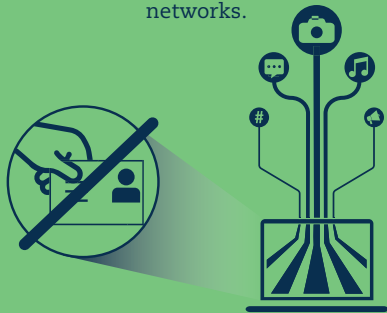


Chapter 7

STRENGTHENING TRUST

7. STRENGTHENING TRUST

Almost **30%** of Internet users **mistrust** social and professional networks.



✔ Address digital security, privacy and consumer protection concerns to improve trust.

One in four Internet users in the European Union is **concerned about payment security**.

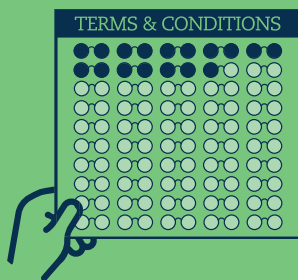


✔ Empower everyone to assess and better manage digital security risk.

TRUST



Only **17%** of peer platform users **read terms and conditions** in full.



✔ Design and implement more effective measures to protect consumers online.

A majority of **privacy measures** aims to raise awareness and **empower individuals**.



✔ Develop and implement a national privacy strategy with a whole-of-society perspective.

STRENGTHENING TRUST: WHAT MATTERS MOST FOR POLICY?

Adopt a risk management approach to ensuring trust

- Use risk management as a framework to develop policies to increase trust, including to assess and manage risks related to technologies, data and cross-border flows.
- Help small and medium-sized enterprises (SMEs) realise digital opportunities by increasing awareness and promoting good risk management practices through public and private efforts.

Develop strong, inclusive and interoperable privacy frameworks

- Privacy frameworks enable the free flow of personal data, spurring growth and social prosperity. Measures to increase transparency on the purpose and use of personal data collections and to enhance user access and control over their data are needed. Technological solutions can help increase trust through “privacy by design”.
- National privacy policies should be supported at the highest levels of government and take a whole-of-society perspective. More than half of privacy measures across OECD countries aim to raise awareness and empower individuals.
- Encourage interoperability of privacy frameworks across jurisdictions, including through national privacy strategies and other practical approaches.

Manage digital security risk rather than trying to eliminate it

- Digital security concerns, including malicious interference, are rising, and hold back almost 30% of Internet users from providing personal information to online social and professional networks. In addition, one in four Internet users in the European Union is concerned about payment security.
- Digital security needs to be a strategic priority for individuals, firms and governments, not a technical question. Managing digital security risk is the responsibility of everyone online.

Protect consumers as the online and offline worlds converge

- Digital consumers face challenges related to information disclosure, misleading and unfair commercial practices, confirmation and payment, fraud and identity theft, product safety, and dispute resolution and redress, including when using connected devices where offline and online experiences are blurring.
- Terms and conditions are not effective to communicate important information to consumers. For example, only 17% of people read the terms and conditions of peer platforms (such as Airbnb and BlaBlaCar) in full. Other approaches are needed to protect consumers online.

To fully embrace and benefit from digital transformation, individuals, firms and governments need to be confident that engaging in the digital environment to conduct their social and economic activities will bring more benefits than downsides. Such downsides can arise from various sources of uncertainties affecting digital technologies, data and cross-border flows. Many are related to potential digital security incidents (e.g. breaches of availability, integrity or confidentiality of data, systems or networks). Other downsides are related to information asymmetries, power imbalances or jurisdictional challenges exacerbated by the digital environment. These may translate into breaches of laws and regulations such as privacy, consumer protection or product safety, intended to reduce these imbalances and challenges. To ensure trust, it is critical to mitigate as much as possible such uncertainties.

Adopt a risk management approach to ensuring trust

The consequences of undesirable events, for example the theft of business assets or of an individual's identity, or the misuse of personal data, can affect all actors' reputation, finances, freedom, autonomy, health, well-being, safety, competitiveness or efficiency, and ultimately limit their willingness to fully engage in the digital environment. They can also affect the functioning of our society as critical infrastructure and essential services such as energy, finance and transport can be disrupted by digital security incidents.

In practice, the most effective way to deal with uncertainties is to manage digital risks. Because uncertainties cannot be entirely eliminated, some degree of risk has to be accepted. In other words, digital risk needs to be reduced to an acceptable level in light of the objectives and benefits to be achieved. This requires learning to assess risks and to manage them, which eventually includes deciding whether to accept, reduce, transfer or avoid risk, the latter by not engaging in digital activities.

7.1. What is trust?

Trust can be considered in many facets of life – trust in political institutions, government, statistics, the rule of law (institutional trust) or trust in other people (interpersonal trust) (see Chapter 6). While there is no universally agreed definition of trust, the OECD has broadly defined trust as “a person's belief that another person or institution will act consistently with their expectations of positive behaviour”, and has contributed to its better measurement through guidelines for national statistical offices (OECD, 2017^[1]) and through experimental work (Murtin et al., 2018^[2]).

