SECURING CONSUMER TRUST IN THE INTERNET OF THINGS

PRINCIPLES AND RECOMMENDATIONS 2017

INTRODUCTION

Consumer applications in the internet of things can bring social and economic benefits to people around the world including: more responsive services; shorter feedback loops; remote fixes; greater convenience; decision making support; better allocation of resources; remote control of services and insights into behaviour.

However, there are some causes for concern: privacy and security; lack of transparency; complex liability; lock-in to products and systems; and an increase in hybrid products which erode ownership norms, leaving consumers exposed to remote contract enforcement, loss of control and the risk of devices becoming unexpectedly redundant if support is stopped.

The potential benefits will only be achieved if services and products can be designed with trust, privacy and security built in so that consumers feel they are fair and safe to use. Working together on the following areas will be essential to building a thriving and trusted internet of things environment for consumers.

Each heading contains the main challenges and opportunities for consumers in this particular area, along with a set of principles from which specific recommendations in terms of policy, standards, testing and business practice will be developed.

Photo credit: Canadapanda / Shutterstock.com

1. CONNECTIVITY AND INCLUSION

As connected products become ubiquitous in people's lives, having access to a high quality, affordable internet connection, both mobile and fixed, nationally and internationally, will become even more essential for all consumers. More than ever, internet access providers shall not unjustifiably slow down, block access to, or otherwise discriminate against certain applications or services.

1.1 Consumers should have access to an affordable, high-quality, high-speed internet connection to enable them to take up the opportunities brought about by internet of things technology.

1.2 Particular attention should be given to ensuring access for marginalised or disadvantaged and vulnerable groups of consumers and those in remote or underserved geographical areas and access measures should reflect low-income groups and demographic equality.

1.3 Countries should address all drivers of affordability such as device costs and the application of unfair data caps that can keep the price of connectivity artificially high.

1.4 The principle of net neutrality should be respected.

2. INFORMATION AND TRANSPARENCY

Having the right information to understand how digital products and services work and to help make decisions is central to an internet of things environment that consumers can trust. However, it is particularly challenging to get easily accessible, clear, concise, meaningful and verifiable information that gives full clarity to people at the right time.

Reliance on the concept of "notice and consent" alone to provide information and choice will become more problematic for consumers in the internet of things environment, given the potential for large amounts of granular data used from many different types of devices, and the number of suppliers involved.

2.1 Clear, succinct and easily understandable information about internet of things products, providers, processes and consumer rights should be prominent and readily available.

2.2 This information should enable consumers to understand the implications of their usage of internet of things products, and facilitate confident, informed decision-making. This means, in particular, informing consumers about what a product can/cannot do without being connected.

2.3 Critical information should be made prominent prior to purchase.

3. OWNERSHIP AND USE

Digital technology has changed the nature of many services and products because connected software is now contained in an increasing number of general consumer products. Established expectations of ownership are challenged in the internet of things as most products have a significant service component, or become services. They are thus subject to greater controls over use, sharing, modification and transfer to alternative services. Providers can enforce sanctions remotely due to centralised nature of their control over software and platforms and there is a lack of ability on part of the consumer to challenge sanctions or decisions made about people based on their usage. Other problems occur if the software provider changes hands and ends support for the product, or has different data governance processes.

3.1 The contractual clauses and technology that define the usage of an internet of things product or service must be fair in light of legitimate consumer expectations, with rights to fair use guaranteed.

3.2 Controls that producers can exercise over the use of a product should be legitimate, fair and proportionate, and companies should follow due process.

3.3 Depending on the nature and functionalities of a given product, it must be ensured to the full extent possible that all basic functionalities would still work without connection to the internet.

4. SECURITY AND SAFETY

The internet of things provides hackers with more vulnerabilities to exploit in more environments and, because of the high quantity of interconnections between devices and systems, potentially a faster pathway to multiple devices. Security must be ensured in all parts of a connected system, as vulnerabilities in any given component of the system can potentially compromise the whole system. Consumers will become ever more reliant on manufacturers to provide updates and maintain security.

In many jurisdictions, existing product safety legislation and standards cover the safety of individual devices but may not be fit to properly protect consumers from the security risks of internet of things as devices are part of a bigger system. To ensure the safety of the system as a whole, additional provisions and standards will need to be adopted when the device is controlled and operated as part of a wider internet of things system. This wider system also brings the risk of lower quality connection and security as more and more components and devices share frequency bands.

ESTABLISHED EXPECTATIONS OF OWNERSHIP ARE CHALLENGED IN THE INTERNET OF THINGS

4.1 The concept of 'safety' in general and sector specific product safety legislation should be broadened to reflect new cybersecurity, data security and product safety concerns.

