CSA GROUP RESEARCH

The Role of Standardization in Emerging Technologies

March 2019

Authors

Tony Capel, Comgate Engineering Ltd.

Ahmed Shalabi, Comgate Engineering Ltd.

Advisory Panel

Jim MacFie, Microsoft Canada

Francois Coallier, École de Technologie Supérieure

Stephen Michell, CSA Group (Project Manager)

Cliff Rondeau, CSA Group

Shawn Paulsen, CSA Group

Hélène Vaillancourt, CSA Group

This work has been funded by Microsoft Canada and CSA Group.

Contents

Executive Summary

Continued advances in information and communications technology (ICT) have enabled the delivery of new and increasingly complex products and services. These advances range from social media services such as Facebook and Twitter, to new "intelligent" internet-connected products for the home. Evidence is growing that the general public, including both end users and governments, are having difficulty understanding the potentially serious impacts the use of these technologies may have on their safety, security and privacy. Governments are concerned that data misuse can lead to the manipulation of public discourse. Vendors are concerned that the resulting loss of customer confidence will limit popularity or may result in regulatory requirements which are costly to implement.

Assuring the public that the products they use are safe to use has historically been the role of standards-based regulation. National and international standards are developed to define the required safety requirements, and regulations are set in place to ensure that all products are tested and certified to meet these standards. Confidence in less important product properties have traditionally been supported by reliance on the vendor's reputation and warranties, or by reference to trusted sources of opinion, such as published product reviews.

For these new and emerging ICT-enabled products and services important new concerns that go beyond simple product safety are being identified. Existing regulation-driven testing and certification, referring to slow-to-change traditional standards, has been shown to be insufficient to address these new concerns. Users and public policy-makers are losing confidence and the assurance that the products and services in use meet all their expectations, including preventing data misuse and preserving privacy, security and safety in a timely manner. The ICT product lifecycle is much shorter than other market driven products, hence, developing standards in a timely manner is problematic.

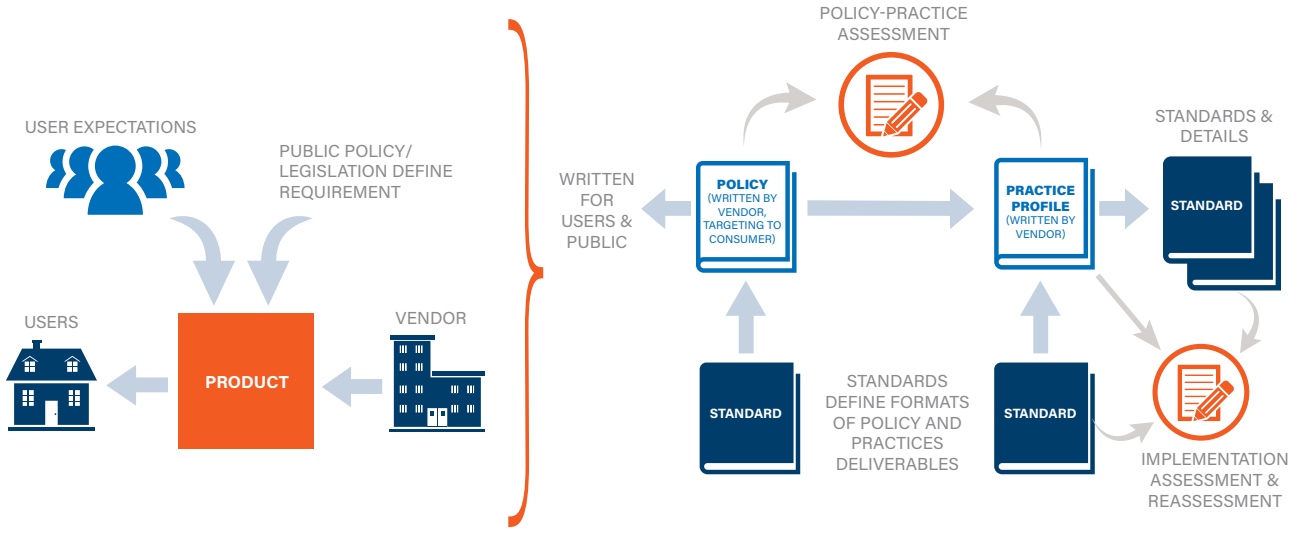
To identify the gaps in the assurance systems used today, a range of stakeholders were interviewed and the relevant literature was reviewed. It was observed that it is becoming increasingly hard for end users and policy-makers to fully understand and directly evaluate the technologies in use. This, along with the wider range of concerns that need to be addressed, has opened a significant gap between existing approaches to provide public confidence, and those needed to support these new products and services.

Any solution must meet the concerns of all stakeholders:

- Users who use the products and services;
- Regulators who implement legislated (public policy) requirements;
- Developers who create any needed standards;
- Organizations who assess individual product or service suitability; and
- Vendors who provide the products and services.

For this report the concerns gathered through the interviews and from the literature were first identified by emerging technology sector, and then reorganized by stakeholder. This step was essential to ensure that any proposed solution would be applicable to all sectors. It was not necessary to identify all concerns, or attempt to prioritize them, rather it was important to identify the range of concerns from the viewpoint of each stakeholder. This report proposes a modified framework, shown in the figure below, to meet the unaddressed gaps in meeting stakeholder concerns.