Digital transformation adds a new dimension to the concept of trust for individuals, societies and the economy. This chapter addresses trust from the perspective of uncertainties and interdependences (Mayer, Davis and Schoorman, 1995^[3]) because digital environments encapsulate these factors. Trust in digital environments depends on the context and varies with what is at stake, including opportunities and challenges.

From an individuals' point of view, trust in the digital age is about the willingness to risk time, money and disclosure of personal data to engage in commercial and social activities, and to become vulnerable if a purchase goes wrong or if their data are stolen or if they are used to monitor their behaviour, to discriminate against them or to violate their privacy. From an organisations' point of view, trust is also about accepting a certain level of risk resulting from possible digital security, privacy, consumer protection or other incidents, to benefit from digital transformation. Trust is therefore a key condition to fully realise the potential growth and social progress in the digital age.

Digital risk management applies to individuals as well as organisations, from small businesses to large firms to public entities. All actors share some responsibility to manage the digital risks of their activities according to their roles, ability to act and the context, and they need to be equipped with the right skills to do so. As risk is a cross-boundary, cross-sector and multi-stakeholder issue, digital risk management provides a common reference framework for different policy communities to consider trust policies in an integrated and holistic manner, building on the fundamental components of a risk management cycle. These components include:

- establishing the objectives and the context of an activity and determining the acceptable level of risk in light of the expected benefits
- assessing risk by identifying risk factors, and evaluating the likelihood and severity of risk occurrence
- treating risk, including through accepting some, reducing it to an acceptable level through appropriate measures, sharing or transferring some, and/or avoiding some altogether
- monitoring and reviewing on an ongoing basis the risk management cycle to adapt it to a constantly changing environment.

Policies that foster digital risk management are crucial to increase trust and enable individuals and organisations to maximise their economic and social objectives. Risk management practices are likely to differ according to whether the objective is digital security, privacy, consumer protection or product safety, but policies need to account for interrelations between different categories of risks. Any measures to manage digital risk should be appropriate to and commensurate with the risk and the objectives at stake for the actors concerned. Measures that may be appropriate for an individual may not be the same for a large private firm, even though both actors may pursue the same objective.

Among private sector firms, start-ups and SMEs merit particular attention from policy makers, not only given their crucial role for the economy, but also in view of limited capacity to sustain major incidents and manage digital risk effectively. SMEs, and early-stage start-ups in particular, are critical to economic growth and they contribute to competition, innovation and job creation. However, they also face distinct challenges in managing digital risk. For example, a digital security incident that results in a loss of consumer trust, damage to reputation or a drop in revenue, may be more damaging for SMEs than for larger firms because SMEs are more likely to find it difficult to weather a temporary loss of revenue.

Typically, SMEs also lack the awareness, resources and expertise to effectively assess and manage risk. On the positive side, awareness of digital risk and robust risk management practices may bring them competitive advantage when seeking partnership opportunities with larger organisations. To help SMEs realise these opportunities, and to avoid that unmanaged risks from putting an SME and/or its business partner(s) in danger, it is essential to increase awareness and promote good practices.

Develop strong, inclusive and interoperable privacy frameworks

As digital transformation progresses, privacy, and the protection of personal data in particular, is emerging as an ever more critical influence on trust. Personal data have come to play an increasingly important role in our economies, societies and everyday lives, and new technologies and responsible data use are yielding great societal and economic benefits. At the same time, the abundance of personal data gathered, processed and exchanged has elevated the risks to individuals' privacy.

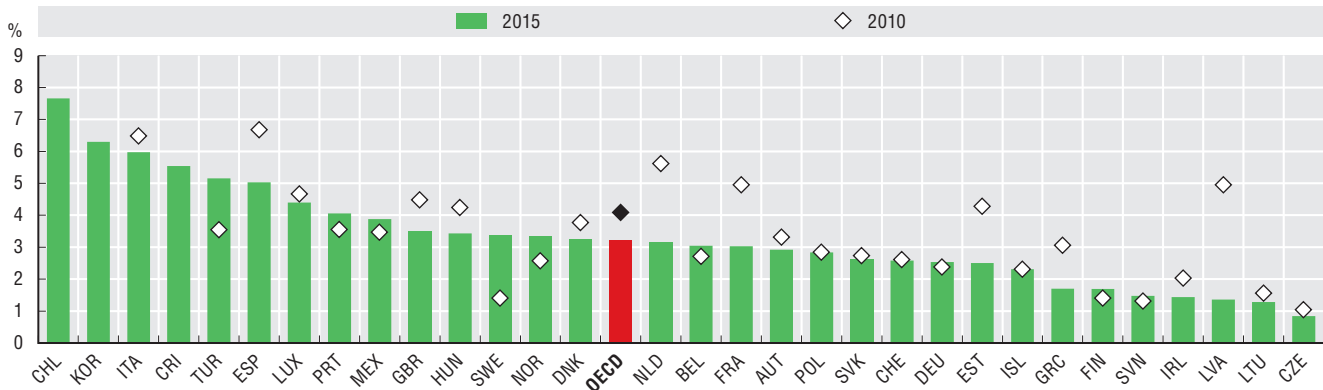
As firms, Internet service providers and governments increasingly collect and store personal data, privacy risks increase. About 3% of individuals on average in OECD countries reported experiencing a privacy violation in the past three months (Figure 7.1), although large variation exists across countries. In Chile, for example, about 7.5% of individuals reported a privacy violation, whereas in the Czech Republic the share was less than 1%. Personal data breaches are a major source of privacy violations, and digital technologies are increasingly being used to derive personal data by matching and “mining” datasets (OECD, 2017^[4]).

