for consuming their various services.	Consumers and businesses	Singh & Malhotra (2022)
People's confidence that a platform will protect their information and provide a safe environment for them to create and engage with content.	Users and platforms	Business Insider Intelligence (2020); Williamson (2022)
An attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited.	Consumers and businesses	Corritore et al. (2003)
Digital trust is an evolution of traditional trust models to cover the additional requirements of digital business — deriving levels of measurable confidence to make risk-based decisions.	Consumers and businesses	Gaehtgens and Allan (2017) as cited in Kożuch (2021)

Digital trust as relational trust		
A reliance on a firm by its stakeholders with regard to its business activities in the electronic medium, and in particular, its website.	Consumers and businesses	Shankar et al. (2002)
Confidence placed in an organisation to collect, store and use the digital information of others in a manner that benefits and protects those to whom the information pertains.	Consumers and businesses	Accenture (2014)
Belief that a brand is reliable, capable, safe, transparent and truthful in its digital practices.	Consumers and businesses	Lynch et al. (2016)

Integrated "ecosystem" approach that incorporates relational and mechanical trust		
Digital trust is trusting not only in people we know and abstract systems, but also in technical and technological systems.	Users, platforms and businesses	Kożuch (2021)
Confidence that participants have in the digital ecosystem to interact securely, in a transparent, accountable and frictionless manner.	Users, platforms and businesses	SGTech (2022a)

Confidence in the integrity of the relationships, interactions and transactions among suppliers or providers and customers or consumers within an associated digital ecosystem.	Consumers and businesses	ISACA (2022)
The level of confidence in people, processes and technology to build a secure digital world.	Users, platforms and businesses	PwC (2018) Paliszkiewicz and Chen (2023)

Two commonalities stand out across the definitions. First, **confidence** is the most common term used to describe the concept of digital trust. Confidence is commonly expressed as between consumers and businesses and between users and platforms.

The second commonality is the notion that **trust is a two-way street**. Across various disciplines and the approaches discussed above, risk and interdependence are two important aspects that characterise a trust relationship (Coleman, 1990; Rotter, 1967; Williamson, 1993). The source of risk is the uncertainty regarding the intention of the other party. Corritore and colleagues (2003) argued that there are similarities in trust relationships that cut across both online and offline settings. Transactions are impeded by risk, fear, complexities and costs, and enhanced by cooperation and coordination in both settings. Therefore, trust — in both online and offline settings — can be defined as a form of expectation of the trusted parties' behaviour, and **requires the trusting individual to be subjected to vulnerability or risk**.

Interdependence is characterised by the fact that the interests of the two parties are related and cannot be achieved without relying on each other. Just as trusting individuals subject themselves to risk, **trusted parties must also work to portray themselves as trustworthy in both the online and offline environment** (Boyd, 2003). The relationship is not a trust relationship if these two conditions do not exist (Sherchan et al., 2013). Since risk and interdependence are necessary conditions for trust, changes in these factors over the course of a relationship may alter both the level and the form of that trust (Rousseau et al., 1998).

Having introduced the two main types of digital trust — mechanical and relational — and explored the definitions under these two approaches for understanding digital trust, we will examine the dimensions and factors that contribute to mechanical and relational digital trust in the following two chapters. After that, we will explore how a digital trust ecosystem can be built in Singapore by enhancing mechanical and relational trust. Understanding these different dimensions is important because building digital trust cannot be done at the abstract and general level and requires specificity in addressing each dimension:

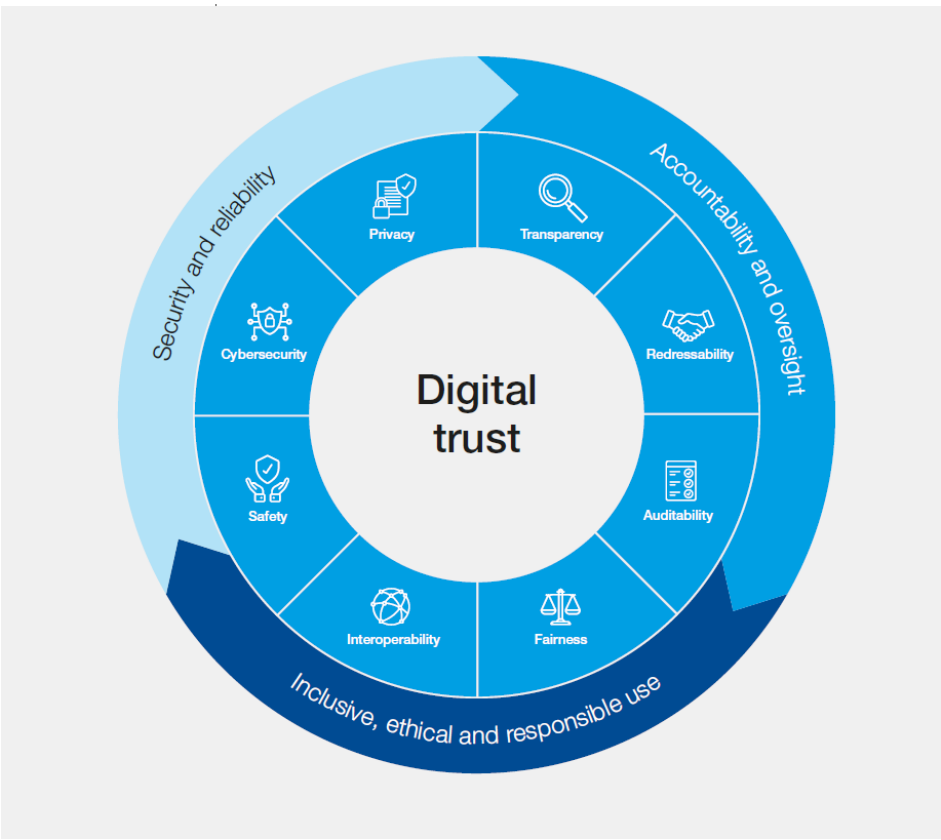
> [Bill Dutton on *assessing* digital trust] "It's okay to ask people, do you trust the Internet or do you trust digital media, but it's very generic and very diffused…. So, I would try to ask specific questions about privacy, about information accuracy, about protection of your privacy, about protection of your security…. Those will be more concrete…. It becomes more specifically related to what you're trusting…. If you ask in broad, abstract terms, people often say things that does not apply to concrete realities."

2 Mechanical Digital Trust (Trustworthy Technology)

In November 2022, the WEF published the report "Earning Digital Trust: Decision-Making for Trustworthy Technologies" in collaboration with Accenture, KPMG and PricewaterhouseCoopers. The report represents one of the first global attempts to provide a unifying concept of digital trust and offers a framework to develop digital trust based on discussions among government officials, prominent consumer advocates as well as delegates from major tech and consumer-centric companies. The report defined digital trust as "individuals' expectation that digital technologies and services — and the organisations providing them — will protect all stakeholders' interests and uphold societal expectations and values." The framework specifically targets companies to commit to earning digital trust.

It defines three set of shared goals or values that inform the concept of digital trust, including: security and reliability; accountability and oversight; and inclusive, ethical and responsible use (see Figure 3).

Figure 3. Digital Trust Framework (WEF, 2022, p. 9)



The framework also defines eight dimensions against which **the trustworthiness of digital technologies** (or mechanical digital trust) can be operationalised and evaluated:

- Cybersecurity
- Safety
- Privacy
- Auditability
- Transparency

- Interoperability
- Redressability
- Fairness

We cross-referenced these dimensions against several other typographies of digital trust in our review (see Table 2). Among the various typographies, the most mentioned dimensions include cybersecurity (and) safety, privacy, accountability and auditability, and societal benefits. Transparency, accountability and auditability are frequently discussed in conjunction. Interoperability, fairness and redressability are exclusively listed by the WEF. Other researchers such as Marcial and Launer (2019) have proposed a smaller set comprising safety, security, reliability, privacy, and data ethics. The rest of this chapter explores the full 10 dimensions in order of their frequency of mentions across different typographies, starting with the most mentioned dimensions of cybersecurity and safety.

Table 2. Dimensions of (mechanical) digital trust

(WEF, 2022)	**(Accenture, 2014)**	**(PwC, 2018)**	**(ILNAS, 2017)[2]**	**(Business Insider Intelligence, 2020)[3]**	**(Kożuch, 2021)**
Cybersecurity	√	√	√	√	√
Safety		√			√
Privacy	√	√	√		√
Auditability	(Accountability)	√	(Accountability)	(Legitimacy)	(Accountability)
Transparency					
Interoperability					
Redressability					
Fairness					
Benefits for users	Consumer value	Stakeholder value	Benevolence	Good ad relevance	Benevolence to users

[2] The Luxembourg Institute of Standardisation, Accreditation, Safety and Quality of Products and Services (ILNAS) identifies criteria for assessing technical and technological systems as assurance, accountability, benevolence, competence and ability, integrity, predictability, privacy, reputation and security (ILNAS, 2017).

[3] Business Insider Intelligence's definition of digital trust is platform-specific and refers to the confidence individuals have in a platform's ability to safeguard their information and provide a secure environment for content creation and engagement (Business Insider Intelligence, 2020). Their five-dimension typology model of digital trust includes security, legitimacy, trustworthy community, bitter ad experience, and good ad relevance.

2.1 Cybersecurity

The importance of cybersecurity for digital trust cannot be overstated. **Cybersecurity focuses on the security of digital systems, including data, technologies, and processes; and is crucial for maintaining the confidentiality, integrity and availability of data and systems** (NIST, 2020). Given the significant threats digital processes are exposed to today, having strong and effective cybersecurity programmes — and as a result being seen as strongly protective of the data and information that users share — as well as being resilient to potential attacks is paramount for secure and reliable digital technologies and systems (WEF, 2022).

When individuals use digital services and products, they expect them to meet their expectations and protect their data. The reliability of these offerings is closely tied to the trust users place in them and their providers. If a service or product fails to function predictably, reliably and securely, users may withhold support, discontinue usage or refuse to share their data (WEF, 2022). Therefore, cybersecurity is essential for establishing and maintaining trust in digital technologies and the digital economy.

Another key reason why cybersecurity is essential for digital trust is its role in defending against threats. Security threats encompass various circumstances, conditions or events that can result in economic hardship, including destruction, disclosure, data modification, denial of service, fraud, waste and abuse (Kalakota & Whinston, 1997). Security features act as protective measures against these attacks, establishing a perception of reliability and trustworthiness for technology systems (Jøsang et al., 2007).

Furthermore, in today's sophisticated threat landscape, traditional access control mechanisms such as username and password combinations are insufficient. Companies must implement advanced technologies, such as biometric authentication, to offer stronger security measures for safeguarding sensitive information and addressing concerns related to identity and privacy (Accenture, 2014).

Studies have also found that the presence of security-enhancing features on websites reassures digital users and builds trust (Benlian & Hess, 2011; Gauzente, 2004). In the e-commerce setting, Suh and Han (2003) found that consumers' perceptions of data security controls on an e-commerce website affect their trust in the platform. The use of secure payment mechanisms and technologies against hackers has also been found to provide consumers with a sense of security (Mukherjee & Nath, 2003). When users identify security features and protection measures, like security policies and authentication, they recognise the web vendor's commitment to meeting security requirements (Chellappa, 2008), which reduces perceived risk in online transactions.

In fact, Belanger et al. (2002) found that respondents in their study placed more importance on security features than privacy statements, security seals and privacy seals. They suggested that this is because digital users were able to understand and identify security features better than privacy statements. Nevertheless, it is important to note that digital users' perceptions of how secure a technology is also dependent on their ability to understand the level of security measures implemented by the web vendor (Friedman et al., 2000).

Failing to prioritise cybersecurity can have dire consequences for organisations. In today's interconnected age, even a minor cybersecurity incident or a brief downtime of a major digital

service provider can result in significant reputational and financial damages, especially when security is compromised (WEF, 2022). Therefore, it is vital for organisations to ensure the proper security of their information systems, protecting customer data and addressing identity and privacy issues (PwC, 2018). By implementing effective cybersecurity measures, organisations can mitigate risks and safeguard the resilience of their digital processes and systems. Neglecting cybersecurity is a risk that no organisation can afford to take.

2.2 Safety

Safety as it relates to digital trust is often discussed with security. The WEF distinguishes safety as **efforts to prevent harm** (e.g., emotional, physical, psychological) to people or society from technology uses and data processing (WEF, 2021). Online harm can be broadly understood as “user generated content or behaviour that is illegal or could cause significant physical or psychological harm to a person” (gov.uk, 2021); and some of the most egregious harms that are being perpetrated online include child sexual exploitation, terrorism and materials that advocate self-harm and suicide. The trustworthiness of technology and trust in online activities is compromised when users encounter online harms and consequently, feel unsafe navigating the digital world.

> [Tammy Lin on the importance of digital users feeling safe] “I think the platform needs to offer options for users to feel safe and autonomous. For example, in the VR platform, because there’s so much harassment, the first thing is to feel safe…. Every person has a boundary, like I prefer a lot of space when I talk to you or I prefer really intimate space. Everyone has different boundaries, so the system has to be able to allow people to set up these kinds of boundaries. If people can feel safe, then they will definitely trust the platform.”

When organisations prioritise the best interests of their users and stakeholders by implementing appropriate safeguards and safety mechanisms, they enhance their digital trustworthiness. Conversely, digital trust is compromised when organisations are perceived as negligent in protecting the safety of their stakeholders and users.

However, the reality is more complex. The list of online harms mentioned earlier is not exhaustive, and as new technological tools and platforms emerge, the nature of these harms and social norms surrounding them will continue to evolve. The ever-changing landscape of technology presents challenges in predicting and implementing safety measures against online harms.

The growing public awareness and concern regarding online safety prompted the establishment of the world’s first independent regulator for online safety — the eSafety Commissioner — in 2015. The eSafety Commissioner is an agency composed of educators, investigators, lawyers, policy analysts, technology experts, digital specialists, and other professionals with the mission to ensure "a safer and more positive online experience for all Australians" (eSafety Commissioner, n.d.). On a global scale, the WEF established the Global Coalition for Digital Safety in 2019. This coalition serves as a public-private platform for global

multi-stakeholder cooperation. Its purpose is to develop innovations and advance collaborations to tackle harmful content and conduct online (WEF, n.d.-b).[4]

Singapore is also at the forefront of online safety and has taken major steps to ensure online safety for its citizens. These efforts are listed in section 6.1 of this report.

2.3 Privacy

The WEF (2022) describes privacy for individuals as the expectation of control over or confidentiality of their personal or personally identifiable information. Privacy relates to the uncertainty of disclosing personal information online and the risk of such information being revealed (Bart et al., 2005). Privacy for organisations is the meeting of this expectation through the design and manifestation of data processing that facilitates individual autonomy through notice and control over the collection, use and sharing of personal information (GDPR.EU, 2016). Digital users' information privacy concerns have a profound effect on trust in web vendors (Malhotra et al., 2004) and online privacy issues most often include spam mails, usage tracking and data collection, and sharing of data with third parties (Belanger et al., 2002).

Perceptions of privacy protection on websites can contribute to the development of system trust and decrease digital users' perceptions of uncertainty (Gauzente, 2004). It enables digital users to feel that their personal information is being handled by the web provider in a way that is consistent with their personal convictions (Gauzente, 2004). These features act as a signal to digital users that web providers are not misusing the data that have been collected, which increases digital users' trust with the system and their willingness to share personal information (Wu & Tsang, 2008).

However, digital users and organisations often have different perceptions of digital trust in relation to privacy. A survey by Frost & Sullivan revealed that organisations overestimate the degree to which digital users trust them to use their data in appropriate ways. Digital users scored an average score of 62 out of 100 in digital trust while organisations scored 75 out of 100 on average — a perception gap of 14 points.

Other studies have found what digital users are worried about when engaging in online activities. A 2022 survey by MAGNA, a global media investment and intelligence company, found that 82 per cent of respondents were concerned about how companies were collecting and using their personal data and 64 per cent of respondents believed that they had little control of how their data was being utilised. Privacy concerns also increase when digital users are unaware of who is collecting their personal information, how the data was obtained and what it was being used for (Lanier Jr & Saini, 2008).

Although privacy protection features have been shown to increase web vendors' perceived trustworthiness (Lauer & Deng, 2007), studies suggest that digital users rarely read the privacy statements provided on websites before disclosing personal information (Arcand et al., 2007; Vu et al., 2007). According to the CISCO 2022 Consumer Privacy Survey, respondents often feel unable to effectively protect their data due to difficulties in understanding how organisations use their data. Digital users are unlikely to review privacy policies if they find

[4] These efforts are also mentioned in our policy review – Digital Sovereignty: State action and implications for Singapore (Soon et al., 2023).

them incomprehensible (Milne & Culnan, 2004). Most digital users are less concerned with the specific details of privacy policies (Earp & Baumer, 2003). However, the mere presence of a privacy policy can convince digital users that web vendors are trustworthy in protecting their personal data (Pan & Zinkhan, 2006).

Jonathan Obar, one of four experts we interviewed, highlighted the need for easy-to-understand privacy statements and what needs to be done to improve the implementation of privacy statements:

> [On the problem of notice statements] "'I agree to the terms and conditions' is referred to anecdotally as 'the biggest lie on the internet'…. People want to enjoy the ends of digital production without being inhibited by the means, at least in terms of the current presentation of the means. I think that if the means of digital production were presented in a more manageable way, then perhaps people would engage more. But at the moment it seems like people find [the] notice to be quite a nuisance.... That's certainly a challenge, to get to a recommendation or an implication for companies, governments, platforms — finding the right opportunity, finding the right time to build trust in the right way to do it is vital because our research has also demonstrated how long and complicated privacy, in terms of service policies, are."
>
> [On the challenges of clickwraps[5]] "Current implementations of notice policy aren't working very well. This isn't to say that we should move away from notice policy. I believe strongly that consent is very necessary, very important in ensuring information protections, and I do agree that people should be making informed decisions all the time…. But there are many challenges to realising this. One thing, for example, is that clickwraps are problematic, if not deceptive, user interface designs that, we argue, put people in, like, fast lanes towards monetisation, towards monetised sections of services, as opposed to helping people to access, engage, read and understand these contracts that they're agreeing to."

2.4 Auditability, transparency and accountability

Auditability is the ability of both an organisation and third parties to review and confirm the activities and results of technology, data processing and governance processes (Johnson, 2021) while transparency is the "availability of information about an actor that allows the other actors to monitor the workings or performance of the first actor" (Meijer, 2013, p. 430).

When organisations are transparent about their practices, trust increases because digital users feel that they have autonomy over the data that is shared with other digital users and the knowledge that others have of them (Gauzente, 2004). Organisations that provide transparent views of the inner workings of technology allow digital users to feel more in control and better evaluate the effects of their actions online.

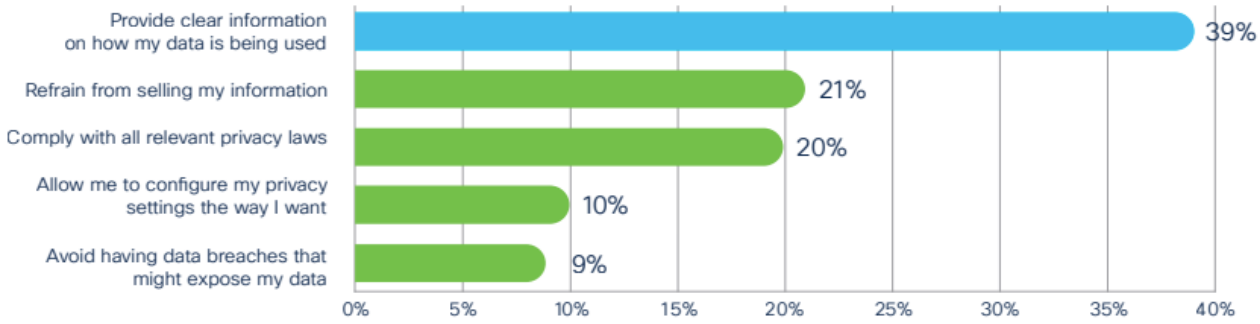
The consequence of presenting consumers with the specific use of their data is that they are more willing to share (KPMG, 2021). In the KPMG study, 57 per cent of their respondents deem the use of facial recognition technology to assist in criminal investigations as acceptable.

[5] The clickwrap is a digital 6 that facilitates consent processes by affording users the opportunity to quickly accept or reject digital media policies (Obar & Oeldorf-Hirsch, 2018).

Additionally, 52 per cent of the respondents are comfortable with organisations using recorded calls for quality and training purposes.

The CISCO 2022 Consumer Privacy Survey found that the most important data practice is providing digital users with the knowledge of how their data is being used (see Figure 4). Lucas and Stein (2020) also found that users want web vendors to provide clear insights on how and why data is collected and used. KPMG (2021) found that 77 per cent of the US general population and business leaders seek greater autonomy and control of their data. Digital users will be more confident in web vendors when they provide specific explanations about how digital users' data will be used (KPMG, 2021).

Figure 4. Activities organisations can do to build trust with customers, regarding their data (Cisco, 2022)



Enabling visibility into an organisation's digital processes also "reduces the information asymmetry between an organisation and its stakeholders" while signalling to individuals that the organisation intends "not only to act in the individual's interest but also to make those actions known and understandable to those inside and outside of the organisation" (WEF, 2022). On the other hand, the lack of information transparency results in uncertainty among digital users (Chatterjee & Datta, 2008).