This framework proposes new deliverables better matched to the needs of stakeholders.



- For both users and regulators, standardized "policy descriptions" are published by vendors to fully define the properties of the product or service. These extend current "terms of use" agreements to add all details needed to address user and public (e.g. regulatory) concerns. By defining a standard format, it becomes easier to assess completeness, and permits the comparative assessment of similar products and services. It also facilitates their endorsement by other parties since many end users may not fully read these documents, instead relying on regulator, peer or trusted third-party endorsements. Policy descriptions are expected to be published prior to product or service delivery, and to remain largely stable over the life of the product or service.
- For vendors of products and services, potentially confidential but standardized, "practice profiles" are written by vendors to describe the practices and controls used to meet the policy description. These documents profile the technical standards along with vendor-specific details. Practice profiles will likely be less stable than policy descriptions since they must continually evolve to address evolving threats and technology change.
- For assessors, procedures and tools are needed to support two types of assessments:
  a. compliance between policy descriptions and practice profiles, and
  b. compliance of the vendor's implementation with the practice profile.

These assessments differ significantly from one another and may be conducted by differing assessment organizations and will occur at differing times. The first case, compliance evaluation between policy descriptions and practice profiles would occur less frequently, while the second case, assessments of implementations, would call on extensive technical system engineering skills applied over the life of the product or service. These must be provided in a manner where trust between the users and regulators is paramount in the chain of assessments between the policy description and the implementation.

1 Introduction

Standards of all types, recognized internationally, regionally or nationally, or simply recognized as de-facto specifications, play an important role in supporting the efficient and safe use of technology. Traditionally standards, along with the necessary regulations referring to these standards, have provided confidence to users that the products and services they use are generally safe and fit for use in appropriate contexts. However, with the new generation of "smart" products and services, enabled by cost effective and powerful information and communications technology (ICT), it has become increasingly difficult for users and policy-makers to be confident that these new products and services continue to be safe and fit for use, and that they are not being misused.

Public confidence has traditionally been supported by government-provided regulatory oversight, by reliance on the reputation and warranties of the vendor, or by reference to trusted sources of opinion, e.g., from published product reviews or the opinions of others.

The level of confidence needed depends upon the consequences of a failure to meet product or service expectations. At one extreme, ensuring that products are safe to use has always been a priority, resulting in legislation and regulations to ensure that only products certified to meet minimum safety standards are legally available. Performance and fitness for use requirements, although often specified by standards, have often been left to end users to confirm. In some cases, vendors may offer guarantees, possibly supported by product warrantees. In other cases, where significant costs would arise from a failure, insurance companies may insist on minimum compliance to standards before providing insurance or discounting premiums.

The world is changing as the products and services we buy and use are becoming more complex to understand, and where the enhanced capabilities they offer significantly impact our lives, including our safety, security and privacy.

For this report the concerns gathered through interviews and from the literature were first identified and organized in terms of the emerging technology sectors highly impacted by new ICT. They were then reorganized by stakeholder type, an essential step to ensure that any proposed solution would be applicable to all sectors. Unmet concerns were then used to identify the gaps in the existing standardization and regulatory system. This report also provides a recommended approach to close these gaps and identifies work that still needs to be done.

The report is organized as follows:

- The balance of Section 1 provides a short introduction into the current system of standards development and adherence, both voluntary and mandatory, and regulations which aim to provide confidence in the products and services we use.
- In section 2, emerging technology-driven areas, identified during the interviews, are organized and examined by stakeholder type (that is, by user, regulator, vendor, assessor, standards developer). The technology-related view is collected in Annex B.
- Section 3 suggests a framework to address the unmet concerns (i.e. gaps).
- Section 4 provides the conclusions to this report.
- Annex A recommends topics needing future work.
- Annex B summarizes the concerns of stakeholders by technology, which is consolidated by stakeholder type in section 2.

1.1 Voluntary and mandatory standards and regulations

Society uses a range of mechanisms to provide users and others with the confidence that the products and services in use are appropriate and safe. These range from regulations and codes and standards[1] cited in legislation, to voluntary standards with a range of assessment and certification tools, including none at all.

[1] A code is a type of standard that focuses on installation and maintenance of products and systems.

The need to ensure public confidence remains a key requirement:

- For end users, so they can be confident about the products and services they use;
- For suppliers, so they can be confident that the market for their products and services will remain open to them; and
- For governments and others who want to ensure public safety and security, and that other important public policy objectives are met.

For traditional products establishing strong regulatory environments for product safety is relatively straightforward. For a simple product such as an electrical appliance, compliance testing can be carried out on product samples, with subsequent identical production also assumed to comply.

This is demonstrated in Figure 1 where at the top of the figure the vendor provides products to end-users. In this traditional case, the vendor provides product samples to an accredited assessment organization that tests for compliance to one or more standards. These standards have been developed in turn to meet safety and other public policy objectives. A compliance certificate issued by the assessment organization is used to support vendor supply of identical products to users.

For less important quality assurances, the reputation of the manufacturer's brand, or reference to general consumer reports and user feedback in online stores, may give users sufficient confidence. For these cases, no explicit assessment is usually needed.