Personal data are being increasingly used in ways unanticipated at the time of collection, including in ways that allow sensitive information to come to light or to link supposedly anonymous data to specific individuals. With the growth in use and value of data, personal data breaches have become more common (OECD, 2017^[4]). These risks implicate not only the individuals concerned, but the core values and principles which privacy and personal data protection seek to promote, including individual autonomy, equality and free speech, which may have a broader impact on society as a whole. Privacy and personal data risks therefore need to be better managed to provide effective safeguards.

7. STRENGTHENING TRUST

7.1. Privacy violations vary considerably across countries

Individuals who experienced privacy violations, as a percentage of Internet users, 2015



Note: See Chapter notes.¹

Source: OECD (2019^[5]), *Measuring the Digital Transformation*, <https://dx.doi.org/10.1787/9789264311992-en>, based on OECD^[6], *ICT Access and Usage by Households and Individuals* (database), <http://oe.cd/hhind> (accessed September 2018).

StatLink <https://doi.org/10.1787/888933915411>

Privacy is not only a recognised fundamental value that merits protection, but a condition for the free flow of personal data across organisations and borders, and with it data-driven innovation, economic growth and social prosperity (OECD, 2016^[7]). Individuals, at home and on the job, share more personal data today than ever before – willingly, on social networks and elsewhere, but also unknowingly, through web-browsing tracking or smartphones. As a result, more than half of privacy measures across OECD countries aim to raise awareness and empower individuals (OECD, forthcoming^[8]). At the same time, individuals seek more assurance and control of the way their data are handled: they want to know if and what personal data about them are collected and stored, how they are used, and whether they can delete or correct data, or control any secondary uses.

In other words, individuals want to know whom they can trust with their data. Measures to increase transparency on the purposes and uses of personal data collections and to enhance user access and control over their data are particularly relevant to trust in the digital age. Technological advances can help increase trust through “privacy by design” processes whereby privacy implications are considered at the initial design phase of a product or service rather than as an afterthought. This may enable privacy-protective approaches to be embedded or coded in technologies, or help minimise personal data collection from the start. For example, encryption can play an important role for privacy as mobile devices and the Internet of Things (IoT) expand (OECD, 2017^[4]). Another response to privacy concerns may be the re-decentralisation of the web, a set of technological innovations that enable the distribution of personal data storage among Internet users themselves instead of its centralisation in a small number of companies.

While technology can play a positive role to help protect privacy and personal data, domestically there is a need for national data strategies, supported at the highest levels of government, that incorporate a whole-of-society perspective to strike the right balance between various individual and collective interests. Such strategies would provide clear direction to reap the social and economic benefits of enhanced reuse and sharing of data while addressing individuals’ and organisations’ concerns about the protection of privacy and personal data, and intellectual property rights. They would also facilitate interoperability of national frameworks and thus the free flow of data.

Towards interoperable privacy and data protection frameworks

While countries apply different privacy frameworks, they are largely pursuing the same outcomes, and frequently use similar approaches, as demonstrated by agreement on high-level guiding principles and good practices or legislation. The need to develop mechanisms that foster interoperability among data protection and privacy frameworks is also well-recognised (OECD, 2016^[7]; OECD, 2013^[9]). While interoperability provisions should be a characteristic of national privacy strategies, most countries across the OECD have yet to implement national privacy strategies (OECD, 2017^[4]), and other mechanisms to ensure interoperability can be identified.

Regional convergence and harmonisation of privacy frameworks

Instruments with a harmonising effect include the recently updated Convention 108 of the Council of Europe which binds 47 Council of Europe member states and is also open to non-members. Another example is the European Union's General Data Protection Regulation (GDPR), which harmonises data protection laws of all countries in the European Economic Area. Non-binding arrangements can also encourage convergence of privacy laws and facilitate privacy-respecting data flows. The Asia-Pacific Economic Cooperation (APEC) organisation has implemented a voluntary but enforceable system of Cross-Border Privacy Rules (CBPR), through which participating APEC economies work to lift the overall standard of privacy across the region. Approaches differ: for example, the APEC CBPR system establishes baseline privacy standards without changing domestic laws, while the EU GDPR harmonises laws through a directly applicable regulation.

Recognition of “equivalency” or “adequacy” of privacy measures

National authorities responsible for data and privacy protection can certify that other countries have principles that are adequate or equivalent to the protection afforded under domestic privacy regimes. For example, Article 45 of the EU GDPR enables flows of personal data from the European Union to third-party countries that have been deemed adequate, such as Israel and New Zealand. Other types of measures include model contracts, binding corporate rules for multinationals, and certification mechanisms to enable cross-border data flows along with enforceable protections for individuals whose data are transferred. One example of the latter mechanism is the US-EU Privacy Shield, which enables participating companies to transfer data between the two economic areas after making an enforceable commitment to comply with a set of principles aligned with EU data protection requirements.