2.5 Usability and ease of use

When digital trust is mechanical, digital users also consider functional attributes of the technological system (McKnight & Chervany, 2001). Assessing the trustworthiness of a system is akin to assessing the trustworthiness of a person, as a user will draw on past experiences with the system to estimate the risk and uncertainty involved (Cheshire et al., 2010). The usability of a technology is an important functional attribute that is frequently mentioned in the literature.

Usability refers to "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" (Karat, 1997, p. 34). Research suggests that poor usability — such as low-quality design, errors and information deficiency — is often associated with low trust in a website (Everard & Galletta, 2005). For instance, Benlian and Hess (2011) found that the absence of usability-enhancing IT features, such as poor access to information and navigation cues, results in

lower levels of trust among digital users. Similarly, a study by Belanger et al. (2002) indicated that poorly designed websites detract users from engaging in online transactions.

On the other hand, easily accessible and clearly organised information on a website demonstrates consistency and reliability, thereby lowering digital users' perception of the risk of wasted time and frustration (Hampton-Sosa & Koufaris, 2005). Furthermore, a professionally designed website containing navigation elements integrated in a logical manner allows digital users to be more confident in using it, while promoting an overall perception of trustworthiness (Benlian & Hess, 2011). Consequently, digital users are likely to display higher levels of trust.

Perceived ease of use is related to usability in that it refers to the extent to which digital users believe that the use of technology would require little effort (Davis, 1989). Several studies in the e-commerce setting have found that the perceived ease of using technology has effects on the formation of trust. Bart et al. (2005) found that electronic vendors whose websites contain features that are easy to use and can swiftly direct digital users to their desired destination are able to obtain their trust. The ease of using and navigating a website is particularly important during the initial stages of using technology (Chau et al., 2007). Digital users may recognise a technology as less trustworthy based on their ability to make the technology do what they desire (Lippert, 2001). When they can understand the technical processes in using technology, digital users are likely to perceive it as reliable and less risky (Gefen et al., 2003). On the other hand, low levels of usability can result in technical errors, leaving digital users to distrust the technology and dissuading them from participating in online exchanges (Flavián et al., 2006).

Research in the e-government context suggests that e-government websites that are perceived to have greater ease of use result in greater levels of trust among digital users (Ayyash et al., 2013). Digital users who find e-government websites user-friendly will have a greater urge to use them (Ayyash et al., 2013). This is supported by a study by Al-Faries et al. (2013) who observed that e-government services that can be easily accessed by digital users can encourage users to adopt these services. Additionally, the accessibility of e-government services has been found to increase trust in government as it enables digital users to better evaluate the government's behaviours, policies and programmes (Mensah et al., 2021). This will in turn affect citizens' decision to trust or not trust in government. Conversely, e-government websites that are perceived to be complex will deter users (Lean et al., 2009).

2.6 Reliability and predictability

Reliability is another functional attribute that is closely related to digital trust. Digital users' assessment of technological reliability is based on its accessibility when needed (Lippert, 2001). When digital users rely on technology to complete a task, it creates a situation of vulnerability for them (Mayer et al., 1995) due to their dependence on it to be functioning properly (Goodhue, 1998). This dependence also makes them vulnerable to technological downtime (Lippert, 2001); and the greater their reliance on technology, the greater the vulnerability they experience.

Digital users will therefore have higher trust of websites that meet their expectations, based on their experience and knowledge accumulated through using similar websites — a phenomenon described as situational normality by Gefen et al. (2003). Digital users who

perceive high situational normality in technology use believe it to be appropriate, well-ordered and favourable for conducting transactions (McKnight et al., 2002). Lippert (2001) describes this as predictability that is related to digital users' expectations of how consistently a technology performs based on their previous experiences and future expectations. It is seen as predictable if it performs in a consistent manner over time.

To develop general trust when interacting with new technology, users typically look for cues that demonstrate reliability and predictability (McKnight et al., 2002). Structural assurances, such as privacy and security features in a website, are major contributors to the development of trust in websites (Gefen et al., 2003). The presence of structural assurances can be signalled by seals of approval, privacy statements, guarantees, affiliations with other respectable web vendors, and clickable icons that allow digital users to contact web vendors. These features enable digital users to develop a sense of security towards the situation and contribute to the formation of trust (McKnight et al., 1998; Shapiro, 1987; Zucker, 1986).

All this is because digital users are most likely to rely on general feelings about the context in which they interact with an unknown vendor. Koehn (2003) argued that third-party guarantees can compensate for the absence of previous transactions with web vendors, particularly during initial encounters. Ongoing interactions are facilitated by the perception of fair play (Kumar, 1996), and structural assurances denote the presence of fair play in a transaction by relying on external guarantors of trust and through the absence of suspicious elements (Gefen et al., 2003).

High levels of structural assurance enable digital users to perceive web vendors as trustworthy and reliable, regardless of whether they are or not, while perceptions of low structural assurance become a barrier to trusting unfamiliar web vendors (McKnight et al., 2002). However, the effect of these features depends on digital users' digital literacy, their familiarity with them, and how much attention they pay to identifying these features (Jarvenpaa & Grazioli, 1999). When digital users gain experience in using technology, they also become increasingly confident in making predictions about how consistently a technology will function. Conversely, technology and websites with an unusual interface and processes or requests that are not commonly expected will fail to imbue digital users with a sense of trust (Gefen et al., 2003).

2.7 Information and content quality

Information quality refers to digital users' perception of the extent to which information related to transactions and products presented on websites is complete and free from errors (Kim et al., 2008). Digital users who perceive a website to present quality information are more likely to develop greater confidence that the web vendor is reliable and trustworthy (Kim et al., 2008). Information that is accurate, current and complete (Kim et al., 2005), that uses appropriate grammar, syntax and spelling, are more likely to be trusted by digital users (Koehn, 2003). However, online information varies greatly in terms of accuracy and reliability, and may also be intentionally misleading (Kim et al., 2008). In a survey by Business Insider Intelligence (2020), respondents indicated that platforms that displayed deceptive content were one of the top three factors that affected their trust.

High-quality information on a website provides digital users with the necessary materials to engage in online transactions in a controlled manner, which lowers their perception of risk and uncertainty (Kim et al., 2008). A study by Shelat and Egger (2002) found that a website's

information was the most important dimension in developing trust. They noted that digital users wanted to know about the web vendor, its staff and its policies. However, such information must be easily found on a website to be beneficial.

Researchers such as Wangpipatwong et al. (2005) and Gilbert et al. (2004) observed that information quality has a significant effect on digital users' decision to use e-government websites. Ayyash et al. (2013) noted that good information quality — such as information that is current, prompt, relevant, useful, free from errors and extensive — influences digital users' trust in e-government websites and motivates them to adopt the use of e-government websites. Lee and Levy (2014) found that the following three informational quality factors significantly contribute to the development of trust in e-government systems: accuracy or dependability, accessibility or completeness, and representativeness (see Table 3).

Table 3. Information quality factors that affect citizens' trust in e-government platforms

Information quality key factors	**Characteristics of information quality factors**
Accuracy or dependability	Availability of links Believability of information Reliability of information Information accuracy Validity of information Dynamic information Precision and recall of information Information provided is clear for the task
Accessibility or completeness	Robustness of information Continuous and repeated exchanges of information Amount of uptime of information Accessibility of information Credible source of information Information provides ease of operation Information is available in printable form Information relevancy Information is comprehensive Information is current Perceived value of information Type of language used is interpretable Security of information
Representativeness	Essentialness of information Efficiency of information Flexibility of information Information has added value

The next three dimensions of mechanical digital trust are only mentioned in the WEF Digital Trust Framework (2022) and short descriptions from the report have been reproduced below for completeness.

2.8 Interoperability

Interoperability is the ability of information systems to connect and exchange information for mutual use without undue burden or restriction (Soares & Amaral, 2014). In order for technology to coexist and interact with other technologies and data, a certain level of openness is required. This includes the use of open-source code and common data standards, although it may not be sufficient on its own to enable effective sharing and integration (Almeida et al., 2011). When the source code is publicly accessible, users can verify that the technology functions as intended and understand how their safeguards rely on other technologies and organisations. Even if the source code cannot be publicly disclosed, providing adequate assurances of security and reliability promotes interoperability between systems. This interoperability is not only a result of digital trust but also contributes to building trust among stakeholders (NIST, 2020).

Interoperability in technology standards can lead to broad economic growth and social good. The Singapore Quick Response Code (SGQR), for instance, is a single QR code that combines multiple e-payment solutions into one. It is intended to simplify QR e-payments in Singapore for both consumers and merchants (IMDA, 2017). This interoperable payment option that is now widely used in Singapore encourages consumers to adopt e-payment options because the SGRQ improves the simplicity and speed of e-payments. The interoperable payment option also benefits merchants in that they would only need to display a single SGQR label showing the e-payments it accepts, which means less clutter for them and quicker payments by consumers.

2.9 Fairness

Fairness requires organisations to strive for just and equitable outcomes for all stakeholders, considering the relevant circumstances and expectations (WEF, 2021). Achieving fairness involves balancing factors such as equity, equality and consistency, as fairness is ultimately a subjective decision. Demonstrating that the fairness of systems, products or processes has been assessed before deployment is therefore crucial for signalling trustworthiness to external stakeholders (WEF, 2022). Fairness can be demonstrated by being transparent about the assessments that went into evaluating data use and retention policies, and considering multiple personas to address fairness relative to different individuals or groups. In these processes, standardisation is crucial to enhance fairness by ensuring consistent decision-making processes aligned with ethical and responsible use norms (Microsoft, 2022). As such, organisations should justify and document their fairness-related decisions, especially when defining and implementing fairness within technology and data processing.

2.10 Redressability

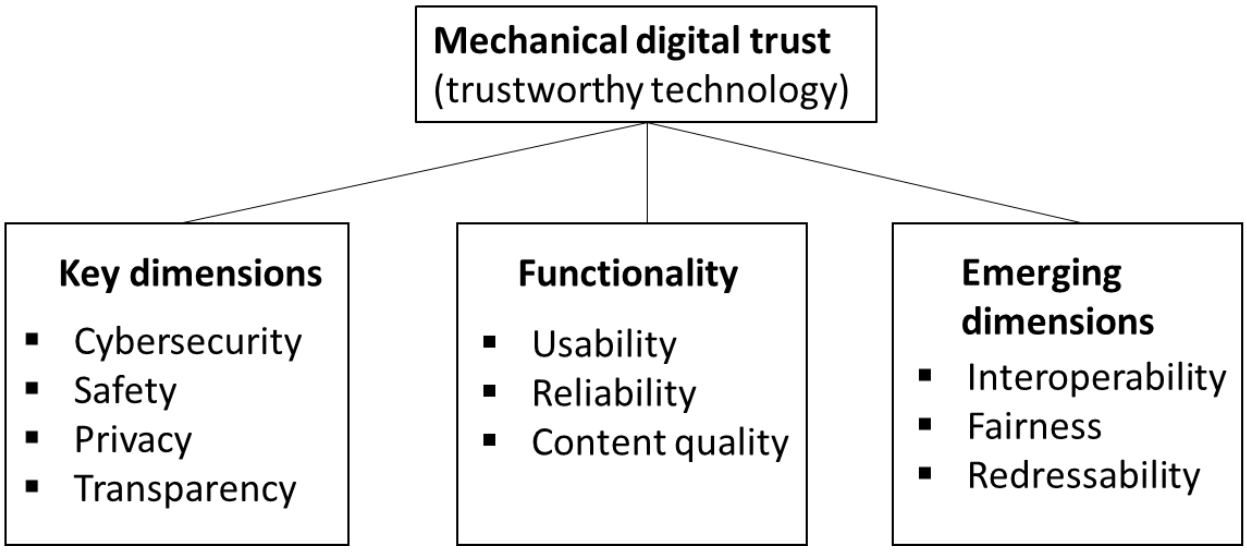
Redressability represents the possibility of obtaining recourse where individuals, groups or entities have been negatively affected by technological processes, systems or data uses (Shell & Buell, 2019). Even with state-of-the-art technology and the best deployment plans, unintentional technical errors and unforeseen circumstances are inevitable and should be

expected. When security breaches or significant periods of system downtime occur, the trustworthiness of a technology or an organisation is compromised. When these incidents occur in conjunction with a failure to provide adequate compensation or a reluctance to rectify the losses suffered by partners, customers or individuals affected, the erosion of trust becomes even more pronounced (WEF, 2022). For consumers and users, having a transparent and user-friendly means of seeking redress when there are lapses in security or reliability allows for the technology providers to assess and rectify any harm that may have transpired, thereby stemming further loss of digital trust.

The Online Safety (Miscellaneous Amendments) Act that was passed in Singapore in November 2022 contains elements of the redressability dimension. The legislation stipulates that social media services should have in place an accessible, effective and easy-to-use user reporting mechanism for online harms, and should also submit annual accountability reports on the effectiveness of their measures to combat harmful content. These reports will be made public for transparency and accountability, which are also the dimensions of mechanical digital trust that were discussed earlier.

We sum up the key dimensions of mechanical digital trust in Figure 5 below. Digital trust as it relates to trustworthy technology needs to be understood in terms of the core dimensions of security, safety, privacy and transparency or accountability. Digital trust is enhanced when the technology is perceived as easy-to-use and reliable, and delivers high-quality content. Emerging mechanical digital trust dimensions include interoperability, fairness and redressability, which technology companies should consider in the planning and development phases. In the next chapter, we discuss digital trust in the form of relational digital trust.

Figure 5. Key dimensions of mechanical digital trust (authors' compilation)



3 Digital Trust as Relational Trust

Relational trust in the offline world has been studied in various contexts by researchers from different disciplines, resulting in an array of definitions. Existing research suggests that environmental factors, experiences, attitudes and behaviours are all drivers of (relational) digital trust (Fletcher School, 2021).

Earlier work by Worchel (1979) identified three types of relational trust:

1. Trust as traits of groups and individuals
2. Trust as a product of human interactions
3. Trust as an institutional phenomenon or group norms

The first type of relational trust, developed by personality psychologists, focuses on individual differences in one's readiness to trust and how this readiness is affected by developmental and social contextual influences (Rotter, 1967). Trust is defined as a belief, expectancy or feeling rooted in an individual's personality and stemming from early psychological development. Business schools have also developed a similar definition of trust (Mayer et al., 1995) at this micro or individual level of analysis.

The second type of relational trust, developed by social psychologists, focuses on interpersonal transactions between individuals that either build or erode trust at both personal and group levels (Boon & Holmes, 1991; Deutsch, 1958). **Trust is defined as an expectation about another party's behaviour in a *transaction*, emphasising the development and maintenance of trust and how contextual factors might strengthen or constrain it.** Interpersonal trust can also be broadly categorised as limited trust and generalised trust. Limited trust pertains to trust between people familiar with one another, such as family, friends, and neighbours, while generalised trust involves trust between acquaintances and strangers (Putnam, 2000). Research also suggests an inverse relationship between limited trust and generalised trust (Ermisch & Gambetta, 2010).

The third type of relational trust, developed by sociologists and economists, focuses on the structural nature of trust (Fukuyama, 1995; Gambetta, 1988; Zucker, 1986). Trust is approached from a macro or societal perspective as an institutional phenomenon, with definitions frequently encompassing the following dimensions:

- Risk — trusting individuals cannot control or predict if trust will be broken, requiring them to take a risk.
- Positive expectation — trusting individuals anticipate that the trusted party will not behave detrimentally.
- Confidence — trust is built on confidence in the trusted party's integrity or competence.
- Dependence — trust requires one to depend on others' actions, as the interests of one party cannot be achieved without reliance upon another.

When trust is approached from this societal perspective, it relates to trust in social, political, legal and non-governmental institutions. This type of trust occurs when governments or institutions are appraised as promise-keeping, efficient, fair and honest (Blind, 2007). Institutional trust itself has two components: structural assurances and situational normality (which have also been discussed in the earlier chapter on mechanical digital trust):

> **Structural assurances** refer to an assessment of a transaction's success in a specific context due to safety nets like legal recourse, guarantees and regulations (McKnight et al., 1998; Shapiro, 1987; Zucker, 1986). Sociologists observed that trust between people is facilitated by institutional structures providing a safe and secure environment (McKnight et al., 2002).

> **Situational normality** refers to individuals' perception that a transaction will be successful based on the setting's conventionality (Baier, 1986; Lewis & Weigert, 1985). In such situations, individuals are assured that the situation is as it should be, and those around them share a common understanding of what is happening (McKnight et al., 1998; Zucker, 1986). Conversely**, trust erodes when circumstances appear abnormal.** In other words, **trust develops when interactions align with the norm and are therefore expected.**

The rest of the chapter focuses on the individual traits and the interpersonal interaction and norms that comprise the dimensions of relational digital trust.

3.1 Individual traits that affect relational digital trust

Existing literature on traditional trust suggests that factors such as personality, age, education level and level of income affect the development of trust and digital trust. The experts we consulted spoke extensively about these individual differences as they relate to relational digital trust:

> [Bill Dutton on why some people are more distrustful than others] "People who are least trusting of technology tend to be those who are the least experienced in technology and are also more marginal in society. That is, **they're not the mainstream in society** — so, retired people, the elderly, women versus men, minority groups and so forth, are more likely to be distrustful of the privacy issues."

> [Jonathan Obar on the varied experiences of digital users and how they affect digital trust] "I think it's very important in research like this to emphasise the differences in the experiences of individuals who are engaging with these technologies. **The research is clear that members of marginalised and vulnerable populations are most likely to be harmed by discriminatory AI and discriminatory data practices.** And within that evidence is individual experiences that are specific to individuals. So, it's hard to generalise and it's difficult for people to trust sort of across the board, because I think there are variations in experience."

3.1.1 Digital literacy and attitudes towards technology

The UNESCO Institute for Statistics and the Global Alliance to Monitor Learning provides the following definition of digital literacy:

> "Digital literacy is the ability to define, access, manage, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies and networked devices for participation in economic and social life. It includes competences that are variously referred to as computer literacy, ICT [information and communications technology] literacy, information literacy and media literacy." (Law et al., 2018, p. 6)

Digital literacy is perhaps the most consistent driver of digital trust mentioned by the experts we interviewed:

> [Jonathan Obar on the importance of digital literacy] "I think governments should be investing in digital literacy resources, opportunities, and things like that. I'm not sure

> what they call it in different parts of the world, but when children are young and they're learning in school about computers and the internet, learning about information protection, learning about information literacy — these things are very, very important and not just in schools. There should be programmes at libraries and places where individuals from different communities can have their needs met."

Several studies have argued that digital literacy can help digital users avoid negative experiences online which can result in a decrease in relational trust. For instance, Jones-Jang et al. (2021) found that digital users with greater information are more likely to identify and refute fake news online. Similarly, Graham and Triplett (2017) argued that digital literacy decreases the chance of digital users responding to phishing emails. They found that digital users with high levels of digital literacy have a higher likelihood of recognising such emails. They also have greater awareness of the existence of malicious actors online and that they may be potential targets of online crimes. Therefore, digital literacy can help digital users navigate the digital environment in a safer manner. Digital users who are more proficient in using the Internet are also more proficient in using the internet. They are more inclined to perceive lower risks in using it and are more likely to develop trust in when transacting online (Metzger, 2006).

However, the relationship between literacy and trust is complex and not always linear, and higher digital literacy does not always mean higher digital trust. Studies have shown that digital users with high levels of digital literacy encounter more online risks as compared with those with digital users with lower levels of digital literacy (Livingstone et al., 2017; Rodríguez-de-Dios et al., 2018; Cabello-Hutt et al., 2018), which can undermine digital trust (Dutton & Shepherd, 2006). Vissenberg et al. (2022) noted that digital users with lower levels of digital literacy generally spend less time online and are therefore more cautious.

Closely related to digital literacy are attitudes towards technology, which refer to people's receptivity towards it (Blank & Dutton, 2012). It affects their willingness to learn new aspects of technology and provides motivation to overcome challenges when doing so. Those with negative attitudes towards technology tend to be less trusting, while those who display positive attitudes towards technology are better able to overcome challenges when learning to use it. Higher digital literacy generally improves attitudes towards technology use.

For a more complete review of digital literacy, please refer to the IPS Working Paper No. 39 Towards A Unified Framework For Digital Literacy In Singapore.

3.1.2 Experiences in using technology

Digital literacy and attitudes are closely related to one's experience in using technology. Experience in using the internet is in turn associated with greater confidence in technology and higher levels of trust (Dutton & Shepherd, 2006). Repeated use of the internet leads to increased ease of use and comfort, which leads to greater trust and the ability to use technology in more sophisticated ways.

Research on e-commerce has shown that customers' level of experience in using the internet influences their likelihood of trusting technology (Corbitt et al., 2003). Similarly, Metzger (2006) found that customers' perceptions of risk in e-commerce can be attributed to their experience

with it, suggesting that frequent users of the internet are more likely to perceive lower risks and develop trust in online transactions.

However, early studies by Aiken (2006) suggest that digital trust increases only in the early stages of gaining experience, and that as digital users become more knowledgeable about the threats posed by the digital environment, they become more concerned with issues of privacy and security, and this may result in a decline in trust.

One particular experience of using technology was consistently discussed by the experts we interviewed — encounters with misinformation, disinformation and fake news.

> [Bill Dutton on how misinformation reduces digital trust] "The other is information trust. Do we trust the information we get online, and whether we're trapped in an echo chamber or filter bubble by algorithms on the internet. In other words, is AI sort of putting us in an echo chamber or filter bubble."