4.2 Internet of things cybersecurity measures should protect against any security vulnerability, in particular, hacking or unauthorised access and misuse.

4.3 Internet of things data and identity security measures should, among other things, protect payment details, financial assets and personal identity against fraud or misuse.

4.4 Internet of things product safety measures should protect the personal safety of consumers, reflecting the risks posed by close proximity use, shared frequency bands, the risk of electromagnetic fields exposure, and potential interference with vital connected equipment.

4.5 Consumers should not bear the risk of new advances in internet of things technology, market surveillance mechanisms should be fit for purpose and able to ensure that unsafe or potentially insecure connected products do not reach the market or will be immediately taken off the market when a hazard is identified.

4.6 Companies should adopt best practice standards such as security by design and by default, and be subject to independent assessments of compliance. In case of security incidents or data breaches, they must be subject to timely and adequate notification obligations, liability and compensation rules, and sanctions in case of neglect.

4.7 Companies and regulators should develop systems that make it easier for consumers to adopt safe and secure practices in the internet of things , for example simple settings, warnings and updates.

4.8 International standards should be developed to ensure companies provide essential security updates for internet of things products during the product's expected lifecycle for a specified and reasonable period after sale.

5. LIABILITY

The internet of things can connect devices from different manufacturers, retailers, or software developers. This complex ecosystem of connected devices can make it much harder to establish who is liable under traditional laws and regulations when something goes wrong. Additionally, many of those in the design, production and delivery chain may not have had experience of designing in security and data protection for networked devices.

A new approach to liability is required to ensure that consumers are protected in an environment where products (a) can become defective and unsafe as a result of digital security incidents; (b) increasingly take, anticipate and predict decisions without human intervention.

5.1 A clear and robust product liability framework that protects consumers if they suffer a damage caused by unsafe connected products or services is essential. As new risks arise, tort law rules governing the safety and liability standards should be introduced, replaced or updated, where necessary.

5.2 It should be clear which entity is responsible for performance and security at each point of product delivery and during the full lifespan of the connected product. Clear rules on liability should ensure that consumers are fully compensated in case they are harmed because of a defective product.

5.3 Liability rules should cover all types of products, digital content products, and (digital and other) services that comprise the internet of things ecosystem.

5.4 Liability time limits should be avoided or at least be extended to cover the expected lifespan of a product. Compensation thresholds should also be avoided to enable flexible application of awards.

5.5 There should be joint liability of all professionals in the product supply chain if their activities have affected the safety of a product. This would reflect the risk-oriented approach of product liability law and avoid problems to identify the liable person when the product is made by several producers and contributors.

5.6 Where complaints or problems involve multiple providers and/or sectors, it must be clear where a consumer should go for assistance. Alternative dispute resolution (ADR) is needed where suppliers are in different sectors, and if possible, this should have a single contact point for consumers.

6. DATA PROTECTION AND PRIVACY ONLINE

Consumers should be able to exert control over their personal data and privacy preferences. It is also important to consider the impact of multiple products, services and organisations aggregating data on individuals and their rights as a consumer and citizen.

As a principle, the user or owner/user of a device should be in control of how the data it generates is used and by whom. The sheer scale of different types and amounts of data able to, not just, be collected in the internet of things , but aggregated and merged with other data poses a large risk to privacy. Objects within a connected internet of things system may collect data or information that is innocuous on its own but which, when collated and analysed with other information could reveal quite accurate knowledge of things like individuals' habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling.

One of the most significant internet of things-related data privacy risks stems from the fact that devices are able, and indeed designed to, communicate with each other and transfer data autonomously to an external partner (such as a device manufacturer). With applications made with proprietary software operating in the background, it will become more difficult for individuals to see if, when and how processing takes place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially limited.

6.1 Consumers' privacy and data protection rights must be properly protected and upheld to address potential harms such as discriminatory practices, invasive marketing, loss of privacy and security breaches.

6.2 Internet of things companies and regulators should regularly review and re-evaluate the scope of personal data collection, and assess to what extent the data processed is proportionate and necessary for the service delivery.

6.3 Privacy aspects and impacts must be assessed and integrated throughout the whole conception, design and development cycle of a connected product and the networked ecosystem in which it operates (privacy by design). By default, the settings of any connected product must be set to the highest level of privacy protection from the outset (privacy by default), preventing unwanted tracking of users' behaviour and activities.

6.4 Consumers should be made aware of the implications of how data collected by internet of things products and services could be used and given simple and effective ways to assert control and mitigate risks.

6.5 Consumers' data belong to them. They must have full control over the data that stems from their connected products and their use. Companies should provide simple, secure ways for consumers to access and control their data, including the possibility to transfer their data to other services as they see fit. Consumer should be able to benefit from the economic value of their data, and other opportunities of sharing their data, in line with their preferences, expectations and legal rights.

