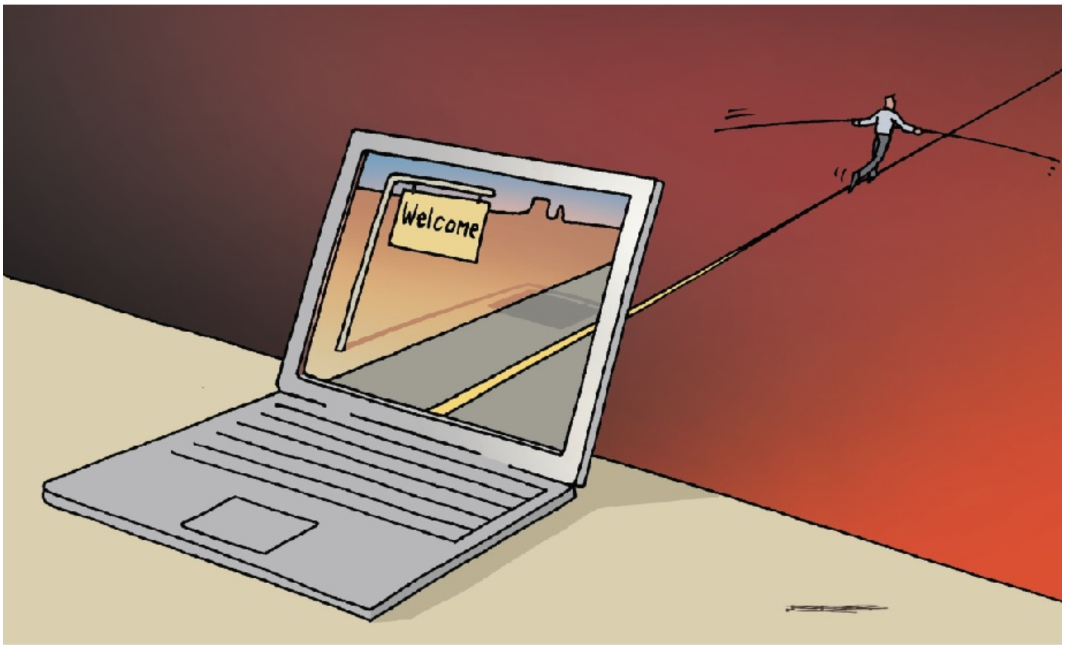
OECD Observer

Bridging policy silos to boost trust online

Last update: 8 March 2017



© Rooney

Three out of four people access the Internet everyday across the OECD. But one-third of those daily users don't yet buy online. Why not? According to a 2014 consumer survey the top two concerns reported by EU Internet shoppers are the misuse of personal data and security of online payments.

In a 2015 US Census Bureau survey 45% of online households reported that privacy and security concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet. These concerns extend to small business owners. While almost 95% of small and medium enterprises (SMEs) in the OECD had broadband access in 2014, only 20% used it to conduct e-sales. Recent surveys show that uncertainty on data privacy and digital security risk are critical elements. Trust issues rank highest in the list of obstacles for SMEs to realise the full economic potential of the Internet.

The links between consumer protection, privacy and security have long been clear, but with personal data now at the core of e-commerce business models, and increasing digital security threats, the need for joined-up approaches in managing consumer protection, privacy and security risk has become compelling. The vitality of the digital economy is at stake.

Today information communication technologies (ICTs) and the Internet are increasingly used for data-intensive economic and social activities which rely on an open and interconnected digital environment, and on the ability to move data easily, flexibly and cheaply across the world. Reduced transaction costs make it possible for a large number of buyers and sellers to interact over long distances. In this ecosystem, uncertainty can be high and trust is essential to realising the full economic and social benefits of the digital economy.

Trust is the state of mind that enables a person to be willing to make herself vulnerable to another an essential component of a healthy society and economy. From the privacy point of view trust is about the willingness of an individual to become vulnerable to an organisation by disclosing personal data. From a consumer protection point of view trust is the willingness of a consumer to risk time and money to engage in commercial activity. Digital security concerns can undermine trust, cutting across the consumer protection and privacy dimensions, but can also expand more generally to impact business, the economy and society. It takes patience and effort for a company to establish customer trust; however, one wrong move can destroy it forever.