Cross-border co-operation between privacy enforcement authorities

Mutually agreed upon high-level principles, such as those in the 2011 *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (OECD, 2007^[23]), can help ensure that privacy enforcement authorities align in safeguarding the personal information of individuals no matter where it is located. Participation in fora such as the Global Privacy Enforcement Network, which enables information sharing and co-operation and has also led to some joint initiatives, or bilateral co-operation between privacy enforcement authorities, is also useful to increasing cross-border co-operation. Ensuring the effectiveness of interoperability mechanisms also highlights the importance of co-operation and cross-border enforcement. For example, for an economy to participate in the APEC CBPR mechanism it must also commit to APEC's framework for enforcement co-operation. Other forms of co-operation can include memoranda of understanding and information-sharing agreements (Casalini and López González, 2019^[8]).

Regional trade agreements

Countries are also beginning to address data flow issues in bilateral or regional trade agreements with privacy-related provisions, typically to enable cross-border data flows. For example, the United States-Mexico-Canada Agreement (Article 19.8) – which has not yet been ratified by legislatures – references the adoption or maintenance of a legal framework that provides for the protection of personal information, while mentioning that no party should restrict the cross-border transfer of information subject to limited exceptions for legitimate public policy objectives (Article 19.11) (Casalini and López González, 2019^[10]).

Measures for companies and entities in countries that do not recognise each other's data protection systems

The GDPR, which includes mechanisms for multinational enterprises to implement “binding corporate rules” on all affiliates to enable transfers of data between them, even if the sub-entities are based in countries that have not forged a specific mechanism or agreement, is a practical example of how privacy rules can work for countries that do not recognise each other's data protection laws. Similarly, some privacy enforcement authorities have developed standard contractual clauses that can be used in any contract or agreement mediating transfers of data between entities in countries that do not recognise each other's data protection or privacy arrangements. However, some firms believe these clauses carry onerous obligations and can lead to high administrative costs (Casalini and López González, 2019^[10]).

Manage digital security risk rather than trying to eliminate it

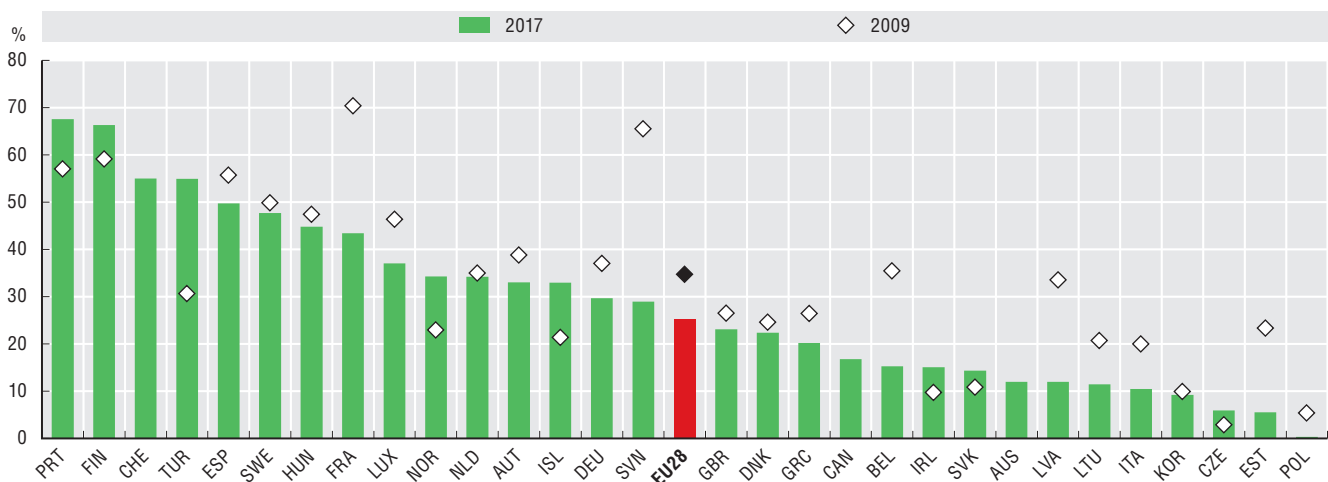
One important issue inherent to digital transformation is the need for resilience and better security to mitigate possible disruption of economic and social activities by digital security incidents. Digital security incidents take advantage of the global nature of the Internet to rapidly spread across jurisdictional, organisational and sectoral boundaries, as demonstrated by the recent Wannacry, NotPetya and Dyn attacks. Digital security incidents can disrupt the activities of all businesses, both SMEs and larger firms, governments and individuals, and generate financial and reputational harm. For example, NotPetya caused a temporary production shutdown at several global companies (e.g. Merck) which had to borrow doses of its vaccines from the US Center for Disease Control and Prevention stockpile to fulfil customer orders, reducing the company's third-quarter sales by USD 240 million (Merck, 2017^[11]; Hufford and Loftus, 2017^[12]).