Standards have long been used to:

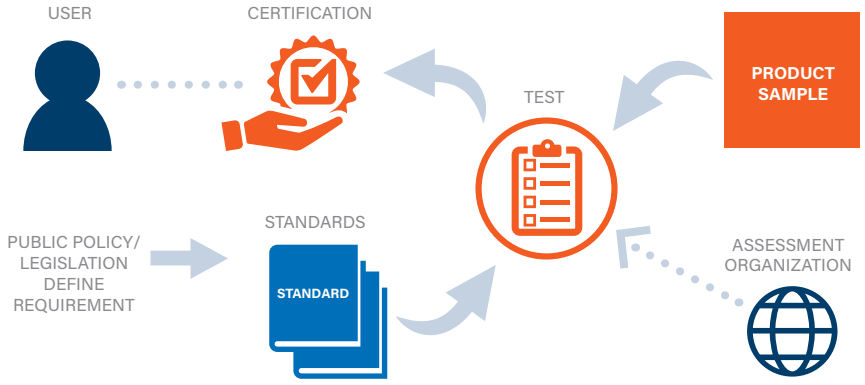
- Define safety or security requirements;
- Identify performance requirements; and
- Provide common metrics to allow users to compare products.

Times are changing however. Modern ICT has enabled increasingly complex products and services to be deployed with global reach. In addition, suppliers are now able to provide products and services of radically differing scope and complexity as witnessed by the growing range of "smart appliances" and online social media services. These products and services introduce new challenges to the traditional systems used to provide the needed confidence.

1.2 Regulation as a provider of confidence

Regulations are used by governments to achieve their policy objectives and improve the quality of life for its citizens. They are used in combination with other instruments, including standards and codes, to achieve

Figure 1: *Certification framework for traditional products*



"Regulations often cite specific standards that must be met by products within their jurisdiction."

these objectives. Key objectives are to protect and advance the public interest in terms of health, safety and security, environmental quality, and the social and economic well-being of its citizens. Regulations often cite specific standards that must be met by products and services offered within their jurisdiction, including applicable procedures to ensure compliance. These may also include requirements related to manufacturing and testing, terminology, symbols, and packaging, marking or labelling requirements. While most standards are voluntary, a regulation citing such a standard can make conformance to a standard mandatory.

Based on the risk to the public, regulations define specific procedures that must be followed to meet conformance requirements. For high-risk situations, suppliers may be required to obtain the services of an accredited assessment service to certify their product[2]. The International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO)[3] and others have established international mutual recognition schemes[4] of such testing services, which are accepted in many jurisdictions. International schemes are generally aimed at ensuring that local regulatory requirements do not become a technical barrier to international trade. In lower risk situations, regulations may only require the manufacturer to test for conformance to specific standards and to make the results available[5]. In some cases, the manufacturer may be required to self-declare conformity to the applicable standards and make supporting information available only if a problem arises[6].

Regulations form the foundation of the Canadian Electrical Safety System. Canadian electrical standards now cover everything from installation procedures and overhead and underground electrical distribution systems, to products and system components such as door openers and remote heaters. This collective group of standards, the Canadian Electrical Code [4] (CE Code), has been in place for nearly a century. This series of standards are developed and maintained through committees with representation from all sectors of the electrical industry, including all regulatory jurisdictions across Canada.

[2] In Canada, this is used to ensure compliance with important safety standards.

[3] International Electrotechnical Commission (IEC) www.iec.ch
International Organization for Standardization (ISO) www.iso.org

[4] The IEC *System of Conformity Assessment Schemes for Electrotechnical Equipment and Components* (IECEE) is the IEC organization responsible for conformity assessments [7]. See www.iecee.org

ISO's *Committee on Conformity Assessment* (CASCO) is the ISO committee that develops policy and publishes standards related to conformity assessment. See https://www.iso.org/casco.html

In Canada, these schemes are managed by the Standards Council of Canada (SCC). See www.scc.ca

[5] In Canada and the USA, this is used to ensure compliance with electromagnetic compatibility (EMC) standards for radio equipment. In Canada, this is defined in: RSS-Gen — *General Requirements for Compliance of Radio Apparatus*. See http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf06128.html

[6] This is true for some regulations in the European Union (EU). For example, the European "CE" mark requires the manufacturer to declare conformance to all applicable EU requirements. See https://ec.europa.eu/growth/single-market/ce-marking_en

Regulatory enforcement of the CE Code is the responsibility of individual provinces and territories, each with distinct legislation and regulations concerning electrical safety. Most provinces adopt the Code without significant technical changes, while other provinces, such as Québec and Ontario, add their own deviations. See for example the Québec Electrical Code [5].

Occupational health and safety and workers' compensation in each Canadian jurisdiction outlines the general rights and responsibilities of the employer, supervisor and worker [2]. Each of the ten provinces, three territories and the federal government has its own legislation. Federal legislation applies to employees of the federal government, federal corporations and federally regulated industries such as inter-provincial and international transportation, shipping, telephone and cable systems. Provincial or territorial legislation applies to most other workplaces, for example, Commission des normes, de l'équité, de la santé et de la sécurité du travail (CNESST) provides this function in Québec.

1.3 Non-regulatory means to provide confidence

The citing of standards, not specifically called for by regulation, may also provide confidence that a product or service is fit for use. For example, a supplier might cite a standard in their marketing or contractual material and offer guarantees of compliance. This is an area of some confusion, since only some standards have supporting systems to certify claims of conformance, while others do not. Furthermore, these systems may or may not have strong national and/or international acceptance.