According to Wardle & Derakhshan (2017), the various types of problematic information can be categorised into three types of information disorder:

1. Misinformation — when false information is shared, but no harm is meant
2. Disinformation — when false information is knowingly shared to cause harm
3. Mal-information — when genuine information is shared to cause harm, often by moving private information into the public sphere

Cheng and Chen (2021) examined how misinformation on social media platforms influences digital users' attitudes towards it. Their findings indicate that encountering misinformation on Facebook influences digital users' trust in the platform. Their study suggested that trust in the platform was affected by the effect of misinformation elaboration. Wei et al. (2010) defined information elaboration as an individual's inclination to judge a message. Through the process of relating new information to one's existing knowledge, information elaboration causes a greater effect of the message on the individual. Accordingly, Cheng and Chen (2021) argued that misinformation elaboration results in digital users' perception that the effect of misinformation has a greater severity, causing them to have lower trust in the platform in which the misinformation was circulated.

For a more complete review of misinformation, please refer to the IPS Study on Singaporeans Susceptibility to False Information.

However, it was observed that self-efficacy, which is defined as an individual's belief in their capacity to execute the relevant actions to produce specific effects (Bandura et al., 1999), is positively related to trust. In other words, digital users who have greater confidence in identifying misinformation by themselves were more likely to develop trust in the social media platform. Such digital users also become more experienced and comfortable with online information on social media platforms, and therefore, are more likely to trust in the platform.

Blank and Dutton (2012) also argued that experienced digital users would have developed skills to handle negative experiences, and concerns with privacy and security do not always undermine digital trust.

> [Bill Dutton on developing a learned level of trust] “Obviously, an experience of technology is not always good. Therefore, the trick is to enable people to get experience so they have a learned level of trust, but also ensure that they have a positive experience, that is, to avoid bad experiences, which means skills and training and awareness of the kinds of risk that they can confront…. Somebody telling you that this is safe is not going to be as important as you experiencing it.”

Taken together, these findings suggest that while digital users are exposed to negative experiences online, digital literacy can equip digital users with the skills to mitigate online risks. Even as organisations and governments work to enhance mechanical digital trust along the dimensions discussed in the preceding chapter, digital trust may not increase unless these individual traits of digital literacy, attitudes and experiences improve over time.

3.1.3 Propensity to trust

The propensity to trust or dispositional trust is defined as “the general willingness to trust others” (Mayer et al., 1995, p. 715). It is a stable characteristic that results in one’s generalised expectation that others can be trusted (Costa et al., 2009) and varies across individuals (Gefen, 2000). When entering a trust relationship, people do so with a certain degree of trust (Mayer et al., 1995). Those with dispositional trust either believe that others generally mean well, or they believe that trusting others will result in better interpersonal outcomes (McKnight & Chervany, 2001).

In the digital environment, studies on e-commerce suggest that some digital users display a greater propensity to trust and are more trusting towards web vendors despite having limited knowledge, while others require more information to develop trust (Salam et al., 2005). However, dispositional trust plays an important role only in the early stages of a trust relationship (Mayer et al., 1995). As trusting parties interact more with each other, dispositional trust loses its influence as the nature of the interaction becomes more important (Zahedi & Song, 2008).

Experience and socialisation can affect an individual’s propensity to trust (Rotter, 1967) and are therefore expected to vary across cultures (Gefen, 2000). As a result, different cultures are likely to vary in terms of degrees of trust and the rate of adoption of technology. Tan and Tambyah (2011) found that Singaporeans had a low propensity to trust when compared with other Asian countries such as South Korea and Taiwan, especially among those who were less educated and earned a lower income. This suggests that for digital users in Singapore to develop digital trust, they may require on average a higher level of digital literacy and more positive experiences with technology.

The next three demographic traits of age, income and education have been found to affect traditional trust in the offline context. In our review, we have not found studies that discuss the direct relationship between these demographic factors and relational digital trust that are independent of other factors such as digital literacy and experiences in using technology. To motivate future research, we have included the discussions around why age, income and education affect the formation of traditional relational trust in the offline context — and identify this as a research gap in the current literature on digital relational trust.

3.1.4 Age

Previous studies have shown that trust in others increases with age (Alesina & La Ferrara, 2002). Older adults tend to prefer familiar partners who can help them attain emotionally meaningful goals rather than novel partners (Fredrickson & Carstensen, 1990). They also tend to have higher levels of social connectedness by focusing on close social partners, resulting in a social environment that is more trustworthy (Lang & Carstensen, 2002). In comparison to younger individuals, older adults are more motivated to strengthen and maintain their social relationships. Furthermore, they are more adept at maintaining their relationships due to their greater tendency to forgive when interpersonal conflict occurs, further contributing to higher levels of trust (Allemand, 2008).

3.1.5 Income

Similarly, individuals with higher income levels are found to have higher levels of trust (Alesina & La Ferrara, 2002; Putnam, 2000). Those with higher socio-economic status are more likely to be treated with dignity while those with a lower socio-economic background are more likely to experience discrimination and social exclusion (Putnam, 2000). Therefore, individuals with higher income levels perceive their environment as more friendly and less hostile (Gallo et al., 2006).

3.1.6 Education

Education is also positively correlated with trust (Alesina & La Ferrara, 2002) for various reasons. For instance, education allows people to make informed decisions (Keefer & Knack, 2005). Other studies also suggest that people perceive better educated people to be more trustworthy and therefore are more likely to trust them (Putnam & Helliwell, 2007). Furthermore, those who are better educated develop a better understanding of how the government functions, which furthers trust in institutions (Christensen & Lægreid, 2005).

3.2 Interpersonal factors that affect digital relational trust

The preceding section discussed individual traits that affect digital relational trust. Another important aspect of relational digital trust is the trust *between* people in the digital environment, given the density and frequency of online interaction between digital users today. This is evident from the global popularity of online social networks (OSNs), which are considered the most popular sites on the internet due to the massive numbers of digital users who participate in these platforms. Popular OSN such as Facebook, for example, have almost 2 billion daily active users (Meta, 2022). Locally, the IMDA (2019a) reported that the top primary internet activity that users in Singapore engaged in was related to communications (see Table 4).

OSNs provide a platform for digital users to maintain social relationships, connect with other users who share similar interests, and consume content and knowledge provided or verified by other users (Mislove et al., 2007). However, Insider Intelligence reported that trust in social media platforms have declined significantly, particularly in areas pertaining to privacy and security (Williamson, 2022). As OSNs becoming increasingly embedded in the lives of digital users, these risks are becoming more complicated and occur more frequently, resulting in a loss of trust between people in the digital sphere. It is therefore critical to understand the drivers of trust in digital relationships and interactions.

Table 4. Primary internet activity groups of internet users, 2017–2019 (IMDA, 2019)

Primary Internet Activity Group	Residents aged 7 and above		
	2017	2018	2019
Communication	94%	95%	96%
Leisure Activities	90%	91%	92%
Getting Information	84%	85%	85%
Purchasing or ordering goods or services	55%	60%	66%
Online Banking	59%	60%	62%
Dealing with government organisations / public authorities	44%	45%	46%
Education or learning activities	24%	26%	27%
Creating Content	26%	26%	24%

Base: Internet users aged 7 and above who had used the internet in the past 3 months

3.2.1 Strength of ties in digital networks relationships

Granovetter (1992) argued that being embedded in a network contributes to the emergence of trust. The notion of embeddedness refers to the impact of social networks on the behaviour of its members (Granovetter, 1992). The network structure contributes to the sharing of information regarding one's reputation, as well as the socialisation of common behaviours. Consequently, those who choose to misbehave in an environment where others act in an ethical manner will experience feelings of guilt (Ganzaroli, 2002).

The strength of ties between OSN participants has implications for the emergence of trust. Strong ties refer to intimate relationships, such as those with immediate family and close friends, and are often multi-stranded and frequently maintained (Ferlander, 2007). Thick interpersonal trusts are embedded in these relationships with strong ties (Putnam, 2000). Coleman (1988, 1990) argued that the value of social capital lies in the individual and collective actions that result from closed networks of personal relations. As members of the social network are familiar and often interact with one another, norms of exchange are more likely to be enforced, as well as the overseeing and imposition of sanctions. An individual who is well-embedded in a social network will thus be seen as trustworthy because frequent interactions increase familiarity, facilitate common understanding, and increase information sharing (Tsai & Ghoshal, 1998).

On the other hand, weak ties refer to non-intimate relationships, such as those with acquaintances, and are often single-stranded and maintained infrequently (Ferlander, 2007). OSNs serve as a platform for digital users to interact with strangers with whom they share weak ties. For instance, Twitter enables the sharing of information with a wide network of followers and also allows for that sharing to go beyond one's social network. Weak ties are associated with "thin" interpersonal trust (Putnam, 2000), which is riskier than "thick" trust, because "thin" interpersonal trust develops in relationships where true motives are unknown (Luhmann, 1988).

Network ties between digital users can range from strong to weak, given that OSNs provide opportunities to connect people from various social circles that range from close family and friends to complete strangers (Brandtzæg et al., 2010). Trust can be developed through well-known and reliable intermediaries who can provide information about the trusted party and affirm that they can be trusted, as well as through institutional trust (Khodyakov, 2007). This means that people can trust a stranger because an intermediary trusts the latter (Putnam et al., 1993). Burt (1992) observed that when two friends share a mutual friend, it results in greater trust between the two.

Additionally, research suggests that high levels of trust in localised domains of family, neighbours, voluntary associations, etc., create greater generalised trust in others (Freitag & TraunmÜLler, 2009; Glanville & Paxton, 2007). Trust can spread from trustworthy interactions to interactions with strangers in communities characterised by dense interactions (Macy & Skvoretz, 1998).

> [Tammy Lin on the effect of source of information on digital trust] “If the information source is public figures or celebrities, or politicians, we know this is a purposefully crafted message; it's not that natural. I do think the social status of the sender will also be a moderator that influences the trust towards these messages. We know if it is from a politician, we know they have a hidden agenda. But if it’s just your friend talking about it, you probably would trust your friends. So, the source, their social tie, with the strong tie, weak ties or their public ties, it definitely influences your trust towards the messages or the content or the purpose.”

3.2.2 Perceived similarity and homophily

There is also evidence to suggest that people are more inclined to trust and develop closer relationships with those who are similar to them (McPherson et al., 2001). Similar characteristics could include interests, experiences and demographics, among others. Higher levels of similarity are associated with greater shared understanding between individuals (Luo, 2002). Walczuch and Lundgren (2004) found that those with higher levels of perceived similarity are more likely to be attracted to each other. They suggested that people tend to be more affected by those who share similar norms and values rather those who have dissimilar ones, which results in the creation of close relationships and trust.

Research by Ziegler and Golbeck (2007) demonstrates how this translates to the digital environment. In their study, using empirical data from a social network that integrates movie ratings and social connections, digital users can rate how much they trust other digital users’ opinions of movies. The researchers found that those with similar profiles developed greater levels of trust than those with less similar profiles. When trust between digital users increased, the difference in ratings they assign to movies decreased. Furthermore, digital users were found to be more similar to those they trusted than to arbitrary digital users. This association between perceived similarity and trust is the basis of the recommendation algorithms used by many e-commerce and digital platforms.

3.2.3 Shared community values

Sitkin and Roth (1993) argued that trusting relationships are rooted in having shared values. Shared values imply that individuals hold similar beliefs about appropriate behaviours, goals

and policies, as well as those that are inappropriate, irrelevant or flawed (Morgan & Hunt, 1994). When a community shares a common vision and values, members can trust one another to work towards collective goals instead of solely pursuing individual interests. In such a community, there is little need for trust to be verified when interacting with others since trust is at a depersonalised level (Tsai & Ghoshal, 1998). Wu et al. (2010) found that a sense of shared values among members of a virtual community influenced levels of trust. They argued that members with similar values trusted one another more, and as they developed common values and goals, this trust grew even more. Walther and Bunz (2005) investigated how trust developed in virtual groups and observed that when group members followed prescribed rules and norms, it decreased uncertainty and strengthened trust among group members.

3.2.4 Increased trust from repeated interactions

According to Rotter (1971), repeated interactions over time allow individuals to gather more information about others to form a generalised expectation that others' behaviours are predictable and trustworthy. It allows people to develop a better understanding of what, why and when others behave the way they do, which results in the creation of a framework to predict future behaviours and increase trust (Gefen, 2002).

Gefen (2000) argued that this predictability results in decreased uncertainty between individuals in the digital environment. When digital users interact frequently, they know one another better and can better predict how others will behave in various situations, leading to higher levels of trust. Frequent interactions that occur within dense networks that comprise of family, friends and community members, allow people to develop an understanding that others can be depended on to fulfil their duties (Welch et al., 2007). These interactions, which are grounded by social norms (Putnam, 2000), enable people to perceive those around them as predictable, resulting in higher levels of trust (Zucker, 1986). Additionally, repeated interactions provide opportunities for digital users to become familiar with one another, which contribute to greater trust (Ren et al., 2007; Coleman, 1990).

Other researchers have suggested that extensive previous interactions between trusting parties create opportunities for trust to develop, because these allow them to develop greater familiarity with one another, enabling trusting parties to develop confidence in their decision to trust the other (Chu & Dyer, 2000). As repeated interactions occur over a period of time, the nature of their interaction gradually evolves from being less risky to more risky (Blau, 1964). Situations of escalating risks allow for an affirmation of trust between the parties involved, causing them to trust one another even more.

Finally, the satisfaction that people derive from repeated interactions also matters. Ramaseshan et al. (2006) argued that satisfaction during initial interactions between people contributes to the creation of trust and sustained relationships. In the digital context, research suggests that digital users of a virtual community who have pleasant interactions will develop greater trust in with one another, as well as develop lasting social relationships (Wu et al., 2010). Studies on e-commerce have also found that people with positive experiences in shopping online develop greater trust in online sellers (Walczuch & Lundgren, 2004).

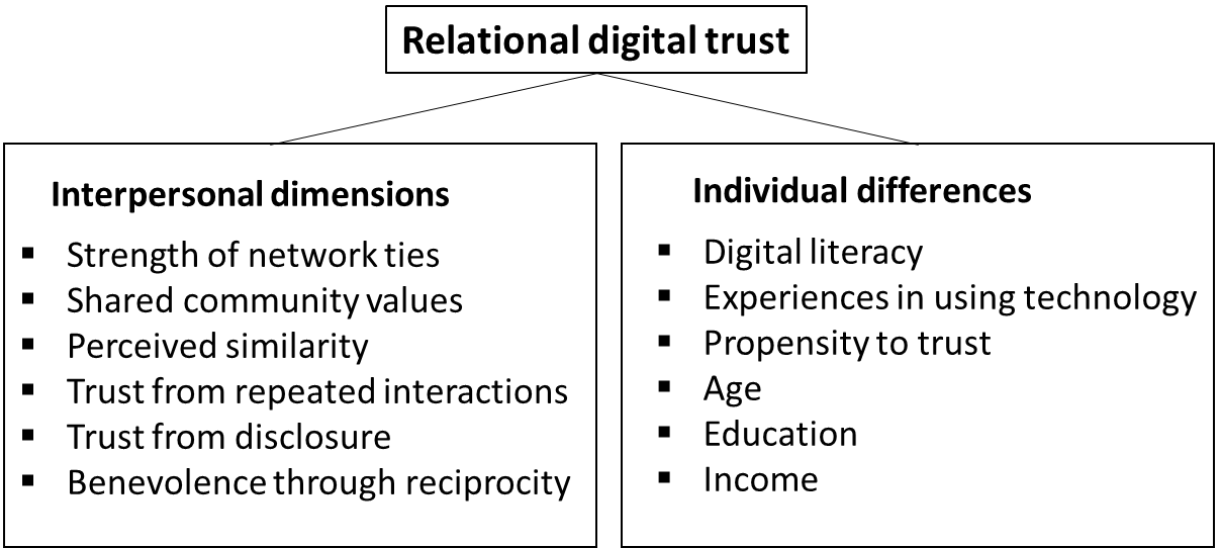
3.2.5 Benevolence demonstrated through responsiveness

Research suggests that reciprocity in exchange relationships leads to the development of trust (Kramer, 1999). In their study of virtual communities, Ridings and colleagues (2002) found that frequent and prompt replies to messages result in higher levels of trust among members in the community. They argued that trust cannot develop in a situation where an individual shares information online and does not receive any response. On the other hand, when others provide a prompt response, it is an indication that they were able to supply accurate and useful information, which increases the belief in their abilities.

Additionally, higher levels of responsiveness suggest that digital users display benevolence, or at least a willingness to help others, which implies integrity through behaving in a way that is in accordance with social norms. For instance, a study done by Wang (2017) revealed that reciprocity in social networks builds trust and is especially important in situations where people are unfamiliar with each other as this is a means of getting to know another person without direct interaction. Thus, supportive responses to other digital users indicates one's integrity and benevolence, which contributes to the emergence of trust.

As with the dimensions of mechanical digital trust, we summarised the dimensions of relational digital trust in Figure 6 below. These dimensions highlight the human element of digital trust that are negotiated between users and within digital communities. They underscore the main premise of this policy review that digital trust is both about trustworthy technologies and trust between people in the online sphere.

Figure 6. Dimensions of relational digital trust (authors' compilation)

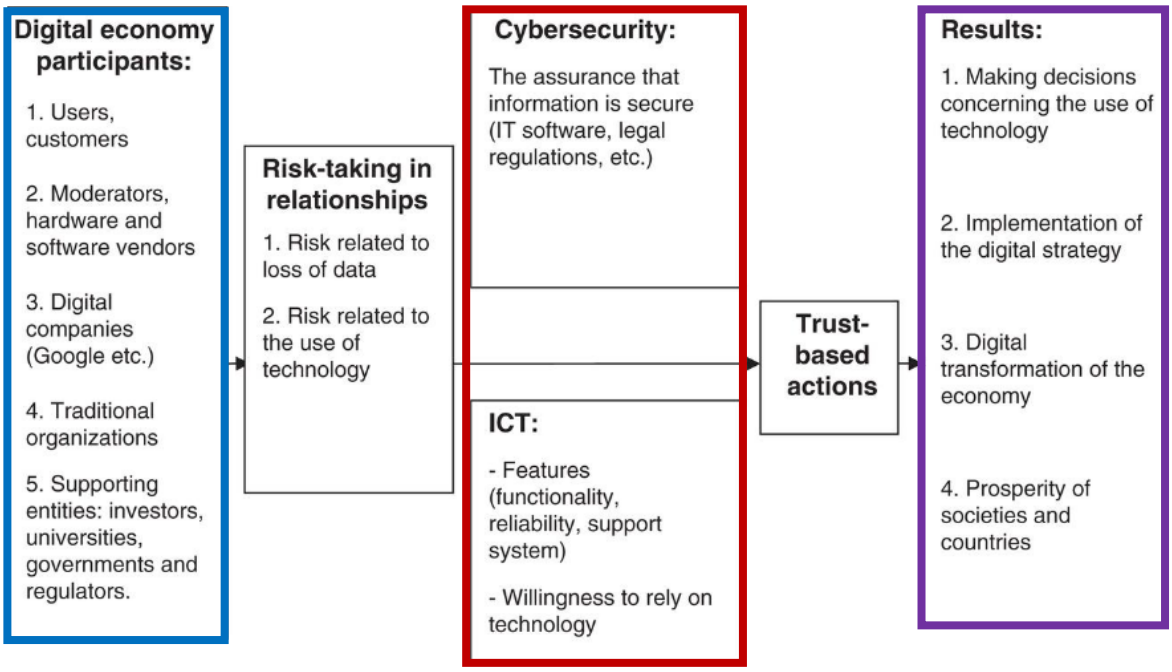


4 Digital Trust Ecosystem

In recent years, scholars have attempted to integrate the two approaches of mechanical and relational digital trust in conceptual models. For instance, Jasiulewicz et al. (2021) presented an integrative conceptual model of trust in the digital economy that identifies five types of participants involved in digital interactions, each with different expectations and challenges

(Figure 7, see box with blue outline). These participants include traditional organisations, users, facilitators, purely digital companies, and supporting entities and are the actors in the dimensions of relationship digital trust described in Chapter 3.

Figure 7. A conceptual model of trust in the digital economy (Jasiulewicz, Pietrzak, and Wyrzykowska, 2021)[6]



The authors explained that it is necessary to guarantee data protection (i.e., cybersecurity) and ensure that other features such as functionality and reliability are in place while noting that no solution can guarantee full cybersecurity, and it remains a joint challenge requiring technical and legal verification based on a common set of standards. These factors are dimensions of mechanical digital trust listed in Chapter 2 (see box with red outline in Figure 7).

Digital trust in the model contributes to several outcomes, such as making decisions on the use of ICT technologies, implementing digital strategies, transforming the economy, and contributing to the wealth of societies and countries (see box with purple outline in Figure 7).

The interplay between dimensions of mechanical trust and relational digital trust can be understood as follows: traditional organisations place a high value on the reputation of their digital operations and processes, while individual consumers are primarily concerned about the privacy of their digital activities. Technology moderators have a significant influence on shaping the reputation and level of risk for both organisations and customers. In the case of digital companies, security should be a vital social responsibility to mitigate risks for users. Regulatory bodies and other supporting entities play a role in overseeing and coordinating efforts to shape customer opinions and build trust in the digital realm.