Incidents can also cause physical damage, as demonstrated by a digital security incident that caused electricity service outages in Ukraine affecting approximately 225 000 customers in 2015 (NCCIC, 2016^[13]; Popescu and Secieru, 2018^[14]). Such incidents could evolve into large-scale crises affecting infrastructures critical to the functioning of the economy and society such as finance, energy, transport and essential government services. In addition to such catastrophic scenarios, digital security incidents can also have subtle but long-term negative effects by undermining trust in the digital environment, limiting innovation, slowing down the adoption of new technologies and hampering digital transformation and its related benefits.

The risk of digital security incidents grows as digital transformation deepens. Digital security concerns hold back almost 30% of Internet users from providing personal information to online social and professional networks (OECD, 2017^[4]). Payment security and privacy concerns remain persistent in many countries, with more than half of Internet users in Portugal (68%), Finland (66%), Switzerland (55%) and Turkey (55%) reporting such concerns in 2017 (Figure 7.2). Individuals in Poland (less than 1%), Estonia (6%), the Czech Republic (6%) and Korea (9%) were the least concerned about payment security and privacy during that period.

7.2. Payment security and privacy concerns remain prevalent in many countries

Individuals who did not buy online for payment security or privacy concerns, as a percentage of Internet users who ordered goods or services over the Internet more than a year ago or who never did, 2017



Note: See Chapter notes.²

Source: OECD calculations based on Eurostat^[15], *Digital Economy and Society Statistics* (database), <https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database>; national sources (accessed December 2018).

StatLink <https://doi.org/10.1787/888933914917>

Given that it is impossible to create an entirely safe and secure digital environment, businesses, other organisations and individuals always take some security risk when deciding to go digital. They should be thus encouraged to understand how to manage risk in a manner that does not reduce the economic and social opportunities of using digital technologies. This can include, for example, the implementation

of security standards (e.g. ISO 27000 series) to increase resilience and maintain business continuity by mitigating the consequences of potential security incidents. Because all stakeholders are interdependent in the digital environment, as well as across borders, it is key to foster partnerships among them to help reduce risk and promote good risk management practices, in particular through information sharing about threats, vulnerabilities, incidents and risk management practices, including for SMEs.

Public policies to foster digital security can play an important role in creating the conditions for organisations to adopt digital security risk management frameworks, for firms to develop less vulnerable and more secure technologies, and for individuals to better understand risks and use digital devices more responsibly. Public policies can also address the growing digital security skills shortage affecting both technical security experts and business managers, encourage digital security innovation and help foster a vibrant digital security industry. Cyber insurance can be an important element of managing risk by enabling the transfer of some digital security risk and creating incentives for better risk management practices.

Digital security and resilience of critical infrastructure and services that are essential for the functioning of our economies and societies are a particularly important aspect of digital security policy, at the crossroads of economic prosperity and national security. Digital transformation significantly increases the interdependencies and complexity of these crucial systems, and the risk of systemic failures cascading across sectors and borders. Governments must adopt policies to support and encourage critical infrastructure and services operators to strengthen their digital security. In doing so, they need to enable them to make the most of digital transformation, including through the adoption of technologies such as IoT, artificial intelligence, big data and blockchain, and to take into account existing sector-specific market, regulatory and cultural specificities. While critical infrastructure and essential services often rely on large and often private sector operators, digital transformation also empowers SMEs to take part in essential services' value chains (OECD, forthcoming^[16]).

One important challenge of digital transformation across the finance, energy and transportation sectors is the increasing role taken on by smaller actors such as SMEs, which extends digital security risks beyond the realm of large central players such as banks or electricity companies. Such SMEs include start-ups offering innovative payment systems, blockchain-based energy trading technologies or mobility services in the area of transport. Besides start-ups, well-established SMEs involved in providing essential services play an increasingly important role in managing digital security risk to mitigate risks to larger firms in their value chains.

Digital security is a multifaceted policy area that includes issues related to economic and social prosperity, technology and criminal law enforcement, as well as national and international security. From the economic and social perspective, digital security risk has traditionally been approached as a technical problem calling for technical solutions, but the changing nature and scale of digital security risk is driving governments to re-evaluate their strategies in order to call for a cultural change in this area.

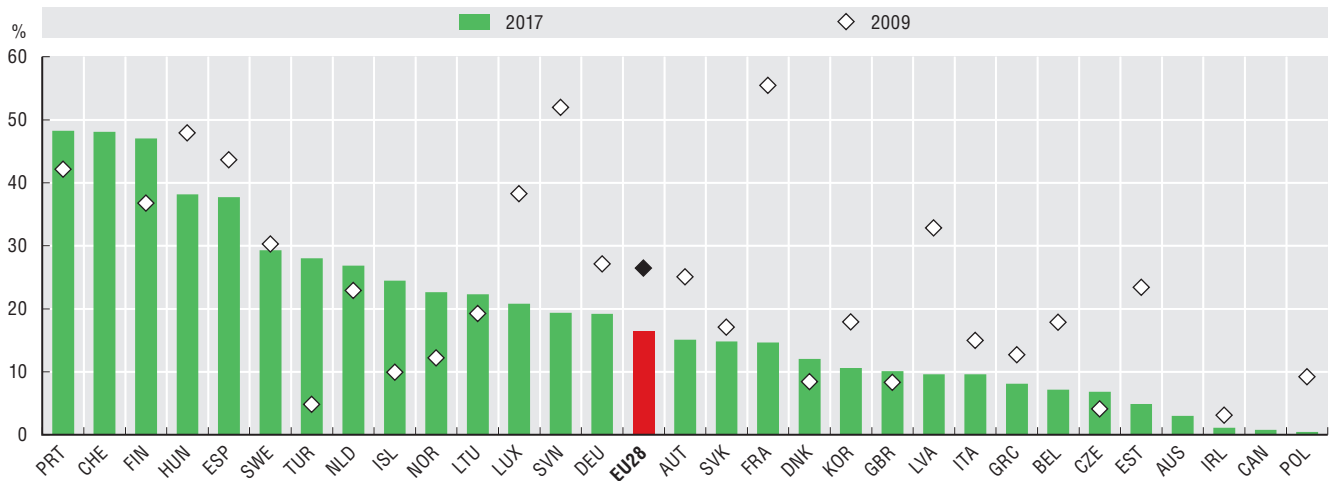
Protect consumers as the online and offline worlds converge