In Canada, the ISO 9001 [8][7] standard on quality management is often cited by suppliers to reassure clients regarding management aspects of the services they provide. While this standard has an international accreditation framework[8] other standards may be cited with little or no obligation on the part of the supplier to prove their compliance.

In some cases "voluntary codes" have been defined which benchmark specific performance properties[9]. Declared compliance to voluntary codes can also offer some levels of confidence to purchasers of products or services.

Quasi-standards writers[10] may fill the gap to address needs not considered important enough by governments to enact regulation. These bodies may identify a series of standards and offer conformance testing services to their members so that their members can affix a trademark logo to their product. Consumers can then be reassured by the presence of this trademark that the product will meet the defined performance requirements[11].

Some member-based professional organizations may also offer testing and certification services in conjunction with the standards they develop[12] [13].

1.4 Providing confidence in complex products and services

While the citing of compliance to standards can be useful for well-known product and services, establishing confidence in complex products and services is more challenging. International regulatory bodies have yet to make significant progress in introducing certification systems useful for large complex products and services.

Complex products and services are typically constructed using unique combinations of components working together as a "system" or a system of systems, requiring

[7] ISO 9001:2015 *Quality management systems – Requirements*.

[8] In Canada, accreditation of those offering certifications is provided by the Standards Council of Canada via the International Accreditation Forum (IAF). See https://www.iaf.nu/

[9] Voluntary codes can specify minimum product standards. Not tied to regulatory requirements they may be cited in purchasing documents. See http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca00963.html

[10] Consortia and other quasi-standards writers differ from Standards Development Organizations (SDO) in that SDO's are named in treaties or legislation to develop standards which can be used in regulations while quasi-standards organizations rely upon a level of market penetration and public acceptance.

[11] The WiFi Alliance and Bluetooth SIG are organizations that manage these types of trade marks.

[12] For example, the Institute of Electrical and Electronic Engineers (IEEE) has the IEEE *Conformity Assessment Program* (ICAP) which supports a range of assessments including self-declaration, third party testing, certification and branding. The International Society for Automation (ISA) has the *ISA Compliance Institute* to support certifications to some of their industrial standards.

"Could smart doors compromise the user by permitting unauthorized entry or by excluding the resident?"

an assessment for each instance of a deployment. Furthermore, these systems are often subject to upgrades and revisions, which results in the need for periodic reassessments to ensure continued compliance.

It is also challenging to write comprehensive standards for such systems since each tends to be unique, and a suite of standards applicable to one configuration may omit important requirements when applied to another.

This has led, especially in the utility sector, to the concept of "performance-based regulation".

Performance-based regulation focuses on desired, measurable outcomes, rather than prescriptive processes, techniques, or procedures. It aims to produce defined results without specific direction specifying how those results are to be obtained. Performance-based regulatory actions focus on identifying performance measures that ensure an adequate safety or performance margin. They may also offer ongoing incentives for improvement[13].

Performance-based regulation places the responsibility to identify the measures and standards needed to meet minimum goals on the supplier. While this offers the supplier some flexibility in attaining the goals, it offloads a lot of the technical investigative burden needed to identify these measures and standards onto the supplier and leads to uncertainty about whether they would be acceptable to the regulator. The regulator also needs to have more oversight in the design and operation of the product or service.

Similar approaches have been taken in other sectors where the requirement to meet safety or performance goals have been insufficiently clear to allow specific standards to be developed or where rapidly developing technology has overtaken standards development and acceptance. For example, while many security and privacy standards are being developed, no single set of standards have been accepted which will meet all security goals for all situations. Furthermore, a regulator may be reluctant to specify a specific standard, rather preferring to cite example standards and requiring the vendor to invest in the design and verification efforts needed to identify the most relevant standards and to provide explanations to confirm these decisions[14].

1.5 The role of standards

Standards play a key role defining the requirements with which a product or service must comply and can be used as a foundation for establishing public confidence.

Standards are developed by stakeholders of the technology or process using consensus-building

[13] In Canada, this approach is used by the Canadian Nuclear Safety Commission for some aspects of the regulation of nuclear facilities.

[14] In Canada, this approach has been used in support of federal privacy policy regulation.

activities through a process of discussion, drafting, review and final approval. The resulting standards are published typically for voluntary use and become mandatory when invoked in regulation, cited in contract terms or specified in product documentation.

The processes used to develop and approve standards varies significantly. At one extreme are the formal ("de jure") internationally accepted processes which result in international standards being approved which are compliant to World Trade Organization (WTO) rules. At another extreme, standards may be informally approved if they simply demonstrate a minimum workability and there are no significant objections. In concrete terms, IEC and ISO, have a formal approval process using multiple rounds of National Body voting, while the Internet Engineering Task Force (IETF) relies upon "rough consensus and running code" rather than formal ratification [11].

National standards of Canada are developed or endorsed by standards development organizations (SDOs) accredited by the Standards Council of Canada (SCC)[15]. Specific requirements are placed on the development and approval of such national standards. For example, the content of a standard is typically developed and approved by a committee of the stakeholders affected by the standard[16]. A fundamental part of the development and approval process is that the makeup of the committee, the balloting and the consideration of disparate views between stakeholder groups ensure that a broad range of views are considered. Also, at specific stages in the development process, the public is provided the opportunity to provide input[17].