6.6 It should be clear to consumers what data will be collected, with whom it would be shared and for which purpose it will be used throughout the duration of the product or service relationship. At the very least, connected products and services using personal data, must have a clear, comprehensive and easy to understand privacy policy in place.

6.7 It should be clear to consumers if and how algorithms used in internet of things products make decisions about them that affect the quality, price or access to a service.

6.8 Regulators should ensure the use of algorithms is lawful and does not discriminate by making detrimental decisions based on information about consumers. Regulators should consider appropriate frameworks to address problems should they arise which should include rights to challenge automated decisions that produce legal effects.

6.9 Independent, well resourced, national data protection agencies that are relevant to the internet of things should be in place. Data protection laws should be fully enforced, and strengthened if necessary where consumer detriment is identified. Given the central importance of data within the internet of things, independent data protection agencies which can fulfil their mandate to protect consumers' data are essential.

6.10 International policy on cross-border data flows should be co-ordinated so that countries involved have in place equally high standards of protection in both substantive and procedural national laws.

7. COMPLAINTS HANDLING AND REDRESS

Interconnected services can increase convenience by removing the friction from consumer tasks involving multiple providers. However, identifying which supplier is responsible for faults or problems is complex, as is verifying claims for the quality or performance of things that rely on multiple partners in the chain to work. These complexities should not affect consumers' right to obtain redress.

7.1 Rights to redress for internet of things products and services should not be less than those available for other forms of commerce. Complaints handling and redress mechanisms should be accessible, affordable, independent, fair, accountable, timely and efficient.

7.2 Companies offering internet of things products and services should have strong internal dispute mechanisms that do not impose unreasonable delays or burdens on consumers.

7.3 Recourse to independent redress should be available to address complaints that are not satisfactorily resolved by internal mechanisms. It should be clear where consumers should go for assistance.

7.4 Where products and services cut across jurisdictions or sectors, regulators should work across jurisdictions and sectoral boundaries to support cross-border dispute resolution. It must also be clear where consumers should go for assistance.

7.5 Aggregate information with respect to complaints and their resolutions should be made public.

7.6 Online dispute resolutions should be provided but not to the exclusion of other avenues.

8. COMPETITION AND CHOICE

If vertical integration and market concentration becomes the norm in the internet of things, it will be increasingly possible to lock people into a vendor's own products or to a closed ecosystem. This has implications for consumers wanting to shop around for different apps or services, use an independent repair service, or link to other preferred apps or data streams.

Competition law and policy should be fit for the purpose of ensuring that the internet of things is competitive in all its subsectors. Consumers often have limited rights to the data they themselves create through transactions or through using the device/service they purchased in the way they want. For example, it is often difficult or impossible to port data or content between providers. Therefore, ensuring data portability is key not only to give consumers control over their own data but to also foster competition between services. Interoperability is also an essential element to prevent consumers becoming locked into closed internet of things ecosystems. Competition authorities have an important role to play in the promotion of a dynamic, consumer-friendly environment for the development of the internet of things.

8.1 Interoperable and compatible device and software standards should be in place to avoid lock-in effects and enhance consumers' ability to easily compare and switch providers.

8.2 Transfer of data between services in order to facilitate switching should be possible whilst respecting the consumers' data protection rights.

8.3 Attention should be given to ensure that the connectivity element of an internet of things service, does not become a lock-in mechanism for consumers and that they can easily switch between connectivity providers.

8.4 Competition regulators should consider competition remedies such as requiring interoperability or access of data by competitors to mitigate the effects of data concentration and dominant players.

ENSURING DATA PORTABILITY IS KEY TO GIVE CONSUMERS CONTROL OVER THEIR OWN DATA AND TO FOSTER COMPETITION.

Photo credit: StockphotoVideo / Shutterstock.com

9. LIFECYCLE

Relentless innovation and competition for market-share means that the underlying technologies in devices keep surging ahead, with faster processors, better cameras, better batteries and so on. Lack of updates and discontinuation of technical support can render perfectly functional products quickly obsolete.

This means that the service life of most electrical appliances is becoming shorter. This has implications for resource use and disposal, as only a fraction of e-waste is recycled. E-waste is often highly toxic, leaching heavy metals and dangerous chemicals into the soil around landfills and releasing greenhouse gas and mercury emissions when burned. In addition, consumers are increasingly unhappy, a recent consumer survey conducted for the study revealed that about one third of those polled are not satisfied with the service life of their appliances.

9.1 Connected products need to be easily upgradeable to reduce the potential for products to be rendered obsolete.

9.2 Updates should be made available to consumers regardless of location.

9.3 As far as possible, devices, adaptors and other connection points should be compatible with each other to reduce the potential for new incompatible interfaces to render devices obsolete.