Protecting consumers in the digital environment is another essential aspect of ensuring trust, whether in e-commerce or in the use of new technologies like IoT (see Box 7.2). It opens up possibilities for new customers and markets, bringing broader economic benefits as well. Establishing a flourishing e-commerce marketplace requires more than broadband infrastructure, hosting and payment facilities, and specialised software. It requires a willingness on the part of consumers to overcome doubts about transacting at a distance where goods cannot be examined in advance, fears about the risks of entering payment details online, and concerns about whether there can be remedies or redress or if something goes wrong.

While consumer protection concerns about receiving or returning goods, complaint or redress have on average decreased over the past decade, they still remain important (Figure 7.3). Such concerns were the highest in Portugal (48%), Switzerland (48%), Finland (47%) and Hungary (38%). In contrast, less than 1% of Internet users in Poland and Canada shared these consumer protection concerns, which were also low in Ireland (1%) and Australia (3%).

7.3. Goods ordered online still raise consumer protection concerns for many people

Individuals who did not buy online due to concerns about receiving or returning goods, complaint or redress, as a percentage of Internet users who ordered goods or services over the Internet more than a year ago or who never did, 2017



Note: See Chapter notes.³

Source: OECD calculations based on Eurostat^[15], *Digital Economy and Society Statistics* (database), <https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database>; national sources (accessed December 2018).

StatLink <https://doi.org/10.1787/888933914936>

Concerns have also been raised over a growing range of non-compliant and unsafe products, which are available for sale online domestically and internationally, while being prohibited from sale or recalled from the market. As part of its annual global awareness campaigns on consumer product safety, in 2018 the OECD conducted an awareness campaign on the safety of products sold online⁴ aiming to inform online platforms, online sellers and consumers about ways to identify product safety risks and navigate product safety regulations across jurisdictions.

It is important to effectively protect consumers engaged in e-commerce and other online activities for the digital economy to flourish. Transactions involving digital content and blurred boundaries between consumers and businesses can also complicate traditional ideas of ownership, liability, rights and obligations. Key challenges relate to information disclosure, misleading and unfair commercial practices, confirmation and payment, fraud and identity theft, product safety, and dispute resolution and redress.

For example, consumers increasingly acquire “free” goods and services in exchange for their personal data through non-monetary transactions, which can challenge traditional mechanisms of consumer dispute resolution (OECD, 2016^[17]). Similarly, novel forms of asset and content usage, including through rental, asset-sharing and subscription services, pose challenges for consumer understanding of their rights and obligations (Box 7.2). Limitations on the functionality and interoperability of digital products are likewise often not made clear. Similarly, pricing practices can be problematic for consumers, for example when businesses fail to disclose all elements of the price up front (“drip pricing”) or use misleading reference prices to exploit consumers’ behavioural biases.

7.2. Trust in peer platform markets

Peer-to-peer transactions have long played a role in commerce, but online platforms enable them on a much greater scale. Early examples include platforms for the sale of goods (e.g. online auction sites). Newer models cover accommodation, transport and mobility services. Other areas being transformed by these platforms involve small jobs, meal services and financial services. These business models are often described as the “sharing” economy or “collaborative consumption”, but those terms do not well capture the commercial exchange dimension that is commonplace in these markets.

7.2. Trust in peer platform markets (cont.)

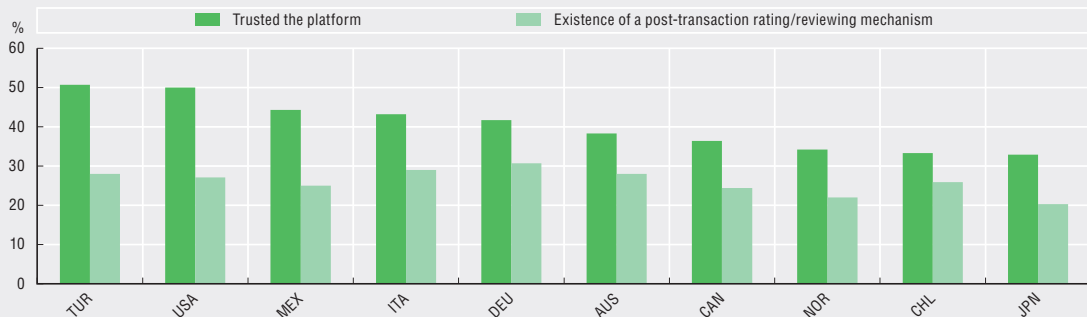
These business models open up economic opportunities for the individuals supplying the goods or services (“peer providers”) and for the platforms making the connections (“peer platforms”). Consumers can encounter issues of trust in their use of peer platforms in many different contexts: trust in the reliability and qualifications of the peer provider; trust in the asset or service; and trust in the guarantees and safeguards offered by the peer platform. Terms and conditions, for example, may not always suffice to communicate important information to consumers, as only 17% of people read terms and conditions of peer platforms (such as Airbnb and BlaBlaCar) in full.