A variety of private organizations may also produce voluntary consensus standards, including industry and trade associations, professional societies, not-for-profit standards-setting membership organizations, and industry consortia. Such standards may also become accepted by the public or by important industry groups, especially regionally, on par with International Standards.

In other cases, private sector technology may become a de facto standard. When one firm's product becomes sufficiently widespread that its specifications guide the decisions and actions of other market participants, those specifications may become a *de facto* market standard.

Some governments may make some standards mandatory as part of general procurement policy. Federal, provincial, municipal, or chartered city governments may mandate certain standards to protect health, safety, and the environment or to meet general financial or local compatibility needs.

- Interest in "open source" standards has grown within the information technology industry over the past two decades, as they can provide quicker standardization for computer systems. Open source standards differ from traditional standards in the following ways: Traditional standards define the requirements but leave implementation to the manufacturer. This encourages innovation by the manufacturer to efficiently meet the standard's requirements while not constraining how the product is made.

- Open source standards take a different approach. Software which implements the requirements is made available as computer source code along with a license for use. Manufacturers that use this code expect to be compatible with others that do the same. This group development approach can lead to cost savings, fewer errors and a more trusted implementation since the code will be subject to wider scrutiny and bugs or security flaws are more likely to be detected. For example, OpenStack[18] is a package of open source software to implement cloud servers which may address the concerns of users of cloud-based services.

[15] The SCC has currently authorized ten organizations in Canada to develop national standards, including CSA Group. In the USA, the American National Standards Institute (ANSI) performs this role. See www.ansi.org

[16] Complete requirements are found here at https://www.scc.ca/en/accreditation/standards

[17] In the information technology community, a number of technologies are produced by consortia and accepted by developers, such as programming languages such as Java, Python or Ruby.

[18] OpenStack is a community of developers. See www.openstack.org

"Are communications capabilities secure enough to prevent unauthorized remote operation or influence?"

- Open source may also be capable of responding more quickly should problems be detected, and general trust may be improved since the computer code is available and open to wider review by experts. The "open source community" has traditionally promoted the open and unrestricted use of software.

2 Emerging Technology Challenges

Today, with non-ICT technology devices, consumers can confidently travel to a local store and purchase a safe appliance such as a bread toaster, range or refrigerator. Standards, codes and regulations are in place to ensure that the appliance will not shock the user or cause a fire when operated appropriately.

As "smart appliances" become more commonly available, however, some of these assumptions have come under threat. Can a failure of software, such as a "soft" on-off switch lead to electrically unsafe situations? Could a firmware update to the appliance (either intended or fraudulent) compromise the safety of the device? Could remote monitoring of appliance operation reveal use-patterns considered confidential? Are communications capabilities secure enough to prevent unauthorized remote operation or influence?

One might consider the example of a home appliance such as a refrigerator.

Traditionally these have been straightforward appliances with a control system to control the temperatures of the cooling and freezing compartments. Safety measures to prevent electrical shock and overheating, which potentially could cause a fire, are largely invisible and taken for granted by the end user. These safety measures are considered sufficiently important that most jurisdictions mandate their presence and identify trusted parties to certify compliance to corresponding standards. This provides confidence to consumers that any product they use is generally safe.

Any additional properties the consumer may wish, such as fitness for use, quality or longevity, must be identified by other means, for example by reference to consumer reports, product reviews, or simply by relying on the reputation of the manufacturer.

While such an approach has been acceptable in the past, a new generation of "smart" refrigerators are envisioned[19] which use an internet connection to provide support for:

- Performance monitoring;
- End-user remote control;
- Monitoring best before dates and quantities; and
- Placing replenishment orders with selected stores.

[19] Smart refrigerators are currently available, but the feature set may not exactly match the ones chosen for illustration.

These new capabilities introduce new vulnerabilities and concerns for multiple stakeholders, as will be shown in the following sections.

While modern advances in communications and information processing are enabling a range of new products and services, these advances are also challenging the traditional methods of ensuring product safety as well as introducing new challenges related to product and service security.

As part of this study, emerging technology sectors were identified (Social Media, Artificial Intelligence, Electronic Commerce, Internet of Things, Cloud Computing, Healthcare, and Smart Everything), and representative stakeholders were interviewed to identify their concerns. Of importance is the identification of unmet concerns, since these represent the outstanding gaps and challenges to the acceptance of this technology. A key observation from this initial step was that concerns, although expressed in the language of each technology sector and stakeholder group, largely overlap. The summary and conclusions of this initial step, organized by technology area, are contained in Annex B and are analyzed by stakeholder group in the rest of this section.

2.1 Stakeholder concerns and gaps

By citing the concerns from the viewpoint of each stakeholder, it is possible to identify the gaps between the existing situation and a potential future framework designed to addresses these gaps (unmet concerns).

For this report the viewpoints of the following stakeholders are considered:

- **User:** the end-user of the product or service;
- **Regulator:** the enforcer of societal requirements (e.g. government);
- **Assessor:** an organization responsible for testing and certification;
- **Standards development organization (SDO):** an entity that develops and writes standards; and
- **Vendor:** manufacturer or supplier of a product or service.