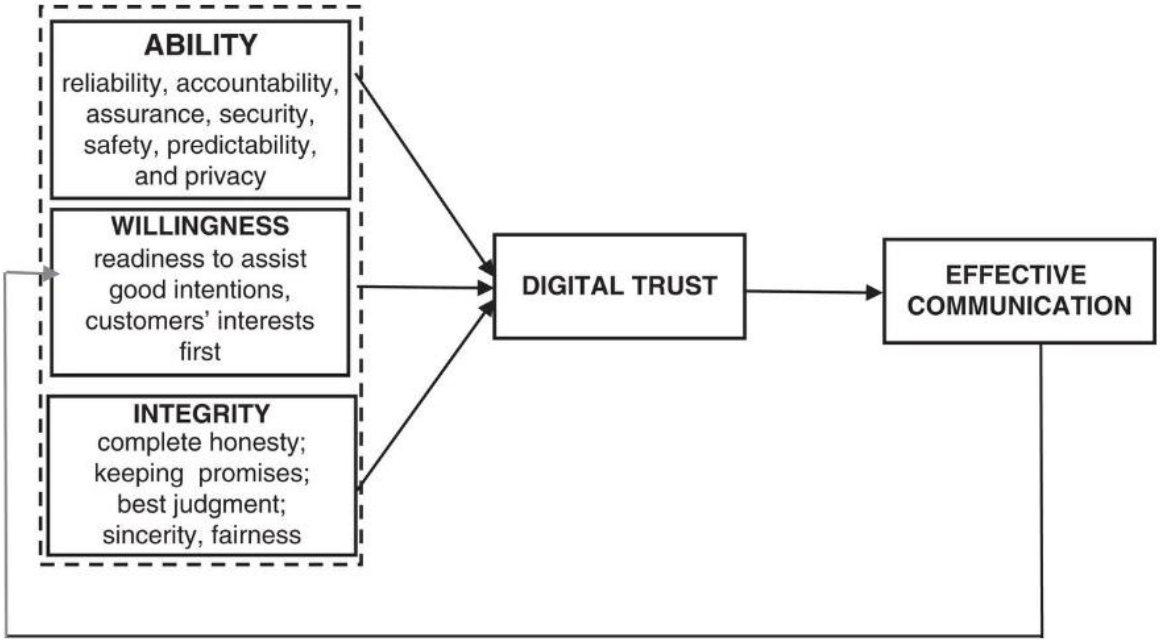
Ensuring trust in the digital economy is crucial for instilling confidence in human interactions with technology, especially considering the potential for unexpected and negative

[6] Outlines in blue, red and purple are authors' additions.

consequences associated with its use. Furthermore, the trust established online facilitates smoother interactions in the real world (Jasiulewicz et al., 2021).

On the other hand, Kożuch (2021) proposed her model of digital trust based on the factors of perceived trustworthiness in the classical Mayer et al. model of trust (Mayer et al., 1995). Kożuch's model (see Figure 8) consists of a set of capabilities that enable individuals, groups, or organisations to build and use advanced digital devices, systems and procedures effectively. Her proposed model does not consider the interdependence of trust with risk-taking and producing good performance. Instead, it focuses on creating a sense of digital perceived trustworthiness through the set of three dimensions.

Figure 8. Simplified model of digital perceived trustworthiness (Kożuch, 2021)



The first dimension of the Kożuch model is effectiveness or ability, which includes reliability, accountability, assurance, security, safety, predictability and privacy. These components are similar to the dimensions of mechanical digital trust discussed in Chapter 2. These are gained through personal or organisational competencies such as transparency, confidence in co-workers and clients following through on agreed-upon actions, and treating confidential information appropriately (United Nations, n.d.)

The second dimension, that is benevolence or willingness, includes the positive orientation perceived by the online user reflected in attitudes such as readiness and motivation to assist, demonstration of good intentions, and putting customers' interests first (Gefen, 2000, p. 42). Additionally, cultural competencies such as awareness of cultural differences, understanding other cultures, and engaging and integrating cultural differences, create benevolence as a dimension of digital trust.

The third dimension of digital trust is integrity, which refers to the adherence to sound moral and ethical principles (Colquitt et al., 2007). This dimension is associated with loyalty, openness, caring and supportiveness as described by Mayer et al. (1995). Ethical behaviour related to digital interactions, such as signalling complete honesty, keeping promises, offering

best judgement, and being sincere and fair, contributes to the creation of this dimension of trust (Gefen, 2000, p. 42). The latter two dimensions in the Kożuch model correspond to the dimensions of relational digital trust discussed in Chapter 3. In the Kożuch model, the outcome of digital trust is effective communication.

We posit the outcomes of digital trust efforts should be that the harms of digital technologies are minimised and the benefits are available to all in society. This will set up a virtuous cycle between digital trust and appropriate technology use.

5 Interrelation Between Offline and Digital Trust in Government

This report being a policy review on digital trust, we turn to the trust ecosystem in the case of e-government to explicate the interaction between mechanical and relational digital trust in the public policy domain.

The adoption of ICT by public authorities to provide public services and information (e-government) has provided an opportunity to foster stronger connections with citizens that have become increasingly critical and demanding in recent decades (Porumbescu, 2016). A commonly cited definition of e-government is “the electronic provision of information and services by government 24 hours per day, seven days per week” (Norris & Moon, 2005, p. 64). West (2004) noted that because “[i]nternet delivery systems are non-hierarchical, nonlinear, two-way, and available 24 hours a day, seven days a week,” e-government is characterised by round-the-clock access to public information and two-way interaction between citizens and bureaucrats.

E-government was initially used by public authorities to disseminate information about services (e.g., opening hours and contact details). In recent years, the use of e-government platforms and initiatives is expanding as ICT becomes more sophisticated and accessible (Porumbescu, 2016) and is now used sophisticatedly to offer services directly to citizens (Öksüz et al., 2016).

5.1 Dimensions of mechanical digital trust in e-government

The dimensions of mechanical digital trust — privacy, security and transparency — naturally apply to e-government. A study conducted by IPSOS in 2022 found that the top three government policies that increase trust in the internet are: protection of internet user privacy (65 per cent); provision of cybersecurity to internet users (65 per cent); and setting standards for how companies make use of user data (64 per cent) (see Figure 9). The CISCO 2022 Privacy Survey also found that more than half of respondents reported that government should play a primary role in protecting personal data, as compared to 19 per cent who said that such responsibility should be delegated to individual users.

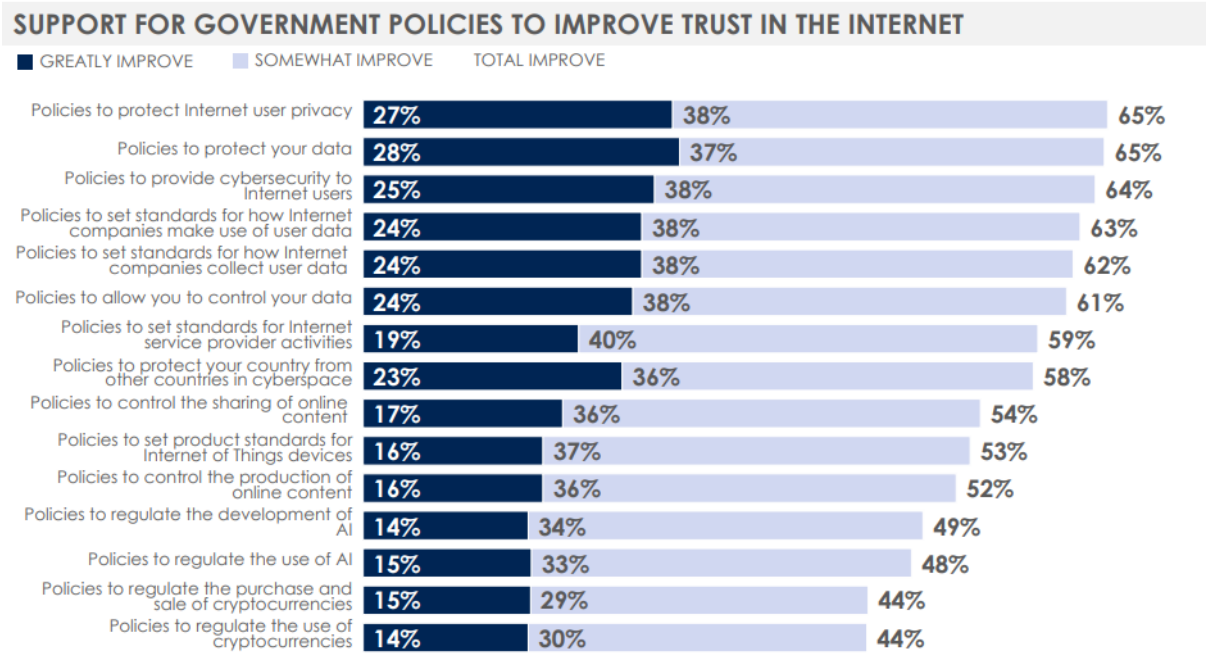
5.1.1 Privacy and security in e-government

The government’s ability to securely store and handle digital users’ personal data is key to motivate digital users to adopt e-government services (Colesca, 2009). Given that digital users are required to submit personal data in e-government websites, when they perceive e-government websites to have low levels of security, they are less likely to utilise e-government services (Kumar et al., 2018). It follows that governments must provide technology

infrastructures that are robust and secure to assure digital users that e-government is safe and secure for them.

Indeed, findings from a study by Ayyash et al. (2013) suggest that privacy and security are the strongest determinants of trust in e-government. Digital users must be assured that e-government websites refrain from sharing their personal data, protect their credit information and personal data, secure transactional information, and have the ability to address threats to the security of the information that has been provided (Ayyash et al., 2013).

Figure 9. Support for government policies to improve trust in the internet (IPSOS, 2022)



Bélanger and Carter (2008) further suggested that government adopt the use of security seals to signal that e-government platforms have high levels of security and communicate to citizens the measures that have been taken to ensure the security of e-government platforms. Such messaging should be provided clearly using plain language and should be posted both online as well as in the offices of government agencies or documents that are mailed to citizens.

Interestingly, while consumers often agree to provide personal information on the internet in exchange for improved service, convenience or incentives, the collection of data by governments is typically seen as an infringement of privacy (Belanger et al., 2002).

> [Gregory Porumbescu on the specific and generalised trust in government] “Trust in government is not equal to trust in data security…. Just because the Singaporean citizens or residents of Singapore trust the government with their data, doesn't necessarily translate into trust in other performance domains or at a more generalised level.”

5.1.2 Transparency in governance through e-government

Digital users who assess e-government as transparent not only display greater levels of trust in government but are also more likely to use it repeatedly and recommend it to others (Sternstein, 2010). The use of social media, in particular, provides digital users with easier access to government information about current events, policies or programmes, which increases their perception of transparency in government (Song & Lee, 2016).

Kim and Lee (2012) observed that e-government services that are user-friendly contribute to the perception of government transparency, which had a positive effect on digital users' trust in government. Mansoor (2021) found governments that provide quality information are perceived to be responsive which increases trust in government.

> [Gregory Porumbescu on the public's greater access to government information] "I think, no matter where you stand in terms of discussions on how transparent government is, one thing that everyone can agree on is that, for the most part, governments today are disseminating more information to more people than at any other time in history. Whether that information contributes to transparency or not is up for debate. But definitely, the public today has access to a lot more information about government."

Transparency through e-government may also work to enhance relational digital trust as the interactions enable digital users to feel a sense of connectedness with the government, which increases their perception of the government as trustworthy. Additionally, digital users who are connected to government through social media play a critical role in bridging the government to other digital users who do not use e-government. The citizens who do not use e-government can learn about the services through other digital users in their networks as interactions between digital users on social media are visible to anyone who joins the platform (Song & Lee, 2016).

However, one of the experts we interviewed was less sanguine about the link between transparency and trust:

> [Gregory Porumbescu on the effect of transparency on trust in government] "Trust comes on foot and leaves on horseback. So, it takes a very long time to build trust, but it's very easy to lose trust. So, what I'm saying here, then, is that transparency may, over the span of several years, build or contribute towards trust. But in the time frames that we're using to assess this… a couple of years, three or four years at maximum, I haven't seen any convincing studies using longitudinal data claiming an impact of trust. So, in the timeframes we're looking at, I don't think we have strong evidence that transparency actually increases trust in government."

> [Gregory Porumbescu on the unequal effect of e-government on trust in government] "People are not going to use the information in an even-handed way. They're going to use this information in ways that align with existing biases to confirm those existing biases, thus bolstering trust in some but leading to a deterioration of trust in other groups."

5.1.3 Functional attributes that drive trust in e-government

The functional attributes that drive trust between users and web entities such as ease of use and quality discussed earlier also apply to e-government services and trust towards the government. For instance, e-government websites that are perceived to have greater ease of use result in greater levels of trust among digital users (Ayyash et al., 2013). Digital users who find e-government websites user-friendly will have a greater urge to use it (Ayyash et al., 2013).

Digital users are also more likely to adopt e-government services that can be easily accessed (Al-Faries et al., 2013). Conversely, e-government websites that are perceived to be complex deter digital users from using them (Lean et al., 2009). The accessibility of e-government services has been found to increase trust in government as it enables digital users to better evaluate the government's behaviours, policies and programmes (Mensah et al., 2021). This will in turn affect citizens' decision to trust or not trust in government.

5.2 Dimensions of relational digital trust in e-government

Many of individual traits and interpersonal dimensions that influence relational digital trust also apply in the e-government context.

5.2.1 Trust in technology

The primary factor in developing trusting relationships through the internet is the technology itself. As such, citizens' adoption of online services is reliant on their confidence in the internet as a reliable medium that can provide secure transactions and accurate information (Sawhney & Zabin, 2002). Trust in technology has been identified as a significant motivator or inhibitor of e-government service use in several studies (Srivastava & Teo, 2009).

Concerns about privacy threats and misuse of data also come into play in the adoption of e-government services (Kumar et al., 2018). In a study done by Colesca (2009), privacy concerns were found to have the greatest influence on trust in e-government. The author observed that digital users prefer to disclose personal data when they are confident that the data will be used according to how they had intended. Similar to e-commerce, digital users' level of confidence in online privacy statements influences their trust in how governments use and handle personal data (Beldad et al., 2012).

5.2.2 Digital literacy and experience

Studies on trust in e-government have also found linkages to the impact of digital users' experience in using technology. Horsburgh et al. (2011) observed that digital users who are experienced in using the internet experience greater levels of trust in e-government services, given that familiarity in using the internet imbues digital users with a sense of confidence in navigating e-government websites. Similarly, Colesca (2009) found that digital users with higher usage of the Internet have greater understanding of how technology is used for the dissemination of information, online transaction, and communication. Therefore, internet experience results in greater trust in e-government websites.

5.2.3 Propensity to trust

Digital users with greater propensity to trust also tend to display greater levels of trust in e-government (Bélanger & Carter, 2008; Colesca, 2009). Bélanger and Carter (2008) suggested that while an individual's propensity to trust cannot be influenced by the government, governments should be cognisant of this and its implications for trust in government and trust in technology itself. More effort should be directed towards digital users with a lower propensity to trust, in order to incentivise them to try e-government services. When digital users have successful encounters with e-government services, they will begin to develop trust in government and trust in technology, which may result in their willingness to adopt e-government services (Bélanger & Carter, 2008).

Parent et al. (2005) observed it is more likely for digital users who have high pre-existing levels of trust in government to develop greater trust in government through their experience in using e-government services. The research suggests that e-government heightens existing levels of trust in government but does not have any effect on digital users who have feelings of distrust or are neutral towards the government.

> [Gregory Porumbescu on building digital trust through targeting] "Finding people who are relatively uninformed, targeting those individuals is going to be more effective at building trust, whereas people who tend to be more plugged in and more informed, better informed, have relatively well-established beliefs."

5.3 Bi-directional nature of trust and digital trust in e-government

The report thus far has attempted to describe the different dimensions pertaining to mechanical and relational digital trust in the context of e-government. However, these dimensions are not exclusively causes or outcomes of trust in e-government. Trust can be simultaneously a cause and an effect, and it is this bi-directional causality that makes the concept complex. In the context of e-government, the adoption of e-government services first requires trust in government (i.e., trust as cause); once adopted, it also reinforces digital users' trust in e-government services (i.e., trust as effect) by allowing digital users to be more aware of government policies (Srivastava & Teo, 2009). The rest of this chapter attempts to articulate the complexities and inter-relatedness of the trust ecosystem of e-government.

5.3.1 Genesis of trust in e-government

Not every citizen can rely on past experiences in using e-government websites to assess the trustworthiness of these websites. Therefore, such citizens have to rely on other criteria in deciding whether to trust e-government websites. Studies done in the e-government context indicate that trust in government is influenced by the government's reputation. For instance, Beldad et al. (2012) found that citizens assess the reputation of governmental organisations when deciding whether they should trust them. Governmental organisations that are regarded as having a positive reputation are more likely to be trusted by citizens. Other research has found that digital users' trust in a government's competency and efficacy translated into interest in utilising e-government services or trust in these services (Al Mansoori et al., 2018; Srivastava & Teo, 2009).

The first contact that users have with e-government is often with information about services. Studies have found that useful information and beneficial services found on e-government websites can contribute to the development of trust in government (AlAwadhi, 2021).

> [Gregory Porumbescu on disseminating information as a trust building mechanism] "Disseminating information on government responsiveness, how the government is responding to the needs of the public, that is a trust building exercise. We can think about spam and scamming…. If you or I open these emails and we get caught, we blame ourselves or we blame the scammers, but I think it's when people are looking for the government to help them…. In general, communicating the benefits of public policy, or how these public policies are being implemented to respond to problems and needs is probably, in my view, the most effective way of building trust."

> [Gregory Porumbescu on how communicating state benefits can build trust] "You have people who don't understand all the policies that they're benefiting from, and in turn they become very sceptical and very cynical towards government, just because they don't realise how much the government is benefiting their everyday lives. So, making an effort to communicate this information, to surface the submerged state, so to speak, I think, also will show benefits in terms of trust."

5.3.2 Interaction with e-government

Engagement with e-government services can be in the form of one-way or two-way communications. Welch et al. (2005) observed that digital users who use one-way communication when seeking information from the government experience less satisfaction when using e-government services. On the other hand, governments that provide two-way communication on social media sites allow digital users to connect directly with the government, which increases digital users' perceptions of government responsiveness, thereby increasing trust in government (Mansoor, 2021). Likewise, Chakiri et al. (2020) argued that digital users' ability to comment and share information provided by the government via social media sites demonstrates government responsiveness and increases trust.

In the current milieu, digital users' satisfaction in using e-government is inexplicably related to interactivity, which is defined as "a measure of the level of convenience or degree of immediate feedback" (La Porte et al., 2002, p. 417). Consequently, the government's disregard for digital users' desire for electronic interactivity, transparency and transactions has negative implications for digital users' trust in government.

Specifically, higher frequency of use of social media engagement with government contributes to greater levels of satisfaction and trust in government. The use of social media in government results in greater trust in government when compared to the use of e-government websites (Porumbescu, 2016). Social media in e-government allows digital users to be more involved with the government through easy access to up-to-date and relevant information which contributes to trust in government (Al-Aufi et al., 2017).

Interestingly, the **frequency of use** of e-government websites was found to have an insignificant or a negative impact on digital users' satisfaction levels and trust in government (Porumbescu, 2016). This is because digital users were more responsive to e-government services that provided less detailed information, such as social media accounts, as compared

to those that transmitted more detailed information, such as e-government websites. It appears that exposure to more detailed information results in critical responses and dissatisfaction, while exposure to less detailed information produces more positive assessments (Kardes et al., 2007).

> [Gregory Porumbescu on the effect of exposure to detailed information on e-government websites] “The more detailed the information gets, the more negative we respond. So, the idea is when governments are communicating on social media, it is really just a short depiction of what's going on, and perhaps this is more effective at building trust than longer explanations of what government is doing, simply because social media is light on details while government websites provide a lot of information. In other words, the more information you give, the more questions people will ask.”

These findings suggest that the two e-government mediums may serve different purposes — social media engagement is better suited for the dissemination of less detailed information and for trust building while government websites provide information of higher quality that contains greater details.

> [Gregory Porumbescu on the effect of government use of social media on citizens’ trust in government] “If we’re asking whether government officials who are getting on TikTok to promote policies and how that impacts trust in government, we’re not necessarily measuring the efficacy of those informational interventions. A better measure of whether this builds trust is not to ask whether it builds trust in government, but rather it builds trust in the policy.

5.3.3 Cycle of use and trust in e-government services

Existing studies have shown that citizen satisfaction with e-government services is influenced by factors such as system quality, information quality, and service quality (Beldad et al., 2012; Christensen & Lægreid, 2005; Welch et al., 2005). In turn, individuals who are highly satisfied with these services tend to develop a greater level of trust in the government.

Moreover, individuals who are satisfied with e-government websites also tend to use and participate in these services more frequently (Zheng & Schachter, 2017). They also hold more positive views regarding government transparency (Kim & Lee, 2012). This positive perception of e-government effectiveness encourages digital users to adopt e-government services, further reinforcing the cycle of use and trust (Ayyash et al., 2013).

6 Digital Trust in Singapore

Governments have long recognised the significance of safety and trust, and this holds true for the digital realm as well. Singapore is widely regarded as an international leader in e-government (Baum & Mahizhnan, 2015). E-government was first launched in 1989 and today citizens can access over 1,700 government services online (GovTech Singapore, n.d.). Singapore aims to be a “smart nation” and places a strong emphasis on digital trust and safety.