Platforms have developed a number of practical, innovative mechanisms to address concerns and barriers to consumer engagement. The most notable trust mechanisms are review and reputation systems. Others include guarantees or insurance; verified identities; pre-screening; secure payment systems; and education, checklists and forms (OECD, 2016^[18]).


To understand better the drivers of consumer trust in peer platform markets, the OECD conducted an online survey of 10 000 consumers across ten OECD member countries (OECD, 2017^[19]). Survey findings include the fact that consumers generally trust peer platform markets, often more so than conventional businesses in the same market. The survey shows that at least 30% of consumers who went ahead with a purchase despite being unsure whether to trust the seller did so because they trusted the platform (Figure 7.4).

7.4. Consumers tend to trust peer platforms

Reasons for purchasing on a peer platform despite being unsure whether to trust the seller/provider, as a percentage of all purchasers on a peer platform who went ahead with purchase while unsure of seller/provider, 2017



Source: OECD (2019^[5]), *Measuring the Digital Transformation*, <https://dx.doi.org/10.1787/9789264311992-en>, based on OECD calculations based on OECD (2017^[19]), “Trust in peer platform markets: Consumer survey findings”, <https://dx.doi.org/10.1787/1a893b58-en>.

StatLink  <https://doi.org/10.1787/888933915430>

Although there is no single key to trust, secure payment, data security and the ability to see pictures of goods and services are the top drivers. Strangely, however, peer platform market consumers do not always read the platforms’ terms and conditions or the privacy policies in detail, despite claiming that the privacy and security of their data are important to them. This factor does not, however, appear to significantly undermine consumers’ trust that these platforms are using their personal data responsibly, especially when they compare peer platform markets to other types of online businesses.

Source: OECD (2017^[19]) “Trust in peer platform markets: Consumer survey findings”, <https://dx.doi.org/10.1787/1a893b58-en>.

In financial markets, individuals (notably groups with low levels of digital literacy) will need new skills and knowledge to be able to use new digital products and services effectively, and understand the potential ramifications of sharing data with institutions. Further, as consumers increasingly rely on automated processes and non-human support (e.g. robo-advice, chatbots), governance and controls must be put in place to ensure financial consumer protection, as they are in the offline world.

Increasingly, frictionless transactions also reinforce pre-existing offline questions with respect to the degree to which consumers understand the terms and the nature of the transactions being made, an issue even more important as more digital activities are undertaken on mobile phones.

7.3. Consumers and the Internet of Things

Consumers purchase and interact with a growing range of connected devices in their homes and everyday life, which are part of the IoT. These include wearables (such as fitness activity trackers, smart watches and glasses), smart home devices and appliances (such as smart locks and thermostats that can inform consumers of their energy usage and patterns), connected toys and childcare equipment.

Convenience, customisation and the ability to remotely control connected devices via a smartphone are among the many IoT benefits which consumers enjoy (OECD, 2018^[20]). In addition, the market is expected to revolutionise the way product design, manufacturing and delivery processes are improved over time, and to bring a number of product safety benefits. For example, connected devices like smart thermostats or smoke alarms can be remotely monitored and updated or disabled to manage product safety risks (including recalls) that emerge after installation (OECD, 2018^[21]; OECD, 2018^[22]).

Despite its promise, the IoT raises risks and challenges, which may affect trust in this emerging market. For example, software updates may introduce new problems to IoT products, or raise compliance issues. Digital security risks and vulnerabilities can also affect the safety of connected products. The complexity of IoT supply chains can create uncertainties about who is liable for consumer harms caused by a connected product and raise broader questions about whether consumer protection and product safety frameworks may need to be adapted to address such challenges.

Overall, to strengthen trust it is crucial to establish risk management as a common reference framework to develop coherent policies to enhance trust, involving the policy communities around digital security, privacy, consumer protection and product safety. In particular, policy makers should consider interrelations between digital risks in each of the areas. For example, a digital security incident where consumer data are stolen to commit fraud can violate privacy and consumer rights. Such interrelations underscore the importance of co-ordinating policies among these areas as a basis of a more comprehensive approach to trust in the digital era.