Table 1 provides for illustrative purposes a correlation between the emerging technologies identified in Annex B with this section on stakeholder concerns and gaps. The table shows that most of the concerns are shared by multiple stakeholders.

During the interviews, it was not possible to definitively identify the specific priority associated with each concern. Rather it was considered sufficient to identify the range and general types of concerns to establish the need for new mechanisms. This section cites these concerns in terms of each stakeholder to ensure that any solution framework addresses the needs of all stakeholders, not only, for example, vendors or users.

2.2 Users

(a) Loss of privacy, information misuse

Potential breaches of privacy and misuse of information is a key area where users have expressed concerns. They have complained about the lack of informed consent and lack of clarity about how their personal information is being used. For smart cities, information may be gathered without explicit consent, may be misused or the gathering of this information may raise excessive surveillance issues. For smart services, users may be forced to trust the vendor of a service since appropriate trusted oversight entities are not available. There is a concern that the service vendor may not be implementing the processes and audit procedures considered essential to protect how their data is gathered, stored, used and ultimately destroyed (forgotten).

For the smart refrigerator example, automated ordering can result in the ability to track user shopping habits and preferences. Smart screens on the door and cameras on the inside can be exploited in ways unknown by the user. End users want to have confidence that the appliance only does what it is supposed to do and that they have control over any information or changes which impact privacy, security, or equipment performance. It is an open question whether this confidence can be conveyed by the traditional manufacturer's assurance designated by their trademark. If not, users may be

Table 1: *Stakeholder concerns per sector*

Sectors (see Annex B) / Stakeholder and Concerns	Social media services	Artificial Intelligence	Electronic commerce	Internet of Things	Cloud computing	Healthcare	Smart everything
2.2 Users							
Loss of privacy, information misuse	✓	✓	✓	✓	✓	✓	✓
Loss of security				✓	✓	✓	✓
Reliance on vendor support					✓		✓
Monetary loss, trust in financial services			✓				✓
Trust in Healthcare, health privacy					✓	✓	✓
Lack of understanding of the technology	✓	✓	✓		✓	✓	✓
Loss of ethical decision-making	✓	✓				✓	✓
2.3 Regulators and legislators							
Public demand for oversight	✓	✓	✓			✓	✓
Need to respond to sudden disruptive technology	✓	✓	✓	✓		✓	✓
Loss of privacy, information misuse	✓	✓	✓			✓	✓
Coordination among Jurisdictions	✓	✓	✓		✓	✓	✓
Distinction between certification & advisory roles	✓	✓	✓	✓		✓	✓
2.4 Assessors							
Need to address multiple regulatory jurisdictions	✓		✓	✓	✓	✓	✓
Call to assess new kinds of products and services	✓	✓	✓	✓		✓	✓
Defining means to assess conformity	✓	✓				✓	✓
2.5 Standards developers							
Privacy standards	✓			✓	✓	✓	✓
Cybersecurity standards	✓	✓	✓	✓	✓	✓	✓
Standards for life cycle assessment of systems	✓		✓		✓	✓	✓
2.6 Vendors							
Concern that regulatory burden will be too high	✓		✓	✓	✓	✓	✓
Concern about public trust	✓	✓	✓	✓	✓	✓	✓
Concern about loss of intellectual property	✓	✓	✓	✓	✓	✓	✓

seeking assurances equivalent to those assumed for product safety.

(b) Loss of security

Users are also concerned that the growing trend to deploy "smart" devices, including IoT devices, and the increasing use of cloud-based services, will open new security vulnerabilities which are outside their knowledge and control. The deployment of an IoT enabled LED light bulb could potentially compromise all other equipment on the same network if it contains a security flaw. A smart refrigerator may provide a back door into the home network, leading to widespread compromise of the user's dwelling. The concern is that vendors will not take sufficient care in the design and life cycle management of their products to ensure that they are safe to use today and throughout their useful life.

Users may be concerned that vendors will not monitor the threat environment or step forward to remedy vulnerabilities to evolving security threats.

(c) Reliance on vendor support

Users are concerned that the products and services are becoming increasingly reliant on ongoing support by the vendor. Computer software products, as well as vehicles, have benefited from such ongoing support for decades, with some updates even provided without user intervention. Such ongoing support can provide important benefits to users and is part of future smart manufacturing plans. Users are concerned, however, that these maintenance operations, potentially applied outside their knowledge and control, will compromise their safety and security, or will not be provided for the product's entire lifetime.

(d) Monetary loss, trust in financial services

Users are increasingly using new financial services, including the use of online purchasing, smartphone payment systems, and potentially, new cryptocurrencies. Users are concerned whether they can identify and trust these new services to protect them from loss, and to keep financial details private. Users will want to be confident that the services are provided as promised and that the provider will stand behind any guarantees should problems arise.

(e) Trust in Healthcare, health privacy

The introduction of ICT into the health care sector has increasingly benefitted users. New clinical tools, information sharing, and remote monitoring are promoting more innovative and personalized approaches to health care. Users are concerned, however that this detailed health information might be misused and want to ensure that detailed personal data, including data from remote health monitoring, is only provided to entities that they have authorized. Users rank privacy and security as critical requirements associated with their health data.