To cultivate and reinforce digital trust, the Singapore Ministry of Communications (MCI) works in collaboration with key agencies, including the Cyber Security Agency of Singapore (CSA) and the Smart Nation and Digital Government Office (SNDGO). The MCI actively engages

stakeholders from both the public and private sectors, employing a multi-faceted approach to enhance the safety of the digital realm. This involves the implementation of regulations, codes of practice, and state-level initiatives. As seen from the legislations to be presented later in Table 5, the country has already put in place policies to address threats, such as cybercrime, phishing scams and various online harms, in order to prevent the erosion of digital trust and optimise the opportunities digital technologies have to offer.

Singapore also ranks well in international indices. In the 2022 Digital World Competitiveness published by the IMD World Competitiveness Center, Singapore was ranked 4th overall and 10th for future readiness. However, in the sub-index of future readiness, Singapore was ranked lowest in privacy protection by law. The relatively lower scores in privacy protection are also reported by the other indices in this review.

In spite of this low ranking in privacy protection by law, another study conducted by Imperva reported that half of Singaporeans indicated that they “completely trust” the government to maintain the privacy of their personal data (Singapore Business Review, 2022). In contrast 40 per cent trust financial institutions and less than 10 per cent trust social media platforms and retailers to do the same. Srivastava and Teo (2009) also observed that digital users in Singapore have fewer security concerns when using e-government websites as compared to other websites, even though they were the most concerned towards the handling and use of their personal information (KPMG, 2017).

Local surveys conducted by Singapore’s Government Technology Agency showed that 99 per cent of citizens and 99 per cent of businesses expressed satisfaction with government digital services (GovTech Singapore, 2021a, 2021b). E-government services is widely available although some segments of Singapore’s population face barriers in access to them due to the inability or unwillingness to purchase ICT hardware and the unavailability of e-government services in Mandarin, Malay and Tamil (Baum & Mahizhnan, 2015).

Another index, the Digital Trust scorecard developed by the Fletcher School at Tufts University (2021) measures four dimensions of digital trust among 42 countries (see Figure 10):

1. Attitudes — the level of trust that digital users have towards providers of trust in the digital sphere
2. Behaviour — the extent to which digital users are engaged in the digital environment
3. Environment— the types of trust-building mechanisms related to privacy, security and accountability
4. Experience — the extent of friction experienced by digital users in relation to infrastructure, access and interaction

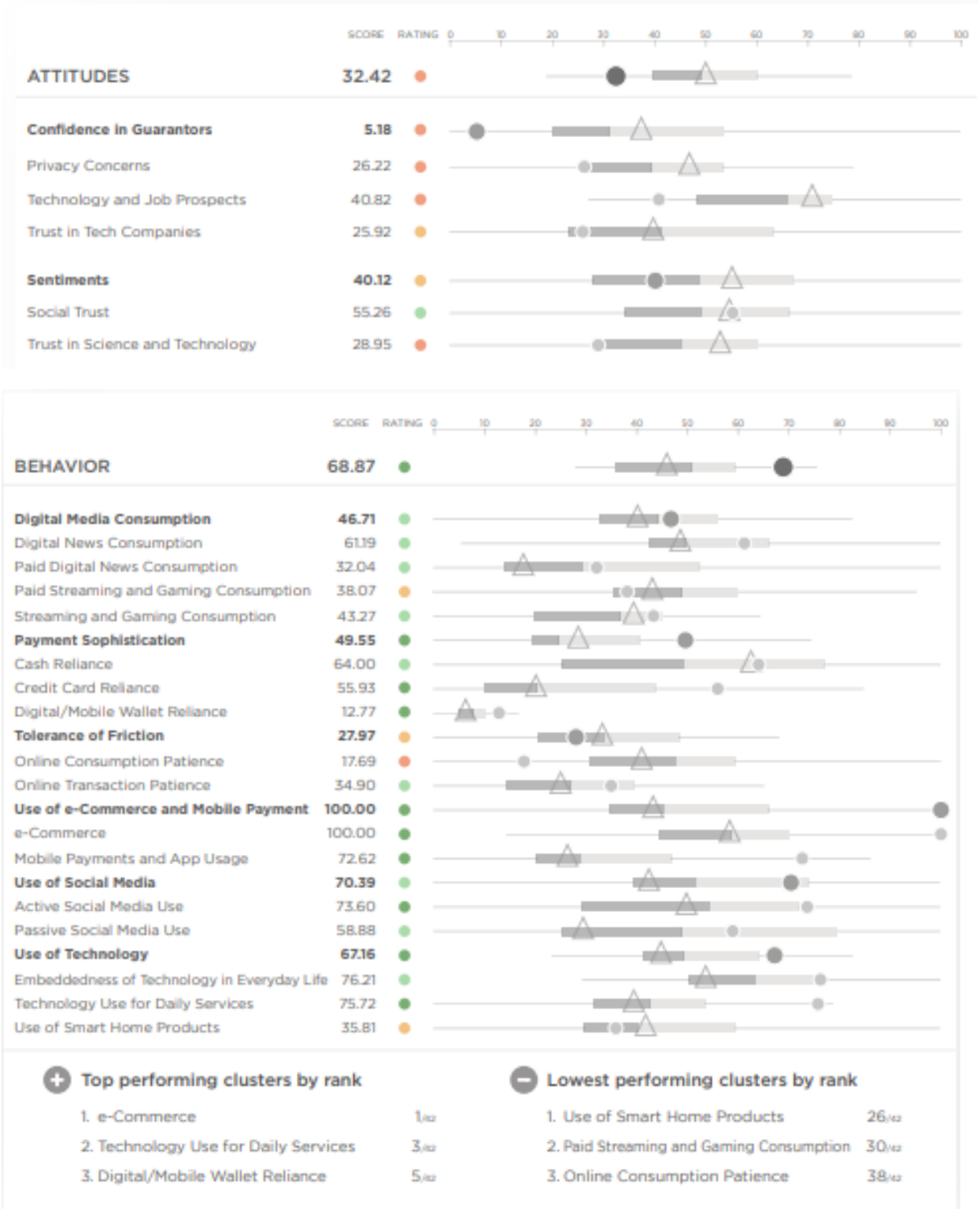
Singapore ranked 38th for attitudes with a score of 32.42. In the sub-indices, the country was ranked in the second quartile for social trust. Additionally, scores on privacy concerns and trust in science and technology were especially low, with a ranking of 33 and 34, respectively.

In terms of behaviour, Singapore ranked 4th with a score of 68.87. In the sub-indices, Singapore performed well in terms digital users’ engagement with e-commerce, use of technology for daily services and reliance on digital or mobile wallets. However, the country was ranked in the bottom quartile in terms of online consumption patience, as well as paid streaming and gaming consumption.

Singapore ranked 12th for environment with a score of 61.66. In the sub-indices, the country ranked first for its digital infrastructure, and second for cost as well as broadband performance. The lowest performing environment aspect was coverage, transaction performance and updated infrastructure, which were nonetheless ranked in the first two quartiles.

For experience, Singapore ranked 4th with a score of 68.68. In the sub-indices, Singapore was awarded high scores in terms of accountability and security — in particular, cyber infrastructure, institutional credibility and digital hygiene. However, the country did not perform as well in terms of privacy, with factors such as surveillance, data governance and institutional capability ranked in the third quartile.

Figure 10. Singapore rankings on the Digital Trust scorecard



6.1 Singapore's approach to building digital trust

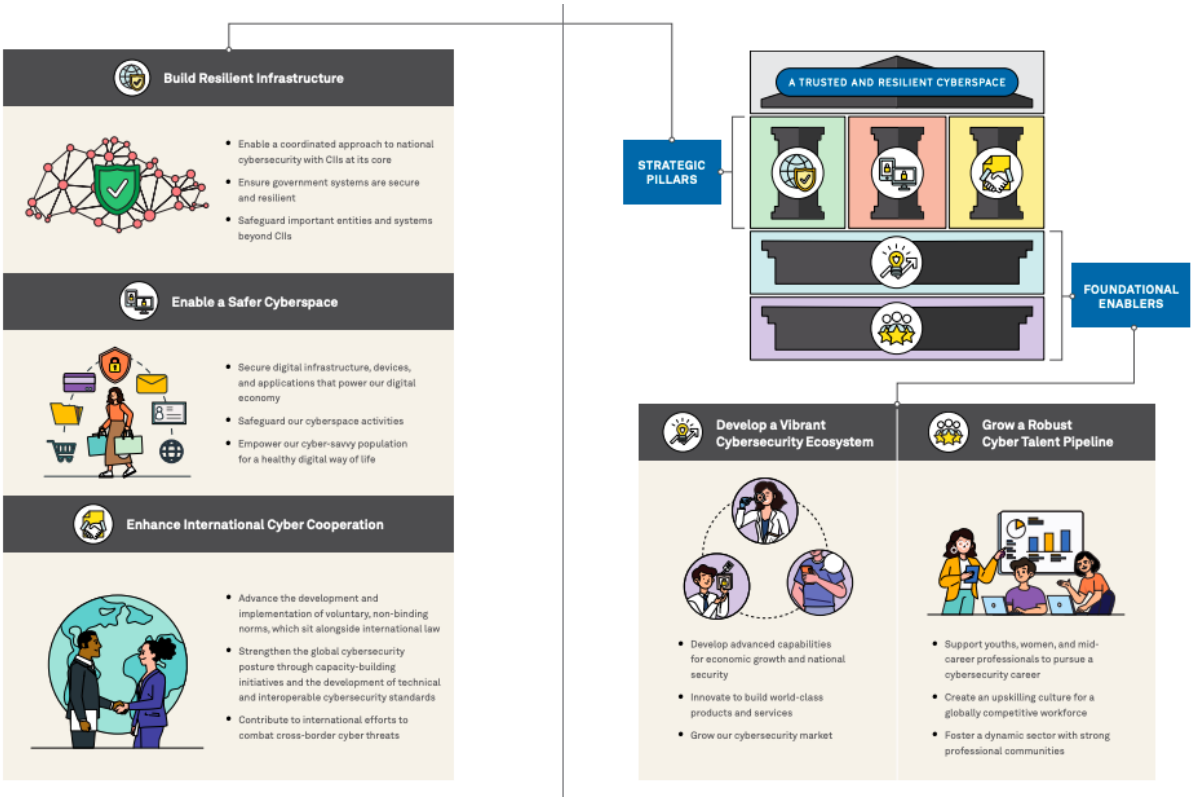
Singapore's approach to building digital trust is reflected in the Cybersecurity Strategy of Singapore that was developed by the government in 2021. It delineates Singapore's goals and priorities to safeguard the country's cyberspace, ensure that digital users in Singapore

experience robust cybersecurity, and advocate for the establishment of global cyber norms and standards (Cyber Security Agency, 2021).

The strategy comprises three strategic pillar and two foundational enablers (see Figure 11):

- Strategic Pillar 1: Build resilient infrastructure
- Strategic Pillar 2: Enable a safer cyberspace
- Strategic Pillar 3: Enhance international cyber cooperation
- Foundational Enabler 1: Develop a vibrant cybersecurity ecosystem
- Foundational Enabler 2: Grow a robust cyber talent pipeline

Figure 11. Overview of the Singapore Cybersecurity Strategy 2021



Source: (Cyber Security Agency, 2021, pp. 3–4)

6.1.1 Build resilient infrastructure

Regulation remains as a vital tool in ensuring that digital infrastructures remain secure and resilient against digital threats. Table 5 lists legislative frameworks that address various digital threats. We mapped these legislations to the dimensions of mechanical digital trust that have been discussed in this review.

Table 5. Legal frameworks that address digital threats

Regulation	Purpose	Digital trust dimension
Cybersecurity Act	• Strengthen the protection of critical information infrastructure (CII) against cyber attacks • Authorise the Cyber Security Agency (CSA) to prevent and respond to cybersecurity threats and incidents • Establish a framework for sharing cybersecurity information • Establish a light-touch licensing framework for cybersecurity service providers	Cybersecurity
Computer Misuse Act	• Criminalise unauthorised access to computer systems or networks such as hacking • Prohibit unauthorised interference with computer systems, networks or data such as introducing viruses and disrupting computer service • Penalise misuse of computer systems such as committing fraud	Cybersecurity
Personal Data Protection Act	• Sets out rules and guidelines on the collection, use, disclosure and care of personal data	Privacy
Online Safety Act	• Authorises the Infocomm Media Development Authority (IMDA) to issue directives to Online Communication Services[7] to remove or block egregious content such as those promoting suicide or self-harm, sexual exploitation, terrorism and hate	Safety
Code of Practice for Online Safety	Social media services that have been designated as having high reach or high risk are required to: • Protect digital users from exposure to harmful content • Provide reporting and resolution mechanisms for digital users to report harmful content and unwanted interactions easily • Provide IMDA with information regarding implemented measures to combat harmful and content and help digital users make informed decisions when using these services	Safety Redressability
Content Code for Social Media Services	• Authorises IMDA to direct social media services to take action against harmful online content to protect digital users or disallow specified accounts to communicate such content and interact with other digital users	Safety
Internet Code of Practice	• Authorises IMDA to remove online content that goes against public interest, public morality, public order and national harmony	Safety

[7] These are electronic services that allow users to access or communicate content via the Internet or deliver content to end-users.

6.1.2 Enable a safer cyberspace

The government has ensured that digital infrastructure, devices and applications that are critical in the digital economy are secure. For instance, in collaboration with internet service providers, the government is in the process of implementing Domain Name System Security Extension (DNSSEC) protocols. These protocols serve to prevent malicious actors from redirecting end users to fraudulent websites or services, thus enhancing security for online activities and prevent cyber threats from reaching end users.

Enterprises and organisations also play a critical role in ensuring a safe digital environment. Self-help tools and cost-effective solutions have been made available by the government to strengthen their cybersecurity and standard of data protection (see Table 6).

Table 6. Resources for enterprises and organisations to strengthen their cybersecurity and data practices

Resources	Purpose	Digital trust dimension
Data Anonymisation Tool	• Free tool that organisations can use to anonymise their datasets to reduce the risk of data breaches	Privacy Cybersecurity
Internet Hygiene Portal (IHP)	• Provides enterprises with self-assessment tools and actionable recommendations to adopt best practices and enhance their overall internet security	Cybersecurity
Privacy Enhancing Technologies (PET) Sandbox	• Facilitates testing and development of new PETs that can help protect individuals' personal data while enabling businesses to collect and use that data for legitimate purposes • Provides resources such as technical expertise, legal and regulatory advice, and funding support	Privacy Cybersecurity
Data Protection Essentials (DPE) Programme	• Supports Small and Medium Enterprises (SMEs) in adopting fundamental data protection and security practices that protect customers' personal data and enable swift recovery during data breaches	Cybersecurity Privacy

Technical capabilities that can help detect, respond to and recover from digital threats have been strengthened through initiatives such as the Cyber Fusion Platform and Singapore Computer Emergency Response Team (SingCERT), which allow the government to detect, resolve and prevent incidents on the internet that are related to cybersecurity.

To encourage businesses to invest in the security of their products, various public sector initiatives have been implemented to allow digital users to access the cybersecurity provisions of the digital service they are using (see Table 7). These initiatives not only bolster the

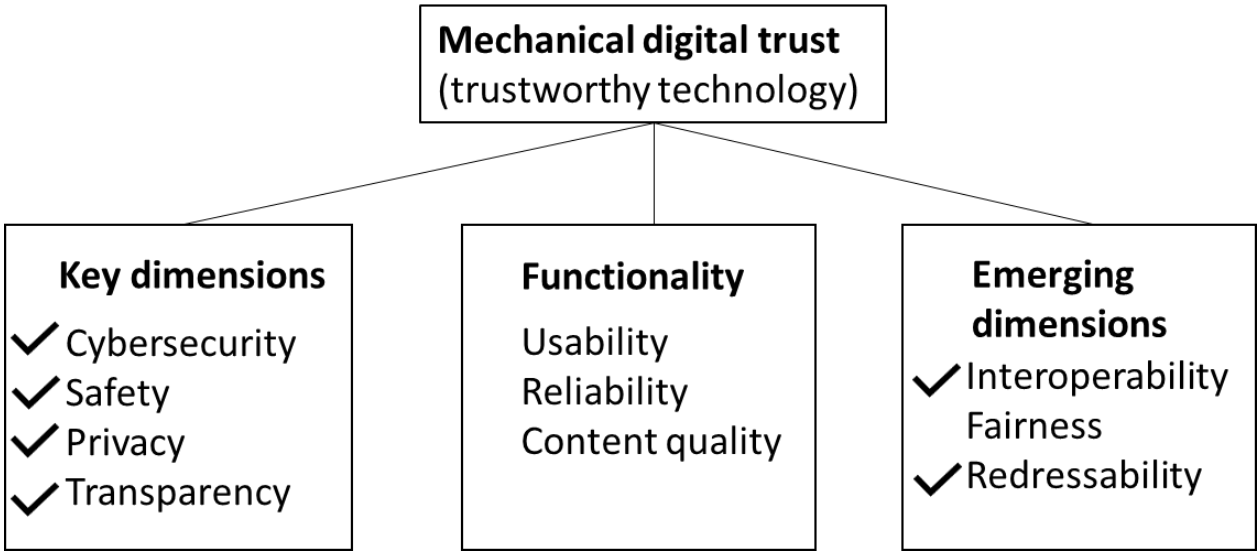
dimensions of cybersecurity and safety but also encourages transparency in digital practices among organisations operating in Singapore.

Table 7. Initiatives that allow digital users to access cybersecurity provisions of digital services

Initiatives	Purpose	Digital trust dimension
Cybersecurity Labelling Scheme	• Enables digital users consumers to identify the security standards of digital devices and make informed decisions	Cybersecurity
E-commerce Marketplace Transaction Safety Ratings (TSR)	• Assigns e-commerce marketplaces an overall safety rating that reflects the degree to which safety features that are critical in combating scams have been implemented	Safety
Data Protection Trustmark (DPTM) Certification	• Verifies that organisations have implemented data protection practices that comply with the obligations of the PDPA	Privacy Transparency
Internet Hygiene Rating	• Provides visibility on the cyber hygiene of digital platforms to help consumers make informed choices to better safeguard their digital transactions from cyber threats	Transparency Cybersecurity
SG Cyber Safe Trustmark	• Verifies that organisations that are larger — and therefore have higher risk levels — have implemented robust cybersecurity practices and measures that are aligned with their cybersecurity risk profile	Cybersecurity Transparency
Cyber Essentials	• Cybersecurity certification targeted at SMEs, which recognises that good cybersecurity measures have been implemented	Cybersecurity Transparency
Singapore Common Criteria Scheme	• Evaluates and certifies the security attributes of information technology (IT) products	Interoperability Cybersecurity

Returning to our earlier compilation of the dimensions of mechanical digital trust, Singapore as a country is checking all the boxes for the key dimensions of cybersecurity, safety, privacy and transparency (see Figure 12). There are a few initiatives directed at interoperability and the Codes of Practice for Online Safety has elements of redressability.

Figure 12. Dimensions of mechanical digital trust revisited



Understandably, there are few legislations and national initiatives directed at the dimensions of usability, reliability and content quality as these are dimensions that manifest in the individual platforms. Fairness is the obvious missing dimension although in our earlier discussions, we noted that fairness is a very subjective notion and requires value judgements of fairness for whom.

Singapore's national efforts are also directed at the relational digital trust dimensions and according to the Cybersecurity Strategy Agency of Singapore, the development of a healthy digital environment also involves empowering digital users in Singapore to be cyber-savvy. Efforts have been made to raise awareness and change attitudes towards cybersecurity as well as promote the adoption of good cyber practices (see Table 8).