Notes

Israel

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

1. Figure 7.1: Except otherwise stated, Internet users are defined as individuals who accessed the Internet within the last 12 months. For Chile, data refer to 2014. For Costa Rica, data refer to individuals aged 18-74 instead of 16-74. For Korea, data refer to 2017 and include both private and business-related purposes. For Mexico, data refer to 2017 instead of 2015. From 2015 onwards, information was collected through an independent thematic survey, unlike previous years during which information was obtained through a module administered in various surveys. This methodological change must be taken into account when comparing data prior to 2015. In 2017, data refer to the following response item: “Fraud with information (financial, personal, etc.)”. For Switzerland, data refer to 2014 instead of 2015. In 2014, data relate to individuals “Having experienced a security problem within the last 12 months”.
2. Figure 7.2: For Australia, data refer to the fiscal year 2012/13 ending on 30 June 2013. For Canada, data refer to 2012. For countries included in the European Statistical System, in 2017 “Payment security and privacy concerns” does not include “privacy concerns”.
3. Figure 7.3: For Australia, data refer to the fiscal year 2012/13 ending on 30 June 2013. For Canada, data refer to 2012.
4. <http://oe.cd/safe-products-online>.

References

- Casalini, F. and J. López González (2019), “Trade and Cross-Border Data Flows”, *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, <https://doi.org/10.1787/b2023a47-en>. [10]
- Eurostat (2018), *Digital Economy and Society Statistics* (database), <https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/comprehensive-database> (accessed December 2018). [15]
- Hufford, A. and P. Loftus (2017), *Merck Swings to Loss as Cyberattack Hurts Sales*, <https://www.wsj.com/articles/merck-swings-to-loss-as-cyberattack-hurts-sales-1509107269>. [12]
- Mayer, R., J. Davis and D. Schoorman (1995), “An integrative model of organizational trust”, *The Academy of Management Review*, Vol. 20, No. 3, pp. 709-734, <http://www.jstor.org/stable/258792>. [3]
- Merck (2017), *Merck Announces Second-quarter 2017 Financial Results*, press release, 28 July, <https://www.mrknewsroom.com/news-release/corporate-news/merck-announces-second-quarter-2017-financial-results> (accessed 21 February 2019). [11]
- Murtin, F. et al. (2018), “Trust and its determinants: Evidence from the Trustlab experiment”, *OECD Statistics Working Papers*, No. 2018/2, OECD Publishing, Paris, <https://dx.doi.org/10.1787/869ef2ec-en>. [2]
- NCCIC (2016), *Cyber-attack against Ukrainian Critical Infrastructure*, <https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01> (accessed 21 February 2019). [13]
- OECD (2019), “ICT Access and Usage by Households and Individuals”, *OECD Telecommunications and Internet Statistics* (database), OECD, Paris, <https://dx.doi.org/10.1787/b9823565-en>. (accessed 28 January 2019) [6]
- OECD (2019), *Measuring the Digital Transformation: A Roadmap for the Future*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264311992-en>. [5]

7. STRENGTHENING TRUST

Notes and References

- OECD (2018), “Consumer policy and the smart home”, *OECD Digital Economy Papers*, No. 268, OECD Publishing, Paris, <https://dx.doi.org/10.1787/e124c34a-en>. [20]
- OECD (2018), “Consumer product safety in the Internet of Things”, *OECD Digital Economy Papers*, No. 267, OECD Publishing, Paris, <https://dx.doi.org/10.1787/7c45fa66-en>. [21]
- OECD (2018), “Enhancing product recall effectiveness globally: OECD background report”, *OECD Science, Technology and Industry Policy Papers*, No. 58, OECD Publishing, Paris, <https://dx.doi.org/10.1787/ef71935c-en>. [22]
- OECD (2017), *OECD Digital Economy Outlook 2017*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264276284-en>. [4]
- OECD (2017), *OECD Guidelines on Measuring Trust*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264278219-en>. [1]
- OECD (2017), “Trust in peer platform markets: Consumer survey findings”, *OECD Digital Economy Papers*, No. 263, OECD Publishing, Paris, <https://dx.doi.org/10.1787/1a893b58-en>. [19]
- OECD (2016), *OECD Recommendation of the Council on Consumer Protection in E-Commerce*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264255258-en>. [17]
- OECD (2016), “Protecting Consumers In Peer Platform Markets: Exploring The Issues”, No. 253, OECD Publishing, Paris, <https://dx.doi.org/10.1787/5jlwvz39m1zw-en>. [18]
- OECD (2016), *The OECD Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity*, OECD, Paris, <https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf>. [7]
- OECD (2013), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris, <http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf>. [9]
- OECD (2007), *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris, <http://www.oecd.org/internet/ieconomy/38770483.pdf>. [23]
- OECD (forthcoming), “Digital security and resilience in critical infrastructure and essential services”, *OECD Digital Economy Papers*, OECD Publishing, Paris. [16]
- OECD (forthcoming), “Towards national privacy strategies”, *OECD Digital Economy Policy Papers*, OECD Publishing, Paris. [8]
- Popescu, N. and S. Secrieru (2018), “Hacks, leaks and disruptions: Russian cyber strategies”, *Chaillot Paper No. 148*, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf. [14]



From:
Going Digital: Shaping Policies, Improving Lives

Access the complete publication at:
<https://doi.org/10.1787/9789264312012-en>

Please cite this chapter as:

OECD (2019), “Strengthening trust”, in *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris.

DOI: <https://doi.org/10.1787/2c24943b-en>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) at contact@cfcopies.com.