(f) Lack of understanding of the technology

As highlighted by the recent Congressional testimony of Mark Zuckerberg[20], both end users and regulators (legislators) have raised privacy, ethical and social concerns. They have also had difficulty understanding the technology, its capabilities and complexities, and the policies and controls implemented by the vendor of the service. Many users are concerned that the parameters of these new services are not easily explained using plain language. "Terms of Use" agreements are generally obscure to the point of being opaque to the average user.

(g) Loss of ethical decision-making

Users are concerned increasing automation, including artificial intelligence and computer self-learning, will begin to erode their ability to ensure that the equipment they use (or drive) will operate consistently with their own ethical framework. This is a growing concern largely brought on by the introduction of autonomous driving systems, although this concern applies to all automation systems. Some of the concerns are:

- that the behavior of these systems will be defined by potentially unknown technical designers;
- that the rules used by learning systems to modify behavior will be set by others and may not reflect the beliefs and priorities of the user (for example, the rules may prefer self-survival over human life); and
- that the user will lack influence, since behavior modification will depend upon a history of previous system experience and the details of particular, and likely unique, situations.

Wrong decisions might be made resulting in undesired outcomes, and users are concerned that responsibility for these bad outcomes may end up resting with them.

2.3 Regulators and legislators

(a) Public demand for oversight

After the revelations about Facebook's failures to protect user data, the public is increasing its demand for more oversight of these new services, including social media. Establishing appropriate policies to address societal requirements and the expectations of the public will prove difficult for regulators and legislators.

[20] Airbnb, Uber, and Lyft are examples of such cases.

"Is my smart home safe for me?"

Many emerging technologies, e.g., the proliferation of IoT devices, will evoke similar regulation and legislative concerns. If other tools to ensure public trust are not available, regulators and legislators may be forced by public pressure to fill these gaps.

(b) Need to respond to sudden disruptive technology

It is becoming common for new services and products to be suddenly introduced which could significantly impact traditional society. Technology disruption can lead to social disruption, as new technologies may use business approaches that are incompatible with the jurisdictions (e.g., cities) in which they intend to operate[20]. These new technologies may be introduced suddenly, with little time for legislative and regulatory entities to prepare. While end users might rely on "web ratings" provided by third parties, cities, municipal regions and provinces cannot meet public expectations of safety, security and assurance of a level playing field for all businesses in their jurisdiction from the same kind of source. There is a concern that traditional legislation and regulation is too slow, and the technical capabilities of smaller jurisdictions are insufficient to respond to these new technologies without the help of others.

(c) Loss of privacy, information misuse

The use of the information aggregated by social media services has raised concerns with regulators and legislators that this information can be misused for improper political or other uses. Policies are needed to define how data may be obtained, retained, shared with others, and used. Regulators are also concerned about the lack of an international assessment and enforcement structure to ensure universal application throughout the world.

In the smart refrigerator example, appliance regulators must now be concerned with security issues and end-user privacy, where previously they were not.

(d) Coordination among Jurisdictions

Coordinating regional, national and international standards is a longstanding concern. Even today, for the Canadian Electrical Code, slight differences exist for many regions in Canada. However, with the rapid deployment of new services and products (e.g. with the widespread deployment of IoT devices and provision of cloud services) agreement on common regulatory practices will become essential. This change occurs because these products and services challenge existing regulatory approaches, and because their development and deployment will be global rather than regional. Long term solutions, therefore require internationally applied acceptance plans. This coordination must recognize the legality of jurisdictional regions since responsibility for privacy, health and many other subjects impacted by these technologies may reside at provincial or even municipal or city levels.

[20] Airbnb, Uber, and Lyft are examples of such cases.

(e) Distinction between certification & advisory roles

Regulators, as well as assessors, may be called upon to provide advice and a process to ensure compliance with requirements. When specifically identified standards cannot be cited, applicants may seek the advice of the regulator on what is needed. However, a regulator explicitly specifying a standard, even in an advisory role, could be interpreted as endorsing the standard and its suitability for use. Regulators are concerned that being overly prescriptive in citing specific standards may later restrict an assessment. Two competing factors are at play: on the one hand the regulator may wish to assist in identifying the standards to be used, but on the other hand, regulators may be insufficiently informed about the details of the product or service to be able to specify a definitive list of the standards needed prior to full details being available.

2.4 Assessors

(a) Need to address multiple regulatory jurisdictions

A common concern of assessors is that the criteria they use may need to vary from one jurisdiction to another. Clearly they want to provide their services in a uniform manner, both nationally and internationally. A framework for the mutual recognition of test results has been possible for the electrical safety of numerous traditional products for some years. However, extending these frameworks to address more complex ICT products and services, including requirements beyond electrical safety, and to address the full life cycle, is a significant challenge. Even for the assessment of electrical installations, there are 16 jurisdictions in Canada[21]. In the USA the number is far larger.

(b) Call to assess new kinds of products and services

The need to assess these new products and services will require assessors to define and develop suitable processes and procedures. They will need to be better able to assess any ICT contained in these products and services. The new services will call upon a range of skills which have traditionally been used primarily by manufacturers and vendors, not assessors. Recruiting the relevant system and software engineering expertise, as well as the relevant functional safety and security expertise, needed to provide these new types of assessment is a cause for concern. This concern is shared with standards development organizations and will be discussed further in section 2.5.