Traditionally, regulators and professionals charged with overseeing these issues come from different types of agencies and communities but there is increasing overlap in the substantive and organisational challenges they face. The need has never been greater for breaking down the traditional 'silo' approach and promoting more co-ordinated governance mechanisms. If even modest projections are correct, the growth of the Internet of things applications and big data analytics could represent a fundamental shift in how users and business alike engage with and are impacted by the Internet. This will most likely raise new issues and different dimensions of existing challenges across consumer protection, privacy and security concerns. Ultimately, silo approaches will increase complexity rather than facilitate solutions for maximising the benefits of these new developments while minimising the potential risks.

The OECD began developing policy frameworks for trust online in the early 1990s with a view to helping governments realise the economic and social potential of the ICTs. With the Council adoption in March 2016 of the revised Recommendation on Consumer Protection in E-commerce (E-commerce Recommendation), the three OECD pillars for trust online (privacy, security and consumer protection) have now all been recently modernised. Prior to this, the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (Security Risk Recommendation) was adopted by Council in September 2015, and the landmark OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines) were revised in 2013.

Taken together, these three Recommendations represent a modern overarching policy framework for addressing the broad scope of the emerging promises and risks of the digital environment. More than that, they also highlight tightening links across the three areas. There has always been a "security safeguards" principle in the OECD privacy guidelines, but the 2013 revisions also highlight the need for a risk-based approach. This is commonplace in the security world and the 2015 Security Risk Recommendation explicitly notes the value of such an approach for implementing the OECD Privacy Guidelines. The revisions to the 2016 E-commerce Recommendation, in turn, bring "free" services exchanged for personal data within its scope and likewise include new provisions on privacy and security to reflect the corresponding need to protect consumer data.

One key element of this modern overarching policy framework is the role of risk management. Despite the increasing awareness of risks and uncertainties when using the Internet, such as security threats, digital risk continues to be approached as a "special" matter, in isolation from economic and social decision making. In businesses, for example, digital security risk is often viewed solely as a technical issue, while privacy and consumer protection are treated as legal compliance challenges. The three areas are rarely understood by business leaders as having economic implications directly affecting reputation, operations, competitiveness, innovation and revenues, and even less so as possible market differentiators, and sources of competitive advantage.

Greater co-ordination across the security, privacy and consumer protection policy communities is called for in addressing an increasingly wide range of issues.

Take, for instance, digital security incidents that result in a breach of personal data, bundling privacy and consumer risks related to fraud and identity theft with security issues in ways that significantly impact trust. The revised OECD Privacy Guidelines call for organisations to provide notifications in cases where there has been a significant security breach affecting personal data.

Meanwhile, businesses and consumers rely on digital identity management in online transactions as a means to reduce fraud, protect personal information (including financial information) and to reduce the likelihood of digital security incidents. Effective approaches cut across security, privacy and consumer protection issues.

Digital risk insurance is another challenge. Although businesses and consumers are beginning to explore the possible benefits of digital risk insurance, standard policies are not designed to cover digital security and privacy risks. Concrete efforts, for instance, to address uncertainties around definitions, or the absence of relevant data on past incidents and losses, are needed to open up opportunities in this area. Data access and portability also raise trust issues.

Data access rights have long been a part of privacy laws, and this is now expanding to data portability, with new initiatives to enable consumers to obtain their data in formats that enable its re-use in other services. Effective authentication and security measures will be essential to making portability mechanisms trustworthy.

Another tricky issue is so-called algorithmic discrimination . Automated decision-making, built on data-fuelled predictive analytics and machine learning, can generate valuable commercial and client insights. At the same time these operations bring risks of stereotyping and discrimination, which must be addressed.

> Another tricky issue is so-called algorithmic discrimination

These are but a few examples of the overlapping issues that could usefully be addressed in a more joined-up way by policy makers in the security, privacy and consumer communities as they work to address the digital risks that threaten trust online.

www.oecd.org/sti