9.4 Consumers should be provided with clear, comparable and credible information concerning expected lifetime and reparability of products.

9.5 Products should be designed and built with resource efficiency in mind – from using sustainably-produced materials and construction methods; to providing clear guidance to consumers on the most efficient use, re-use/repair and disposal of the product and its components.

9.6 Products should be designed so that the time sensitive software can respond to latent or low use periods in order to save energy. Low energy products are to be welcomed.

9.7 Measures should be taken to ensure that the disposal of any heavy metals and other dangerous substances contained in connected products is not harmful to the environment and human health.

GENERAL RECOMMENDATIONS

1. REGULATORY FRAMEWORK

The responsibility for ensuring that consumers' rights are protected online, and autonomy and personal freedom are upheld, cannot be managed by one country alone; it requires international collaboration across governments, international organisations and businesses.

1.1 Protections should be an integral part of the regulatory framework, with effective, proportionate and accessible legal, judicial or supervisory mechanisms available for consumers in the internet of things.

1.2 Regulatory authorities must cooperate cross-sectors and cross-borders to address consumer problems.

1.3 Protection framework should as a minimum meet requirements, as set out in international guidelines, recommendations such as the UN Guidelines on Consumer Protection, and provide an equal level of protection regardless of location and type of activity. Where national, local or regional requirements are higher these should be followed.

1.4 Regulation should address new challenges arising from consumer use of applications in the internet of things on all aspects addressed in these principles.

1.5 Countries should agree to progress together towards the development of global, open and complementary technical standards.

1.6 Regulatory authorities must also have the knowledge and skills to understand internet of things technology. If they do not possess those skills in-house they should cooperate with those authorities or organisations that do.

1.7 A sound measurement of consumer sentiment and experience on internet of things developments and how it affects consumer trust and confidence is essential.

2. RESPONSIBLE BUSINESS CONDUCT AND THE ROLE OF OVERSIGHT BODIES

Treating consumers fairly should be an integral part of the objectives, good governance and corporate culture of all providers of internet of things application.

2.1 Companies operating in different jurisdictions should as a principle apply the highest standards to all their consumers, regardless of where a consumer is based.

2.2 Ethical impact assessment frameworks for internet of things research and innovation activities should be developed and promoted, based on national, regional and international shared understanding amongst actors involved in research and innovation. Such frameworks should be adapted to technological developments and respond to societal concerns.

2.3 Providers of internet of things applications and services should adhere to the best practice guidelines of the United Nations Guidelines for Consumer Protection which state that all consumers of digital products and services should be treated equitably, honestly and fairly.

2.4 Any practices that increase the risk of harm to consumers should be avoided, with special attention given to the needs of disadvantaged or vulnerable consumers, such as children and people with disabilities.

2.5 Countries should have oversight bodies with responsibility for all aspects of digital consumer protection including the internet of things. Such bodies must have the necessary authority and independence to fulfil their mandates and the technical resources and capabilities to respond to developments in the sector.

3. DIGITAL EDUCATION AND AWARENESS

Education and awareness provision should complement rather than replace regulatory and legislative protection. Education is a shared responsibility for all public and private actors involved in the internet of things ecosystem.

3.1 Education and awareness of internet of things devices and implications for consumers should be delivered through the most effective channel, and be highly targeted and evaluated to ensure it addresses specific consumer needs.

3.2 Education and awareness of internet of things products should support consumers to develop the skills and confidence to be able to manage risks and opportunities, make informed choices, know how to get assistance and advice and act to protect and improve their well-being and identity in the internet of things.

3.3 Companies, regulators, consumer protection bodies and consumer organisations should collaborate to develop systems to make it easier for consumers to understand risks and opportunities of connected products and services.

These principles represent the joint work of ANEC, BEUC, Consumers International and ICRT:

ANEC
ANEC is the European consumer voice in standardisation. We represent the European consumer interest in the creation of technical standards, especially those developed to support the implementation of European laws and public policies.
www.anec.eu

BEUC – The European Consumer Organisation
BEUC (Bureau Européen des Unions de Consommateurs) is a not-for-profit organisation that represents 43, independent national consumer organisations from 31 European countries (EU, EEA and applicant countries). For over 50 years, BEUC has worked relentlessly as the voice of European consumers. We bring consumers' viewpoints from across Europe to the EU policy making arena.
www.beuc.eu

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

ICRT
International Consumer Research & Testing (ICRT) is a global consortium of more than 35 consumer organisations dedicated to carrying out joint research and testing in the consumer interest. ICRT member organisations do not accept advertising and are independent of commerce, industry and political parties.
www.international-testing.org