Table 8. Initiatives to raise awareness and promote adoption of good cyber practices among Singaporeans

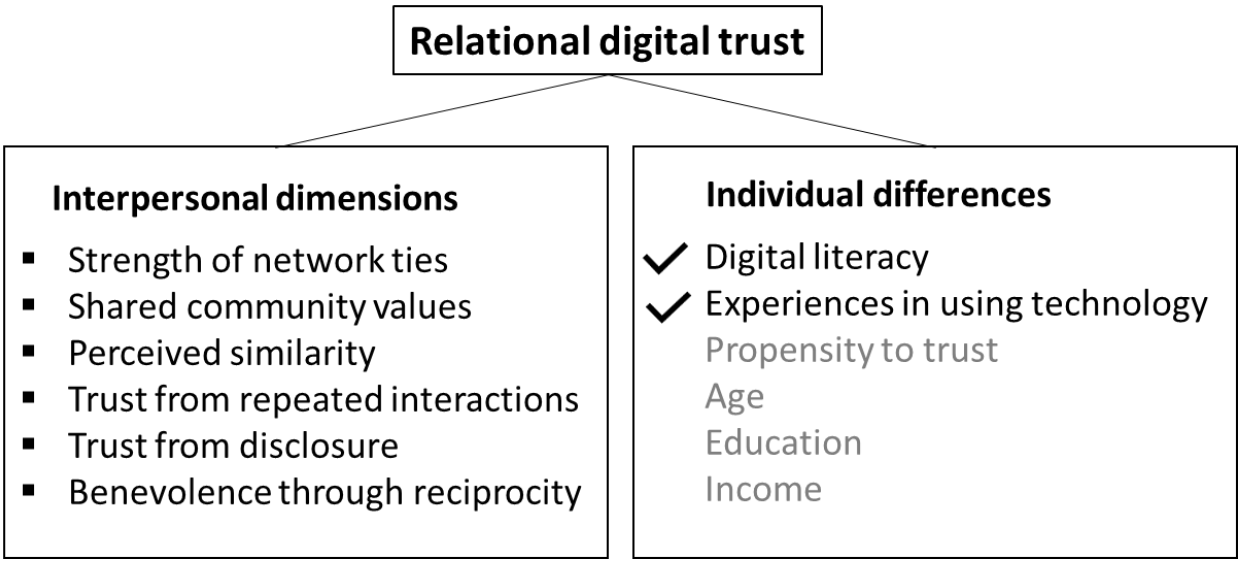
Initiatives	Purpose
Better Cyber Safe than Sorry campaign	Launched in 2021 by CSA, the campaign focuses on four cybersecurity tips that can be used in everyday life: • Using strong passwords and enabling two-factor authentication • Identifying signs of phishing • Using anti-virus software • Making timely software updates
"I can ACT against scams" campaign	The Ministry of Home Affairs (MHA) initiated the campaign in 2023, which emphasises three key actions: • Adding security features • Checking for scam signs and verifying with official sources • Telling authorities, family and friends about scams

Better Internet Campaign	Led by the Media Literacy Council (MLC) since 2014, the campaign aims to enhance public awareness in three key domains: “Be Safe, Be Smart and Be Kind.” It addresses issues such as cyber safety and security, and cultivating critical thinking to identify false online information and cyber-bullying.
SG Cyber Safe Students Programme	CSA works in collaboration with the Ministry of Education (MOE) and partner agencies such as Singapore Police Force (SPF) and IMDA to create educational initiatives and resources that inform students of various digital threats and empower them with skills to stay safe online.
Source, Understand, Research, Evaluate (S.U.R.E)	The National Library Board's (NLB) S.U.R.E. programme promotes information literacy and fosters awareness about the perils of fake news, as well as teaches individuals how to discern these. The enhanced S.U.R.E. 2.0 initiative focuses on three primary areas that cater to students, working adults, and the general public, including segments such as senior citizens.
Be Internet Awesome programme	Google introduced the Be Internet Awesome programme in collaboration with online safety experts in 2017 to educate children about digital safety. The programme incorporates an interactive web-based game called Interland and an educational curriculum. MLC has collaborated with Google to encourage primary school students in Singapore to participate in the game.
Go Safe Online portal	It is a portal overseen by CSA that provides tips on good cybersecurity practices such as how to use anti-virus software and identify signs of phishing.
News and Media Literacy Toolkit	Through a partnership with Common Sense Education, MLC has developed a comprehensive toolkit to enhance media literacy skills among young individuals. Designed for students aged 13 to 18, this toolkit covers various topics, including evaluating the credibility of news sources, recognising digital photo manipulation, and distinguishing between factual information and personal opinions.
Get Smart with Sherlock	MLC has created a fact-checking starter kit to assist young individuals in effectively discerning real content from false information online. It covers topics such as the definition of fake news and its various forms, the ramifications of spreading fake news, and techniques to identify false information.
Factually	A government-operated website that aims to debunk misinformation related to a wide range of topics.
Singapore SMS Sender ID Registry	Protects customers from fraudulent SMS messages that impersonate the SMS Sender IDs of organisations that send SMS to their customers.

ScamShield	Allows digital users to automatically block scam calls and identify scam messages by cross-referencing incoming calls from unfamiliar numbers with a database maintained by the Singapore Police Force.

Nearly all of these initiatives bolster the key dimensions of mechanical digital trust at the level of individual users and work through the relational digital trust dimensions of increasing digital literacy and experiences in using technology. However, returning to the earlier compilation of the dimensions of relational digital trust (see Figure 13), few of the initiatives capitalise on the interpersonal dimensions that drive digital trust. The two exceptions are the "I can ACT against scams" campaign by the Ministry of Home Affairs that emphasises the strength of the network to "tell authorities, family and friends about scams"; and the Better Internet campaign by the Media Literacy Council to "Be Safe, Be Smart and Be Kind", which has an element of benevolence in digital spaces. We offer recommendations in the next chapter on how to infuse and leverage more elements of these dimensions of relational digital trust in future digitalisation efforts.

Figure 13. Dimensions of relational digital trust revisited



6.1.3 Enhance international cyber cooperation

Singapore has been actively involved in promoting the advancement and adoption of voluntary norms in cyberspace through participation in international discussions, including those with the United Nations, such as the UN Group of Governmental Experts where Singapore emphasised the importance of states adhering to cyber norms and stability frameworks (Cyber Security Agency, 2021). Additionally, Singapore collaborates with ASEAN and international partners to implement cyber norms through initiatives such as the UN-Singapore Cyber Programme. This programme aims to develop an implementation checklist that provides action recommendations for countries to undertake to implement cyber norms (Cyber Security Agency, 2021). These efforts not only contribute to stronger cybersecurity and safety in the

region but also helps to improve interoperability of standards and data in the participating countries.

Furthermore, Singapore is actively working towards elevating the global baseline level of cybersecurity through providing support for capacity-building initiatives and fostering the development of technical and interoperable cybersecurity standards. The ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) was established in 2019 as part of the ASEAN Cyber Capacity Programme, and aims to enhance cyber policy, operational and technical capacities among senior ASEAN officials. The centre focuses on conducting research, delivering training on cybersecurity strategy and legislation, and facilitating the implementation of international cyber norms. It provides skills training and information sharing for Computer Emergency Response Teams (CERTs). Participants can also benefit from hands-on practical experience through virtual cyber defence training and exercises.

6.1.4 Develop a vibrant cybersecurity ecosystem

Singapore has been supporting the development of the local research and development research and development (R&D) ecosystem. In 2013, the National Cybersecurity R&D Programme (NCRP) was introduced with the objective of fostering R&D collaborations with academic partners and research institutions in Singapore. This programme aims to strengthen and extend Singapore's cybersecurity capabilities. More recently, in 2022, the Digital Trust Centre was established by Nanyang Technological University. This centre aims to spearhead research and innovative technologies that enhance digital trust, including privacy protection solutions, as well as to contribute to the growth of local talent and businesses in this area.

In order to cultivate innovative cybersecurity products and services, the government has introduced the Cybersecurity Industry Call for Innovation, which encourages cybersecurity companies to develop solutions to critical cybersecurity issues. Singapore also nurtures emerging cyber entrepreneurs and start-ups through the Innovation Cybersecurity Ecosystem at Block 71 (ICE71), which offers innovators and start-ups with support such as entrepreneurship programmes that are designed to engage the cybersecurity ecosystem community.

6.1.5 Grow a robust cyber talent pipeline

Developing fresh talent and upskilling existing professionals are crucial components in achieve the three strategic thrusts outlined above. This entails generating interest among young individuals, women and mid-career professionals to pursue careers in cybersecurity (see Table 9), as well as improving career pathways, providing training opportunities and supporting the continuous growth of existing cybersecurity professionals (see Table 10).

Table 9. Initiatives to support youths, women and mid-career professional to pursue careers in cybersecurity

Initiatives	Purpose
SG Cyber Educators	• Provides principals, teachers and school career counsellors with knowledge about cybersecurity and its career opportunities

Cyber Work-Learn	• Allows those in full-time National Service with cyber talents to develop their cybersecurity skills through vocation training, on-the-job training and academic training
Student Volunteer & Recognition Programme	• Recognises youth volunteers that contribute to enhancing Singapore's cybersecurity
Singapore Cyber Youth Programme	Provides students from secondary to tertiary levels with opportunities to explore cybersecurity as a career, and be exposed to relevant technical knowledge and soft skills. Key initiatives related to training boot camps, competitions, learning journeys and career mentoring sessions: • Cybersecurity Career Mentoring Programme • Youth Cyber Exploration programme • Cybersecurity Learning Journeys • SG Cyber Youth Odyssey
SG Cyber Women	• Encourage women as young as pre-tertiary education age to pursue a cybersecurity profession through education and community engagement and skills development
Cyber Security Associates and Technologists Programme	• Train and up-skill fresh ICT professionals and mid-career professionals for cyber security job roles

Table 10. Initiatives that improve career pathways and training for cybersecurity professionals

Initiatives	Purpose
Skills Framework for Infocomm Technology (SF for ICT)	• A guide for individuals to identify ICT skills and training required to stay relevant
Operational Technology Cybersecurity Competency Framework (OTCCF)	• Maps out various operational technology cybersecurity job roles, the corresponding technical skills and core competencies required, and possible career pathways
Cyber Security Development Programme	• A 15-month programme that provides fresh graduates and mid-career professionals with cybersecurity training • Classroom training with CSA Academy, the Singapore University of Technology and Design (SUTD), and Ngee Ann Polytechnic lasts for the first three months • Trainees will be deployed to one of CSA's divisions or partner agencies during the remaining twelve months
CSA Academy	• Provides experienced cyber security professionals with niche training that is not covered by institutes of higher learning

Cybersecurity Strategic Leadership Programme	• A 15-day training programme comprising of four modules targeted at cybersecurity leaders

Taking a broad overview of Singapore's approach to building digital trust, it is clear that resources and efforts are mostly directed at the key dimensions of cybersecurity, safety and privacy, and rightly so. There are also notable efforts in encouraging transparency of digital practices for companies and state level initiatives to improve the digital literacy and technology experiences for its people. Gaps in these efforts include transparency and privacy in e-government which Singapore scores relatively lower in global indices and national level thought leadership on the kind of Internet community that Singapore wants to nurture and the social norms of users in local digital communities. Developing a trustworthy digital ecosystem poses an ongoing difficulty due to the constant evolution of digital technologies and the changing landscape will in turn, alter the dynamics of human interactions in the digital realm and the way humans interact with digital technologies.

[Authors' note] Many of the indices and benchmarks above are also discussed in Chapter 4 of the companion policy review on digital sovereignty in this series of policy reviews. In the current review, we tabulated the different programmes and efforts thematically. Readers can also refer to "Digital Sovereignty: State Action and Implications for Singapore" by the NUS Centre for Trust Internet and Community and the Institute of Policy Studies for more detailed descriptions of some of these efforts.

7 Recommendations From an Ecosystem Perspective

The first recommendation we offer to policymakers and organisations to stem the erosion of digital trust is not about what they can do but what not to do — and that is **to not conduct surveillance** for the purposes of targeted communications campaigns. Digital users are increasingly concerned and aware about targeted digital campaigns that use data collected from their online activities to generate personalised communications. Online advertisements, when overly personalised, have been found to raise concerns among digital users (White et al., 2008). When digital users see targeted advertisements that contain information that they unknowingly provided, they realise that advertisers have obtained this personal information in ways that were not made known to them (Sheehan & Hoy, 2000).

Such targeted communications and advertisements that imitate digital users' previous behaviours create fear and a feeling of being surveilled (Ruckenstein & Granroth, 2020). Users fear not knowing the type and volume of information that are collected and how they may be used. Users have little control over their data trails, and also how their data may be used against them. In our interviews with key experts, surveillance by social media platforms for targeted advertising was also cited as a factor that diminishes digital trust.

> [Tammy Lin on surveillance by social media platforms] "We always feel like, 'what I type in my Facebook messenger, I'll get the advertisement for whatever is related to it fed to me.' As a result, we have zero trust in the Meta company or the algorithm because we feel like 'Oh, the big boss knows everything, even though it's private messages.'

> "Facebook, would, you know, give you the advertisement that related to what you typed in private messages. That's just horrifying. In Facebook… I'm not actually searching for brands or anything, I just talk in private messages, and then it appears in the ads, then that's creepy, because, you know, it's part of my private conversation. So… when I expect that it's private messenger, it should be private but the Facebook algorithm doesn't make you feel private at all. So, that breaks, you know, breaks the trust issue and all."

Professor Lin emphasised the key role that social media platforms play in ensuring a sense of safety and building digital trust.

> [Tammy Lin on digital platforms as the key to building digital trust] "I think definitely the platform, the technology of the platform plays a really important role… you know, TikTok, we believe that the algorithm is actually by people who are working on giving you all the recommendations. So, I think the platforms itself is the first thing that can address and create this safe environment and the rest is really up to the person themselves. So, the platform is important…. The platform or certain features of the platform help engage in these kinds of processes that would be key to trust."

The rest of the chapter iterates the recommendations for what policymakers and organisations can do to enhance digital trust from a trust ecosystem perspective. Before we present these recommendations, we first acknowledge that we are not cybersecurity specialists, and we offer these suggestions for consideration as social scientists of digital communications and digital literacy. For more technical and technology-specific recommendations in cybersecurity, we would refer the readers to technical experts in these disciplines.

7.1 Adhering to state-of-the-art data privacy practices

In tandem with our first recommendation to not conduct surveillance on end users, adhering to state-of-the-art data privacy practices will improve protect privacy, enhance transparency about data collection processes, and in turn sustain digital trust. In our review, a few best practices are frequency mentioned and should be adopted by both the purveyors of technology and public agencies deploying e-government applications (see Table 11 for a compilation of data privacy best practices that promote digital trust).

Table 11. Data privacy practices that promote trust

Data privacy best practices	MAGNA (2022)	CISCO (2022)	Anant et al. (2020)	KPMG (2017)
Transparency in collecting and using data	*	*		*
Sharing of data with third parties only when necessary	*	*		*
Collecting only essential data / minimising data retention period /	*		*	
Protecting data / avoiding data breaches		*	*	

Promote privacy through compliance with privacy laws, configuration of privacy settings, two-factor authentication		*	*	
Proactively report a hack or breach			*	

Indeed, according to a 2021 study by Insider Intelligence, a platform that protects user privacy and data is the top factor that affects American social media users' decision to engage with ads or sponsored content on social media platforms. The other studies above have also identified important data practices that will increase trust among users. For instance, Anant et al. (2020) reported that digital users are more likely to trust web vendors that minimise the data collected. This includes web vendors withholding from asking for information that is irrelevant, asking for too much personal information, and collecting passive data.

We recognise that the complexities of adhering to these data privacy practices. Each practice entails detailed considerations such as consent management, cross-border data strategies, and third-party accountability. Moreover, compliance requirements in different jurisdictions are constantly evolving, posing challenges to effective privacy compliance. In our companion policy review on digital sovereignty, we delve into the issue of data sovereignty in greater detail.

As one of the responses to the complexities of privacy compliance, the World Economic Forum (2022) suggested leveraging technology to support digital trust. For instance, AI-based data monitoring can validate data accuracy, authenticity, and reliability. Cloud-enabled data trusts can govern and secure data processing and access rights. Additionally, blockchain technology can preserve immutable transaction records, ensuring provenance and protection against tampering.

Given the dynamic nature of privacy compliance, it is crucial for governments to regularly review privacy legislation and programmes, while companies should continuously improve their digital trust efforts in line with evolving expectations and requirements.

7.2 Defining the scope of cyber safety and online harms

The Sunlight Alliance for Action (Sunlight AfA) aimed to tackle online harms, especially those targeted at women and girls. Sunlight AfA exemplified the collaborative efforts of stakeholders from various sectors working together to make the online space safer, particularly for women and girls in Singapore. At the core of its recommendations after a year of public engagements on the issue lies the crucial need to define the scope of cyber safety and assess the impact of online harms (Ministry of Communications and Information, 2022).

The significance of defining the scope of cyber safety and addressing online harms cannot be overstated. It requires proactive anticipation and mitigation of a wide range of potential harms, and considering the unique challenges posed by each technology. These include social media settings with concerns about well-being and content moderation, extended reality (XR) experiences involving personal space invasion, or self-driving cars raising issues of reckless driving and safety (WEF, 2022). Every context demands specific attention.

Engaging the community, technology companies and domain experts is key to developing a comprehensive understanding of the risks and harms involved. Through proactive efforts to define the scope of cyber safety and online harms upstream, we can establish effective safety measures and redress mechanisms downstream. Furthermore, these endeavours to define the scope and nature of online harms that should be address will shape the reach and impact of legislation, such as the Codes of Practices for online safety.

By fostering collaboration among stakeholders to actively define and address the scope of cyber safety and online harms, we can better safeguard the interests of individuals in the digital realm and promote the growth of a trustworthy digital ecosystem.

7.3 Preparing for interruptions in digital services through collective capacity building

It would be naive to assume that with the best intentions and practices, digital disruptions and breaches would be eliminated. When these occur — and we should expect them to — effectively addressing the disruptions and breaches in digital services is crucial to recovering digital trust and should focus on two key areas: the policy framework and human capacity.

For technology companies, user-centric policies play a critical role in establishing a robust framework for addressing disruptions and breaches. In the WEF digital trust framework (2022), developing a comprehensive policy framework involves various aspects, such as estimating the duration of the initiative and identifying potential dependencies that may cause interruptions. It also requires a thorough assessment of regulatory and compliance requirements to ensure adherence to standards and fill any existing gaps. Understanding the benefits that improvements in digital trust can bring is essential for shaping the policy direction, both at the company and at the country level. Additionally, identifying and mitigating risk areas is crucial to enhancing digital trust. Allocating specific teams and resources for cybersecurity, privacy and audit functions helps support the implementation of the risk-mitigation initiatives.

On the other hand, building collective capacity within the community focuses on the people aspect of addressing disruptions and breaches. In the private sector, this involves fostering leadership commitment to risk mitigation policies. In the people sector, it is crucial to develop the necessary skills within the community to meet the capability requirements when technology fails. This may involve encouraging stakeholders and community champions to create a network of digital response teams to help the community navigate disruptions and breaches in the digital realm. Building up to these networks of digital trust teams would involve identifying skill gaps, providing training opportunities and knowledge sharing between teams to enhance the collective community capacity and ensure that digital services remain trustworthy and benefit their users.

7.4 Improving redressability for end users

With the prevalence of digital risks and online harms, redressability is of paramount importance in ensuring trust in technology ecosystems. It enables individuals, groups, or entities that have been negatively affected by technological processes, systems or data uses to seek recourse and have their grievances addressed (WEF, 2022). As the preceding recommendation has pointed out, unintentional errors or unforeseen circumstances are

inevitable and can lead to unexpected harms. Robust methods and mechanisms for redress in these situations are key to preserving digital trust.

In the tech industry, companies have been taking steps to enhance redressability. Many organisations have implemented support functions that cater to users, customers or clients, often starting with automated self-service options like FAQs and expanding to provide support through email, phone calls or chat messages with bots or agents. However, it is essential to strike a balance between automation and dedicated support to avoid burdening individuals seeking redress. Investment in support for customers and empowering capable employees to address grievances directly will contribute to bolstering an organisation's trustworthiness (WEF, 2022).

Another key stakeholder in improving redressability is the state. Australia has taken notable strides in promoting online safety and redressability. The establishment of the eSafety Commissioner, the world's first government agency dedicated to online safety, showcases Australia's commitment to addressing digital harms (Bantourakis & Manojlovic, 2023).The Online Safety Act 2021, introduced by the Australian government, sets standards and requirements for online service providers, granting the eSafety Commissioner the authority to issue notices for removal, blocking, app removal, or link deletion of harmful online content. The Adult Cyber Abuse scheme, a world-first initiative, offers protection for Australian adults and imposes fines and penalties on individuals posting cyber-abuse material targeting adults (Sainty, 2022).

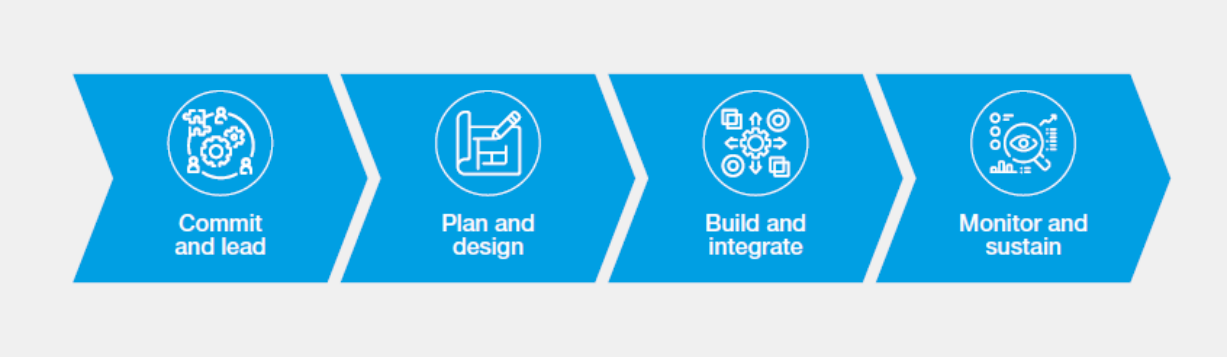
Singapore has already made amendments to the Online Safety Act to include codes of practices that will improve the redressability mechanisms for the users of major technology platforms in the country. The establishment of an oversight agency such as the eSafety Commissioner will greatly advance the avenues for redress and bolster digital trust in the country.

7.5 Building a whole-of-nation mindset for digital trust

Building a whole-of-nation mindset for digital trust requires three things: companies to commit to being trustworthy stakeholders in digital environments; the community to do more to harness the strength of network ties; and the government to provide the appropriate level of oversight.

For the private sector, the WEF (2022) laid out a digital trust roadmap for companies to approach technology decisions (see Figure 14) in order to develop and deploy trustworthy technologies:

Figure 14. Digital trust roadmap (WEF, 2022, pp.30–33)



Commit and lead: Digital trust requires commitment from top leadership. CEOs and boards need to endorse and support long-term digital trust programmes. They should align digital trust with organisational strategy and other key areas like product development, marketing, risk management, privacy and cybersecurity.

Plan and design: Organisations should perform a digital trust gap assessment to identify current capabilities and deficits. The assessment should provide recommendations, identify risks, benefits, timelines, and resource requirements. Organisations need to build and integrate digital trust into their operations and align teams and practices accordingly.

Build and integrate: Leaders should focus on people, processes and technology. They should adopt leadership and behavioural changes, develop necessary workforce skills, and deploy structured change management and communication strategies. Processes should include change management practices, decision-making structures, data governance and risk management. Existing data assets should be understood and integrated for effective digital trust implementation.

Monitor and sustain: After implementing a digital trust programme, ongoing efforts are needed for its effectiveness and longevity. Performance and risk measurement tied to incentives should be established. Regular reporting, including maturity metrics, should be conducted. Continuous improvement is essential to meet evolving expectations and business requirements.

For the community, everyone must develop their digital literacy skills and those who are more skilled will step up to help those who are less able. These actions are also recommended by two of the experts we interviewed:

> [Bill Dutton on developing a cyber security mindset] “In Oxford, everybody rides a bike to work and they always care about the security of their bicycle [or it’ll] get stolen. So, they lock the bike, they park it in a visible place. They often buy a used bike, so that nobody will want to steal their bike. It’s part of their mindset that ‘I've got to protect my bike.’ Online, people often don’t have a cybersecurity mindset. But increasingly, we’re trying to use that as a positive way of teaching the skills and reasoning to think about the things people can do to make sure that they lock up their computer, their data and so forth.”

> [Jonathan Obar on establishing intermediaries that can help users figure things out] "We're being asked to check our data, we have to read privacy policies, we have to follow up and make sure the application of our data is being used properly, and it's being used by thousands of companies all over the world. This is an unrealistic situation to be placed in. Perhaps a form of representative governance — data governance — is required…. Perhaps the goal there is to develop a trusting relationship with a fiduciary or an intermediary to achieve the goals that representative governance achieves, to delegate, so that we can get the deliverables that we want — privacy, reputation, protection — without having to spend hours and hours and hours, figuring everything out."

Governments play a crucial role in meeting society's expectations regarding digital trust. They achieve this by implementing legal and regulatory requirements and ensuring compliance through oversight mechanisms. In Singapore, there has been a collaborative approach to regulation, with consultations involving technology companies and civil society organisations when implementing policies like the Online Safety (Miscellaneous Amendments) Act 2022. However, if self-regulation and codes of practice prove inadequate in meeting society's expectations, the government must be prepared to intervene, and there are instances where stricter regulations have been put in place.

> [Jonathan Obar on imposing fines for deceptive designs] "One of the things that we're debating in Canada is the extent to which fines should be imposed for problematic consent processes. That's something that I would encourage policymakers to consider if self-regulation isn't going far enough, then maybe companies need to be fined in the United States. There have been all sorts of fines in Europe for deceptive designs related to consent processes."

7.6 Expanding the trust ecosystem for cybersecurity to the region

Cybersecurity poses significant challenges, and the risks associated with cyber threats have far-reaching consequences. However, effectively addressing cyber risks often requires substantial financial and human resources. As an island-state, Singapore is a small player in the global digital economy, even as it often punches above its weight. The size of the country is also a limiting factor in navigating the challenges of digital sovereignty, which we discussed in our companion policy review[8].

To tackle these challenges, regional collaboration within ASEAN offers numerous benefits. In this section, we briefly describe the benefits of expanding the trust ecosystem for cybersecurity through regional collaboration and, in turn, enhancing digital trust. The promise of regional collaboration specifically for digital sovereignty is discussed in greater detail in the companion policy review.

In summary, from the policy review on digital sovereignty, addressing the challenges of cybersecurity requires regional collaboration within ASEAN. By spearheading efforts to enhance regional cybersecurity capacity, advocating for greater coordination against cybercrime, and promoting harmonisation of data privacy and protection laws, Singapore can play a vital role in creating a digital trust ecosystem. This can be achieved through initiatives

[8] Digital Sovereignty: State action and implications for Singapore (Soon et al., 2023).

that foster knowledge exchange, capacity building, and the development of interoperable technologies while ensuring robust accountability and oversight mechanisms (Soon et al., 2023).

The overarching theme for our set of recommendations has been collaboration between public agencies, private entities, the community and also between countries. The WEF (2022) noted that people and governments increasingly expect companies that develop and offer digital services to respect societal values and meet user expectations and that trust and support are withheld from those who do not adhere to these principles and responsibilities. But the responsibility does not lie solely with companies. Governments, civil society and individuals each play crucial roles in building trust in the digital realm. By fostering cooperation between all these stakeholders, we can develop technologies that are reliable and trustworthy. This, in turn, encourages widespread technology adoption and benefits a larger number of users in society.

8 Conclusion

Following the World Economic Forum's assertion that digital trust has declined, we undertook this policy review to analyse the dimensions of digital trust and analyse its importance for Singapore. At the outset of this review, the diverse actors, entities and elements of digital trust, as well as the bi-directional nature of trust begetting trust, imply that digital trust has been used as a broad and vague notion:

> [Gregory Porumbescu on ambiguity of digital trust] "I think it's very difficult to say what digital trust is first of all, and I think the other problem is that it's so diverse, so just lumping everything into this big bucket and saying that digital trust is decline, I don't know that that's really accurate. I think that is a dangerous statement in the sense that it creates a perception, an imprecise perception of reality."

> [Jonathan Obar on digital trust as a feeling] "You could argue it's like a construct, not a concept, because it's made of many pieces. It's this challenge of trying to generalise about a concept. I think you can have trust in a privacy context. I think you can have trust in a, whatever you want to call it, like, the information literacy context.… Trust is one of these things you're trying to explain like a feeling that people have."

Furthermore, one could even question the significance of the concept of digital trust since digital users may continue to employ technology despite lacking digital trust:

> [Gregory Porumbescu on the relevance of digital trust] "So what if digital trust is declining — are we going to not bank online? Are we not going to pay our taxes online? What are the key takeaways for the government? I think there needs to be a stronger argument for just why this is relevant, considering that so much of our life is dictated by the internet right now, or we just use it for so much."

A systematic understanding of digital trust is essential for building digital trust and through this policy review, we have attempted to unpack the ambiguity and vagary of digital trust by approaching it as mechanical digital trust (i.e., trustworthy technologies) and relational digital trust (i.e., interpersonal interactions and individual differences). The interrelations between the two approaches were then discussed in the context of a trust ecosystem using e-government

as an illustrative case. In breaking down digital trust into specific dimensions, we aim to enhance policy accuracy and the efficacy of trust building initiatives across policymaking, research, and practice domains.

Beyond the explication of the dimensions of digital trust, there are three key takeaways from this policy review. First, emphasising the importance of digital literacy is crucial. Empowering individuals with digital literacy skills is crucial in addressing digital trust issues and ensuring informed decision-making in the digital realm:

> [Tammy Lin on focusing on digital literacy] “I don't think [there is a decline in digital trust] because I still receive fake information from really prominent people. It’s more like digital literacy is not growing among all kinds of people, only those who are more sensitive and more alert or more literate people will be more alert, then they will have lower trust. Others, I think they have higher trust because they are not literate, like, digital literacy, they’re not alert, they’re not sensitive, so they accept everything. That’s my observation. I don’t think the trust is reducing or growing. It really depends on the people, I think, and the context.”

The second takeaway is the evolutional nature of technology and the fluctuations in trust in technology. Just as the technologies of the day change over time, peoples’ trust of the technologies will also evolve:

> [Bill Dutton on phases of trust and distrust in technology] “The internet has a 20-year history or a 30-year history. That’s not a lot of time. A lot of media last more than one person’s lifetime and it’s very early days for the Internet and digital media. We’re in a stage where people are confused and worried, because it’s still new, I think.”

The final takeaway is that fostering digital trust in an ever-evolving digital landscape requires cooperation and shared responsibility among all stakeholders. This entails recognising the downsides of technology and striving to improve various dimensions that contribute to digital trust. It is crucial to actively promote the benefits of technology while minimising harm in order to address trust-related concerns. By working together, we can foster a climate of digital trust that benefits individuals, organisations, and society as a whole.

9 References

Accenture. (2014). *The four keys to digital trust* [Slideshare]. Retrieved 12 June 2023 from https://www.slideshare.net/OptimediaSpain/accenture-four-keys-digital-trust

Aiken, K. D. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science*, *34*(3), 308–323.

Al Mansoori, K. A., Sarabdeen, J., & Tchantchane, A. L. (2018). Investigating Emirati citizens' adoption of e-government services in Abu Dhabi using modified UTAUT model. *Information Technology & People*, *31*(2), 455–481.

Al-Aufi, A. S., Al-Harthi, I., AlHinai, Y., Al-Salti, Z., & Al-Badi, A. (2017). Citizens' perceptions of government's participatory use of social media. *Transforming Government: People, Process and Policy*, *11*(2), 174–194.

Al-Faries, A., Al-Khalifa, H., Al-Razgan, M., & Al-Duwais, M. (2013). Evaluating the accessibility and usability of top Saudi e-government services. *ICEGOV '13: Proceedings of the 7th International Conference on Theory and Practice of Electronic* Governance, 60–63.

AlAwadhi, S. (2021). Trust factors affecting the adoption of e-government for civic engagement. Proceedings from Electronic Government: 20th IFIP WG 8.5 International Conference, EGOV 2021, Granada, Spain, September 7–9, 229–244.

Alesina, A., & La Ferrara, E. (2002). Who trusts others? *Journal of Public Economics*, *85*(2), 207–234.

Allemand, M. (2008). Age differences in forgivingness: The role of future time perspective. *Journal of Research in Personality*, *42*(5), 1137–1147.

Almeida, F., Oliveira, J., & Cruz, J. (2011). Open standards and open source: enabling interoperability. *International Journal of Software Engineering & Applications (IJSEA)*, *2*(1), 1–11.

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). *The consumer-data opportunity and the privacy imperative*. Retrieved 6 December 2022 from https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Arcand, M., Nantel, J., Arles-Dufour, M., & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, *31*(5), 661–681.

Ayyash, M. M., Ahmad, K., & Singh, D. (2013). Investigating the effect of information systems factors on trust in e-government initiative adoption in Palestinian public sector. *Research Journal of Applied Sciences, Engineering and Technology*, *5*(15), 3865–3875.

Baier, A. (1986). Trust and antitrust. *Ethics*, *96*(2), 231–260.

Bandura, A., Freeman, W. H., & Lightsey, R. (1999). Self-efficacy: The exercise of control. *Journal of Cognitive Psychotherapy*, *13*, 158–166.

Bantourakis, M., & Manojlovic, M. (2023). *Why data is key to protecting kids online and ensuring the digital future we deserve*. Retrieved 13 June from

https://www.weforum.org/agenda/2023/03/why-data-is-key-to-safeguarding-children-online-and-ensuring-the-digital-future-we-deserve/

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, *69*(4), 133–152.

Baum, S., & Mahizhnan, A. (2015). Government-with-you: E-government in Singapore. In *Public affairs and administration: Concepts, methodologies, tools, and applications* (pp. 711–725). Hershey, Pennsylvania: GI Global.

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems*, *17*(2), 165–176.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3), 245–270.

Beldad, A., van der Geest, T., de Jong, M., & Steehouder, M. (2012). A cue or two and I'll trust you: Determinants of trust in government organizations in terms of their processing and usage of citizens' personal information disclosed online. *Government Information Quarterly*, *29*(1), 41–49.

Benlian, A., & Hess, T. (2011). The signaling role of IT features in influencing trust and participation in online communities. *International Journal of Electronic Commerce*, *15*(4), 7–56.

Bissell, K., Fox, J., LaSalle, R. M., & Cin, P. D. (2021). *State of cybersecurity resilience 2021*. https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Blank, G., & Dutton, W. H. (2012). Age and trust in the internet: The centrality of experience and attitudes toward technology in Britain. *Social Science Computer Review*, *30*(2), 135–151.

Blau, P. M. (1964). *Exchange and power in social life*. New York: J. Wiley.

Blind, P. K. (2007). Building trust in government in the twenty-first century: Review of literature and emerging issues. 7th Global Forum on Reinventing Government Building Trust in Government 26-29 June 2007, Vienna, Austria.

Boon, S. D., & Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In R. Hinde & J. Gorebel (Eds.), *Cooperation and Prosocial Behaviour* (pp. 190–211). Cambridge University Press.

Boyd, J. (2003). The rhetorical construction of trust online. *Communication Theory*, *13*(4), 392–410.

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too many Facebook “friends”? Content sharing and sociability versus the need for privacy in social network sites. *International Journal of Human-Computer Interaction*, *26*(11–12), 1006–1030.

Burt, R. S. (1992). *Structural holes: the social structure of competition*. Harvard University Press.

Business Insider Intelligence. (2020). *The 2020 digital trust report*. https://www.businessinsider.com/intelligence/digital-trust-enterprise-report-preview

Cabello-Hutt, T., Cabello, P., & Claro, M. (2018). Online opportunities and risks for children and adolescents: The role of digital skills, age, gender and parental mediation in Brazil. *New Media & Society*, *20*(7), 2411–2431.

Chakiri, H., El Mohajir, M., & Assem, N. (2020). A data warehouse hybrid design framework using domain ontologies for local good-governance assessment. *Transforming Government: People, Process and Policy*, *14*(2), 171–203.

Chatterjee, S., & Datta, P. (2008). Examining inefficiencies and consumer uncertainty in e-commerce. *Communications of the Association for Information Systems*, *22*(1), 29.

Chau, P. Y., Hu, P. J.-H., Lee, B. L., & Au, A. K. (2007). Examining customers' trust in online vendors and their dropout decisions: an empirical study. *Electronic Commerce Research and Applications*, *6*(2), 171–182.

Chellappa, R. K. (2008). Consumers' trust in electronic commerce transactions: the role of perceived privacy and perceived security [Manuscript submitted for publication].

Cheng, Y., & Chen, Z. F. (2021). Encountering misinformation online: Antecedents of trust and distrust and their impact on the intensity of Facebook use. *Online Information Review*, *45*(2), 372–388.

Cheshire, C., Antin, J., Cook, K. S., & Churchill, E. (2010). General and familiar trust in websites. *Knowledge, Technology & Policy*, *23*(3), 311–331.

Chew, H. E., & Soon, C. (2022, March 5). Rebuilding digital trust. *The Straits Times*. Retrieved 12 June from https://www.straitstimes.com/opinion/rebuilding-digital-trust

Christensen, T. O. M., & Lægreid, P. E. R. (2005). Trust in government: The relative importance of service satisfaction, political factors, and demography. *Public Performance & Management Review*, *28*(4), 487–511.

Chu, W., & Dyer, J. H. (2000). The determinants of trust in supplier-automaker relationships in the U.S., Japan, and Korea. *Journal of International Business Studies*, *31*(2), 259–285.

CIGI-Ipsos. (2019). *CIGI-Ipsos global survey on internet security and trust*. https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/

CISCO. (2022). *Cisco 2022 consumer privacy survey*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf

Coleman, J. S. (1988). Social capital in the creation of human capital. *American Journal of Sociology*, *94*, S95-S120.

Coleman, J. S. (1990). *Foundations of social theory*. Harvard University Press.

Colesca, S. E. (2009). Increasing e-trust: a solution to minimize risk in e-government adoption. *Journal of Applied Quantitative Methods*, *4*(1), 31.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology*, *92*(4), 909.

Connolly, R. (2007). The influence of technical skill on consumer trust in on-line shopping in Ireland. *International Journal of Business and Information*, *2*(1), 1–28.

Corbitt, B. J., Thanasankit, T., & Yi, H. (2003). Trust and e-commerce: a study of consumer perceptions. *Electronic Commerce Research and Applications*, *2*(3), 203–215.

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: Concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737–758.

Costa, A. C., Bijlsma-Frankema, K. M., & de Jong, B. A. (2009). The role of social capital on trust development and dynamics: Implications for cooperation, monitoring and team performance. Social Science Information, *48*(2), 199–228

Cyber Security Agency. (2021). *The Singapore Cybersecurity Strategy 2021*. https://www.csa.gov.sg/docs/default-source/csa/documents/publications/the-singapore-cybersecurity-strategy-2021.pdf

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319–340.

Deutsch, M. (1958). Trust and suspicion. *The Journal of Conflict Resolution*, *2*(4), 265–279.

Dobrygowsky, D., & Hoffman, W. (2018). *We need to build up "digital trust" in tech*. Retrieved 12 June from https://www.wired.com/story/we-need-to-build-up-digital-trust-in-tech/

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing*, *61*(2), 35–51.

Dutta, S., Dutton, W. H., & Law, G. (2010). The new internet world: A global perspective on freedom of expression, privacy, trust and security online. The Gobal Information Technology Report 2010-2011 – World Economic Forum in collaboration with INSEAD, comScore, and the Oxford Internet Institute, April 2011.

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an experience technology. *Information, Communication & Society*, *9*(4), 433–451. https://doi.org/10.1080/13691180600858606

Earp, J. B., & Baumer, D. (2003). Innovative web use to learn about consumer behavior and online privacy. *Communications of the ACM*, *46*(4), 81–83.

Edelman. (2020). *2020 Edelman Trust Barometer special report: Trust in technology*. https://www.edelman.com/sites/g/files/aatuss191/files/2020-02/2020%20Edelman%20Trust%20Barometer%20Tech%20Sector%20Report_1.pdf

Ermisch, J., & Gambetta, D. (2010). Do strong family ties inhibit trust? *Journal of Economic Behavior & Organization*, *75*(3), 365–376.

eSafety Commissioner. (n.d.). *About us*. https://www.esafety.gov.au/about-us/who-we-are

Everard, A., & Galletta, D. F. (2005). How presentation flaws affect perceived site quality, trust, and intention to purchase from an online store. *Journal of Management Information Systems*, *22*(3), 56–95.

Ferlander, S. (2007). The Importance of different forms of social capital for health. *Acta Sociologica*, *50*(2), 115–128.

Flavián, C., Guinalíu, M., & Gurrea, R. (2006). The role played by perceived usability, satisfaction and consumer trust on website loyalty. *Information & Management*, *43*(1), 1–14.

Fletcher School. (2021). *Digital intelligence dashboard Singapore*. Digital Planet. Retrieved 12 June 2023 from https://sites.tufts.edu/digitalplanet/files/2021/countrydashboards/Digital_Intelligence_Dashboard_SG.pdf

Fredrickson, B. L., & Carstensen, L. L. (1990). Choosing social partners: How old age and anticipated endings make people more selective. *Psychology and Aging*, *5*(3), 335–347.

Freitag, M., & TraunmÜLler, R. (2009). Spheres of trust: An empirical analysis of the foundations of particularised and generalised trust. *European Journal of Political Research*, *48*(6), 782–803.

Friedman, B., Khan Jr, P., & Howe, D. (2000). Trust online. *Communications of the ACM*, 43(12), 34–40.

Frost & Sullivan. (2018). *The Global State of Online Digital Trust*. Retrieved 12 June from https://docs.broadcom.com/doc/the-global-state-of-online-digital-trust

Fukuyama, F. (1995). *Trust: The social virtues and the creation of prosperity*. New York: Free Press.

Gallo, L. C., Smith, T. W., & Cox, C. M. (2006). Socioeconomic status, psychosocial processes, and perceived health: An interpersonal perspective. *Annals of Behavioral Medicine*, *31*(2), 109–119.

Gambetta, D. (1988). Can we trust trust? In D. Gambetta (Ed.), Trust: Making and breaking cooperative relations, electronic edition (pp. 213–237). University of Oxford.

Ganzaroli, A. (2002). Creating trust between local and global systems [Doctoral Thesis]. Erasmus University Rotterdam.

Gauzente, C. (2004). Web merchants' privacy and security statements: how reassuring are they for consumers? A two-sided approach. *Journal of Electronic Commerce Research*, *5*(3), 181–198.

GDPR.EU. (2016). *What is GDPR, the EU's new data protection law?* Retrieved 12 June 2023 from https://gdpr.eu/what-is-gdpr/

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega*, *28*(6), 725–737.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *33*(3), 38–53.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, 51–90.

Gilbert, D., Balestrini, P., & Littleboy, D. (2004). Barriers and benefits in the adoption of e-government. *The International Journal of Public Sector Management, 17,* 286–301.

Glanville, J. L., & Paxton, P. (2007). How do we learn to trust? A Confirmatory Tetrad Analysis of the sources of generalized trust. *Social Psychology Quarterly*, *70*(3), 230–242.

gov.uk. (2021). *Understanding and reporting online harms on your online platform*. Retrieved 12 June 2023 from https://www.gov.uk/guidance/understanding-and-reporting-online-harms-on-your-online-platform

GovTech Singapore. (2021a). *Annual survey on satisfaction with government digital services (businesses) — for 2020*. Retrieved 16 December 2022 from https://www.tech.gov.sg/digital-government-perception-survey-business-2020

GovTech Singapore. (2021b). *Annual survey on satisfaction with government digital services (citizens) — for 2020*. Retrieved 16 December 2022 from https://www.tech.gov.sg/digital-government-perception-survey-citizen-2020

GovTech Singapore. (n.d.). *Streamlining citizen services through digital identity*. Retrieved 13 June 2023 from https://www.tech.gov.sg/singapore-digital-government-journey/digital-identity/streamlining-citizen-services-through-digital-identity

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, *38*(12), 1371–1382.

Granovetter, M. (1992). Problems of explanation in economic sociology. *Networks and Organizations: Structure, Form, and Action* (pp. 25–56). Boston, Mass.: Harvard Business School Press.

Hampton-Sosa, W., & Koufaris, M. (2005). The effect of web site perceptions on initial trust in the owner company. *International Journal of Electronic Commerce*, *10*(1), 55–81.

Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is public trust in government associated with trust in e-government? *Social Science Computer Review*, *29*(2), 232–241.

Identity Theft Resource Center. (2022). *2021 annual data breach report*. https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf

ILNAS. (2017). *Digital trust in Internet of Things*. https://portail-qualite.public.lu/dam-assets/publications/normalisation/2017/ilnas-anec-ws-digital-trust-in-iot-30-03-2017-v1.pdf

IMD World Competitiveness Center. (2022). *World digital competitiveness ranking 2022*. https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

Infocomm Media Development Authority. (2017). *Annex A — Fact sheet on Singapore Quick Response Code (SGQR)*. Retrieved 12 June 2023 from https://www.imda.gov.sg/-/media/imda/files/about/media-releases/2018/annex-a--singapore-quick-response-code-sgqr.pdf

———. (2019a). *Annual survey on infocomm usage in households and by individuals*. https://www.imda.gov.sg/-/media/Imda/Files/Infocomm-Media-Landscape/Research-and-Statistics/Survey-Report/2019-HH-Public-Report_09032020.pdf

———. (2019b). *IMDA to strengthen Singapore's capabilities in digital trust through new national digital trust centre.* Retrieved 12 June 2023 from https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/

Insider Intelligence. (2022). *What most affects US social media users' decision to engage with ads/sponsored content on social media platforms?* Retrieved 13 June 2023 from https://www.insiderintelligence.com/chart/258336/what-most-affects-us-social-media-users-decision-engage-with-ads-sponsored-content-on-social-media-platforms-of-respondents-june-2021

IPSOS. (2022). *Trust in the internet*. https://www.ipsos.com/sites/default/files/ct/news/documents/2022-11/Trust%20in%20the%20Internet%2C%20Nov%202022.pdf

ISACA. (2022). *Digital trust: A modern day imperative*. https://www.isaca.org/resources/white-papers/digital-trust-a-modern-day-imperative

Jarvenpaa, S. L., & Grazioli, S. (1999). Surfing among sharks: How to gain trust in Cyberspace. *Financial Times, Mastering Information Management*, *7*, 2–3.

Jasiulewicz, A., Pietrzak, P., & Wyrzykowska, B. (2021). Trust and the digital economy: A framework for analysis. In *Trust, Organizations and the Digital Economy* (pp. 96–107). Routledge.

Johnson, K. (2021). *The movement to hold AI accountable gains steam*. Retrieved 12 June 2023 from https://www.wired.com/story/movement-hold-ai-accountable-gains-steam/

Jones-Jang, S. M., Mortensen, T., & Liu, J. (2021). Does media literacy help identification of fake news? Information literacy helps, but other literacies don't. *American Behavioral Scientist*, *65*(2), 371–388.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, *43*(2), 618–644.

Kalakota, R., & Whinston, B. (1997). *Electronic commerce: A manager's guide*. New Jersey: Addiso-WEsley Professional.

Karat, J. (1997). Evolving the scope of user-centered design. *Communications of the ACM*, *40*(7), 33–38.

Kardes, F. R., Fennis, B. M., Hirt, E. R., Tormala, Z. L., & Bullington, B. (2007). The role of the need for cognitive closure in the effectiveness of the disrupt-then-reframe influence technique. *Journal of Consumer Research*, *34*(3), 377–385.

Keefer, P., & Knack, S. (2005). *Social Capital, Social Norms and the New Institutional Economics*. In P. Keefer (Ed.), *Handbook of New Institutional Economics* (pp.701–725).

Khodyakov, D. (2007). Trust as a process: A three-dimensional approach. *Sociology*, *41*(1), 115–132.

Kim, D. J. (2008). Self-perception-based versus transference-based trust determinants in computer-mediated transactions: A cross-cultural comparison study. *Journal of Management Information Systems*, *24*(4), 13–45.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, *44*(2), 544–564.

Kim, D. J., Song, Y. I., Braynov, S. B., & Rao, H. R. (2005). A multidimensional trust formation model in B-to-C e-commerce: a conceptual framework and content

analyses of academia/practitioner perspectives. *Decision Support Systems*, *40*(2), 143–165.

Kim, S., & Lee, J. (2012). E-participation, transparency, and trust in local government. *Public Administration Review*, *72*(6), 819–828.

Koehn, D. (2003). The nature of and conditions for online trust. *Journal of Business Ethics*, *43*(1), 3–19.

Kożuch, B. (2021). The dimensions of trust in the digital era. *Trust, Organizations and the Digital Economy*, 15–26.

KPMG. (2017). *Crossing the line — staying on the right side of consumer privacy*. https://assets.kpmg/content/dam/kpmg/xx/pdf/2016/11/crossing-the-line.pdf

KPMG. (2021). *Corporate data responsibility*. https://advisory.kpmg.us/articles/2021/bridging-the-trust-chasm.html

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual Review of Psychology*, *50*, 569.

Kumar, N. (1996). The power of trust in manufacturer-retailer relationships. *Harvard Business Review*, *74*(6), 92.

Kumar, R., Sachan, A., & Mukherjee, A. (2018). Direct vs indirect e-government adoption: an exploratory study. *Digital Policy, Regulation and Governance*, 20(3), 149–162.

Kumaran, N., & Lugani, S. (2020). *Protecting against cyber threats during COVID-19 and beyond*. Retrieved 8 November 2022 from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

La Porte, T. M., Demchak, C. C., & De Jong, M. (2002). Democracy and bureaucracy in the age of the web: empirical findings and theoretical speculations. *Administration & Society*, *34*(4), 411–446.

Lang, F. R., & Carstensen, L. L. (2002). Time counts: Future time perspective, goals, and social relationships. *Psychology and Aging*, *17*(1), 125–139.

Lanier Jr, C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review*, *2008*, 1.

Lauer, T. W., & Deng, X. (2007). Building online trust through privacy practices. *International Journal of Information Security*, *6*(5), 323–331.

Law, N., Woo, D., de la Torre, J., & Wong, K. (2018). A global framework of reference on digital literacy skills for indicator 4.4. 2. *Information Paper No. 51*. UIS/2018/ICT/IP/51. UNESCO and UNESCO Institute for Statistics.

Lean, O. K., Zailani, S., Ramayah, T., & Fernando, Y. (2009). Factors influencing intention to use e-government services among citizens in Malaysia. *International Journal of Information Management*, *29*(6), 458–475.

Lee, A., & Levy, Y. (2014). The effect of information quality on trust in e-government systems' transformation. *Transforming Government: People, Process and Policy*, *8*(1).

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, *63*(4), 967–985.

Lippert, S. K. (2001). *An exploratory study into the relevance of trust in the context of information systems technology* [Doctoral Thesis]. George Washington University.

Livingstone, S., Ólafsson, K., Helsper, E. J., Lupiáñez-Villanueva, F., Veltri, G. A., & Folkvord, F. (2017). Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation. *Journal of Communication*, *67*(1), 82–105.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 94-107). London: Blackwell.

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, *31*(2), 111-–118.

Lynch, H., Bartley, R., Metcalf, J., Petroni, M., Ahuja, A., & David, S. L. (2016). *Building digital trust: The role of data ethics in the digital age* [Slideshare]. https://www.slideshare.net/AccentureTechnology/building-digital-trust-the-role-of-data-ethics-in-the-digital-age

Macy, M. W., & Skvoretz, J. (1998). The evolution of trust and cooperation between strangers: A computational model. *American Sociological Review*, 638–660.

MAGNA. (2022). *The person behind the data.* Retrieved 12 June 2023 from https://content.ketch.com/consumer-privacy-perspectives-study

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Mansoor, M. (2021). An interaction effect of perceived government response on COVID-19 and government agency's use of ICT in building trust among citizens of Pakistan. *Transforming Government: People, Process and Policy*, *15*(4), 693–707.

Marcial, D. E., & Launer, M. A. (2019). Towards the measurement of digital trust in the workplace: A proposed framework. *International Journal of Scientific Engineering and Science*, *3*(12), 1–7.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, *20*(3), 709–734.

McKinsey & Company. (2022). *Why digital trust truly matters*. https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters#/

McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, *6*(2), 35–59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, *13*(3), 334–359.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, *23*(3), 473–490.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology*, *27*(1), 415–444.

Meijer, A. (2013). Understanding the complex dynamics of transparency. *Public Administration Review*, *73*(3), 429–439.

Mensah, I. K., Luo, C., & Abu-Shanab, E. (2021). Citizen use of e-government services websites: A proposed e-government adoption recommendation model (EGARM). *International Journal of Electronic Government Research (IJEGR)*, *17*(2), 19–42.

Meta. (2022). *Meta reports third quarter 2022 results*. Retrieved 8 November 2022 from https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Third-Quarter-2022-Results/default.aspx

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155–179.

Microsoft. (2022). *Microsoft Responsible AI Standard, v2*. Retrieved 12 June 2023 from https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29.

Ministry of Communications and Information. (2022). *Sunlight AfA celebrates a year's work in tackling online harms*. Retrieved 12 June 2023 from https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2022/7/sunlight-afa-celebrates-a-year-work-in-tackling-online-harms

Mislove, A., Marcon, M., Gummadi, K., Druschel, P., Bhattacharjee, B., & ACM. (2007). Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* (pp.29–42).

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *Journal of Marketing*, *58*(3), 20–38.

Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International Journal of Bank Marketing*, 21(1), 5–15.

NIST. (2020). *Security and privacy controls for information systems and organizations*. Retrieved 12 June 2023 from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Norris, D. F., & Moon, M. J. (2005). Advancing e-government at the grassroots: Tortoise or hare? *Public Administration Review*, *65*(1), 64–75.

Öksüz, A., Walter, N., Distel, B., Räckers, M., & Becker, J. (2016). Trust in the information systems discipline. In *Trust and communication in a digitized world* (pp. 205–223). Springer.

Paliszkiewicz, J., & Chen, K. (2023). Building Digital Trust in Business. In *Trust and digital business* (pp. 3–11). US: Routledge.

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331–338.

Parent, M., Vandebeek, C. A., & Gemino, A. C. (2005). Building citizen trust through e-government. *Government Information Quarterly*, *22*(4), 720–736.

Porumbescu, G. A. (2016). Placing the effect? Gleaning insights into the relationship between citizens' use of e-government and trust in government. *Public Management Review*, *18*(10), 1504–1535.

Putnam, R., & Helliwell, J. F. (2007). Education and social capital. *Eastern Economic Journal*, *33*(1), 1–19.

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. Simon & Schuster.

Putnam, R. D., Leonardi, R., & Nanetti, R. (1993). *Making democracy work: Civic traditions in modern Italy*. Princeton University Press.

PwC. (2018). *The journey to digital trust*. Retrieved 12 June 2023 from https://www.pwc.co.uk/cyber-security/pdf/pwc-digital-trust-insights-survey.pdf

Raguraman, A. (2021). Nearly 470 people lose at least $8.5m in phishing scams involving OCBC Bank. *The Straits Times.* Retrieved 12 June 2023 from https://www.straitstimes.com/singapore/consumer/nearly-470-people-lose-at-least-85m-to-phishing-scam-involving-ocbc-bank

Ramaseshan, B., Yip, L. S., & Pae, J. H. (2006). Power, satisfaction, and relationship commitment in Chinese store–tenant relationship and their impact on performance. *Journal of Retailing*, *82*(1), 63–70.

Ren, Y., Kraut, R., & Kiesler, S. (2007). Applying common identity and bond theory to design of online communities. *Organization Studies*, *28*(3), 377–408.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *The Journal of Strategic Information Systems*, *11*(3), 271–295.

Rodríguez-de-Dios, I., van Oosten, J. M., & Igartua, J.-J. (2018). A study of the relationship between parental mediation and adolescents' digital skills, online risks and online opportunities. *Computers in Human Behavior*, *82*, 186–198.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality*, *35*(4), 651–665.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *The American Psychologist*, *26*(5), 443–452.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *The Academy of Management Review*, *23*(3), 393–404.

Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, *13*(1), 12–24.

Sainty, K. (2022). *Australia: The scope of the Online Safety Act*. Retrieved 13 June from dataguidance.com/opinion/australia-scope-online-safety-act

Salam, A. F., Iyer, L., Palvia, P., & Singh, R. (2005). Trust in e-commerce. *Communications of the ACM*, *48*(2), 72–77.

Sawhney, M., & Zabin, J. (2002). Managing and measuring relational equity in the network economy. *Journal of the Academy of Marketing Science*, *30*(4), 313–332.

SGTech. (2022a). *Digital trust unlocking the next wave of growth in the digital economy.* Retrieved 12 June from: https://globalfutureseries.com/digitrust/wp/wp-content/uploads/2022/10/Digital_Trust_White_Paper_Unlocking_the_Next_Wave_of_Growth_in_the_Digital_Economy_FINAL_lowres.pdf

SGTech. (October 28, 2022b). *SGTech hosts the world's first global forum on digital trust*. Retrieved 13 June from https://www.sgtech.org.sg/articleDetails/VTJGc2RHVmtYMThpVHFXSEQ5dFNNQldUWk9CRnZHVENwWlZOQzgvcjk3az0=

Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: A stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems*, *11*(3), 325–344.

Shapiro, S. P. (1987). The social control of impersonal trust. *American journal of sociology*, *93*(3), 623-658.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, *19*(1), 62-73.

Shelat, B., & Egger, F. N. (2002). What makes people trust online gambling sites? CHI'02 Extended Abstracts on Human Factors in Computing Systems,

Shell, M. A., & Buell, R. W. (2019). Why anxious customers prefer human customer service. Retrieved 13 June from https://hbr.org/2019/04/why-anxious-customers-prefer-human-customer-service

Shen, F., & Tsui, L. (2016). Public opinion toward Internet freedom in Asia: A survey of Internet users from 11 jurisdictions. *Berkman Center Research Publication*, 2016-8.

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys (CSUR)*, *45*(4), 1–33.

Singapore Business Review. (2022). *"I trust you": Singaporeans trust gov't to keep info private*. Retrieved 13 June from https://sbr.com.sg/information-technology/news/i-trust-you-singaporeans-trust-govt-keep-info-private

Singapore Police Force. (2023). Annual scams and cybercrime brief 2022 [Press release]. https://www.police.gov.sg/-/media/Spf/PNR/2023/Feb/Police-News-Release---Annual-Scams-and-Cybercrime-Brief-2022.ashx

Singh, A., & Malhotra, V. (2022). *The cyber trust landscape report 2022*. Retrieved 13 June from https://mkai.org/the-cyber-trust-landscape-report-2022/

Sitkin, S. B., & Roth, N. L. (1993). Explaining the limited effectiveness of legalistic "remedies" for trust/distrust. *Organization Science*, *4*(3), 367–392.

Soares, D. d. S., & Amaral, L. (2014). Reflections on the concept of interoperability in information systems. In *Proceedings of the 16th International Conference on Enterprise Information Systems (ICEIS-2014)* (pp. 331–339). SciTech Press.

Song, C., & Lee, J. (2016). Citizens' use of social media in government, perceived transparency, and trust in government. *Public Performance & Management Review*, *39*(2), 430–453.

Soon, C., Mak, A. R., & Chew, H. E. (2023). Digital sovereignty: State action and implications for Singapore. National University of Singapore Centre for Trusted Internet and Community, and Institute of Policy Studies.

Srivastava, S. C., & Teo, T. S. (2009). Citizen trust development for e-government adoption and usage: Insights from young adults in Singapore. *Communications of the Association for Information Systems*, *25*(1), 31.

Sternstein, A. (2010). *Study links online transparency efforts, trust in government*. Retrieved 15 December 2022 from https://www.nextgov.com/cxo-briefing/2010/02/study-links-online-transparency-efforts-trust-in-government/45965/

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, *7*(3), 135–161.

Tan, S. J., & Tambyah, S. K. (2011). Generalized trust and trust in institutions in Confucian Asia. *Social Indicators Research*, *103*(3), 357–377.

Tsai, W., & Ghoshal, S. (1998). Social capital and value creation: The role of intrafirm networks. *Academy of Management Journal*, *41*(4), 464–476. https://doi.org/10.2307/257085

United Nations. (n.d.). *United Nations competencies for the future*. Retrieved 12 June 2023 from https://careers.un.org/lbw/attachments/competencies_booklet_en.pdf

Vissenberg, J., d'Haenens, L., & Livingstone, S. (2022). Digital literacy and online resilience as facilitators of young people's well-being? *European Psychologist*, *27*(2), 76–85.

Vu, K.-P. L., Chambers, V., Garcia, F. P., Creekmur, B., Sulaitis, J., Nelson, D., Pierce, R., & Proctor, R. W. (2007). How users read and comprehend privacy policies. Symposium on Human Interface 2007, held as part of HCI International 2007, Beijing, China, July 22–27.

Walczuch, R., & Lundgren, H. (2004). Psychological antecedents of institution-based consumer trust in e-retailing. *Information & Management*, *42*(1), 159–177.

Walther, J. B., & Bunz, U. (2005). The rules of virtual groups: Trust, liking, and performance in computer-mediated communication. *Journal of Communication*, *55*(4), 828–846.

Wang, Y. (2017). Antecedents of social network trust in SNS usage: The moderating role of offline familiarity. *Social Networking*, *6*(2), 107–134.

Wangpipatwong, S., Chutimaskul, W., & Papasratorn, B. (2005). Factors influencing the adoption of Thai eGovernment websites: information quality and system quality approach. Proceedings of Fourth International Conference on eBusiness, Bangkok, Thailand, November 2005.

Wardle, C., & Derakhshan, H. (2017). *One year on, we're still not recognizing the complexity of information disorder online*. Retrieved 12 June 2023 from Ahttps://firstdraftnews.org/articles/coe_infodisorder/

WEF. (2021). *Advancing digital safety: A framework to align global action.* Retrieved 12 June 2023 from https://www3.weforum.org/docs/WEF_Advancing_Digital_Safety_A_Framework_to_Align_Global_Action_2021.pdf

WEF. (2022). *Earning digital trust: Decision-making for trustworthy technologies*. . Retrieved 12 June 2023 from https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

WEF. (n.d.-a). *Digital Trust — About.* Retrieved 12 June 2023 from https://initiatives.weforum.org/digital-trust/about

WEF. (n.d.-b). *Why trust in the digital economy is under threat.* . Retrieved 8 November 2022 from https://reports.weforum.org/digital-transformation/building-trust-in-the-digital-economy/

Wei, R., Lo, V.-H., & Lu, H.-Y. (2010). The third-person effect of tainted food product recall news: Examining the role of credibility, attention, and elaboration for college students in Taiwan. *Journalism & Mass Communication Quarterly*, *87*(3-4), 598–614.

Welch, E. W., Hinnant, C. C., & Moon, M. J. (2005). Linking citizen satisfaction with e-government and trust in government. *Journal of Public Administration Research and Theory*, *15*(3), 371–391.

Welch, M. R., Sikkink, D., & Loveland, M. T. (2007). The radius of trust: Religion, social embeddedness and trust in strangers. *Social Forces*, *86*(1), 23–46.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review*, *64*(1), 15–27.

White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters*, *19*, 39-50.

Williamson, D. A. (2022). *User trust in social platforms is falling, according to our new study*. Retrieved 8 November 2022 from https://www.insiderintelligence.com/content/user-trust-social-platforms-falling-according-our-new-study

Williamson, O. E. (1993). Calculativeness, trust, and economic organization. *The Journal of Law and Economics*, *36*(1, Part 2), 453–486.

Worchel, P. (1979). Trust and distrust. In W. G., Austin & S. Worchel (Eds.), *The Social Psychology of Intergroup Relations* (pp. 174–187). Belmont, CA: Wadsworth.

Wu, J.-J., Chen, Y.-H., & Chung, Y.-S. (2010). Trust factors influencing virtual community members: A study of transaction communities. *Journal of Business Research*, *63*(9–10), 1025–1032.

Wu, J.-J., & Tsang, A. S. (2008). Factors affecting members' trust belief and behaviour intention in virtual communities. *Behaviour & Information Technology*, *27*(2), 115–125.

Zahedi, F. M., & Song, J. (2008). Dynamics of trust revision: Using health infomediaries. *Journal of Management Information Systems*, *24*(4), 225–248.

Zheng, Y., & Schachter, H. L. (2017). Explaining citizens' e-participation use: The role of perceived advantages. *Public Organization Review*, *17*(3), 409–428.

Ziegler, C.-N., & Golbeck, J. (2007). Investigating interactions of trust and interest similarity. *Decision Support Systems*, *43*(2), 460–475.

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840–1920. *Research in Organizational Behavior*, 8, 53–111.

10 Appendix: Expert Interview Guide

- Is digital trust a new phenomenon? How do we think about digital trust? How do you unpack the concept?
- What theories can we bring to bear to understand digital trust?
- What are the levels of analysis for digital trust? Where in society is digital trust located?
- [On drivers and erodents] What are the drivers of digital trust and what erodes digital trust?
- [On measurement] How do we measure digital trust? What are good ways of measuring digital trust? How do we know that digital trust has increased in society? What about indices (or global indices) of digital trust?
- [On application] The World Economic Forum recently started talking about the need to rebuild digital trust. Is there really a decline in digital trust? If so, what can policymakers do to restore the deficit in digital trust? How do policymakers and leaders “move the needle” on digital trust?
- Can you share with us any of your works related to the topic of digital trust?