(c) Defining means to assess conformity

Assessors may be concerned that they are not ready to provide the full suite of services required to address these new technologies. The publicity arising from recent privacy and security failures has led to growing public and legislative demands for regulators to provide additional oversight of these new products and services. Absent other options, it will fall upon assessors to implement the detailed work to support this oversight. These technical systems are highly complex and each implementation unique, requiring an assessment for each instance of a system, and regular reassessments over its operating life. Furthermore, a simple test for security and privacy is not feasible, since these assessments must examine the capabilities of the vendor as well as the overall lifecycle of the product or service, from design to ultimate retirement. Clearly this will represent a significant challenge to many assessment organizations.

In the example of the smart refrigerator, firmware updates may compromise the original assessment, thus assessments must cover the full life cycle of the appliance. In order to do this, there should be an assessment of any firmware update before it is made available to the end user.

2.5 Standards developers

(a) Privacy standards

Current legislation and regulations do not identify specific privacy practices. Even the European GDPR only identifies general principles and requirements. Rather, should an incident occur, a request generally is made to explain what procedures are being followed to ensure they meet "due care". While not specifying any particular standards, good practices might cite general guideline standards such as ISO/IEC 27002 [9]. SDOs

[21] In addition to the provinces 'Chartered Cities', such as Vancouver, Calgary, Winnipeg, St. John's maintain their own jurisdiction. In addition, the Provinces do not have legal jurisdiction to enforce safety and security requirements within federal jurisdictions, although special arrangements for local inspections may be used (e.g. for Airports, federal buildings).

will face significant challenges to establish the technical controls and functions needed to meet regulatory and user concerns related to privacy.

(b) Cybersecurity standards

It is difficult for existing safety and security standards to keep up with the rapid introduction of various ICT in products and services. All products are impacted, from consumer electronics and telecommunication equipment to large scale industrial facilities. Traditionally each sector has approached cybersecurity very much from its own perspective. The financial sector has developed its own standards in support of payment and banking systems, electrical utilities define standards for the electrical grid, industrial automation has developed its own standards, and so on. This has resulted in a proliferation of standards, sometimes coordinated, sometimes not. This proliferation has led to some duplication, as well as gaps in the menu of standards available. A key concern of SDOs is the loss of efficiency resulting from this proliferation and the need to identify the standards are the most applicable in each case.

(c) Standards for life cycle assessment of systems

Systems management standardization will need to better address the ICT issues of complex systems over their complete lifecycle from design to retirement. These are complex systems requiring a formal system engineering approach. Standards will likely also be needed to identify the skills needed to work in this "systems" environment. For example, the "Skills Framework for the Information Age" (SFIA), consortia[22] are working on the identification of skills, maturity levels for appropriate skills, and with specific qualification and certification procedures. The general trend for systems management standards is to assess and certify the skills needed for these complex systems.

2.6 Vendors

(a) Concern that regulatory burden will be too high

Vendors are concerned that, if regulator and user demands are met, it may result in a regulatory framework that is incompatible with their business models or too costly to implement. It is clearly important to balance the concerns of all stakeholders, but standards should be capable of being implemented in a way that takes into account the input of vendors. Vendor concern revolves around the potential exclusion of their input, possibly based on the rationale that their input cannot be trusted.

(b) Concern about public trust

Vendors are also concerned that the continued publicity of breaches and failures will erode public trust in the services and products they supply. This loss of trust may erode their success in the market, and once lost it may take a very long time for it to be regained, if ever. For new entrants, establishing initial trust may represent a significant barrier to the introduction of a new product or service. Vendors may be interested in new ways to anchor trust in their product by working with a third party who is already trusted by the public.

(c) Concern about loss of intellectual property

Finally, vendors are concerned about maintaining their intellectual property while, at the same time, revealing sufficient information to establish public trust. While agreements to protect intellectual property might be possible for regulators and assessors, making such agreements with the general public is not possible. In most cases for these new systems however, it is public trust that is needed.

3 A framework to address stakeholder concerns

During the interview process some basic gaps were identified that need to be filled:

- There need to be a better way of ensuring that communications between complex product and service vendors and users (and governments) are clear and unambiguous.
- Practices related to the application of standards, and the assessment of compliance to these standards need to be upgraded since these new ICT products and services tend to be unique and subject to significant variation in use during their life.

[22] SFIA Consortia is a product of the Open Group and is available from https://www.sfia-online.org/en.

- These new complex products and services require new confidence building systems so that public trust can be retained and sustained into the future.
- Intermediaries are needed, armed with standards and certification schemes, who can impartially test and examine these systems and offer the trusted assurances to those unfamiliar with the technology that allows them to use these systems and services with confidence.

Users need to have access to the assurances, available from sources they trust, that the products and services they use comply with their requirements. For complex products and services, it is unrealistic to expect that the general user (or governments) will have the background necessary to conduct first-hand assessments. Furthermore, vendors will be unwilling to release publicly confidential design details.

Figure 2 presents a framework that is proposed to help in responding to these questions. This figure extends Figure 1 to incorporate the additional elements needed to address the identified gaps and to address the provision of services.

The "deliverables" in this framework are identified in the lower part of the figure. Policy descriptions represent assessment operations and will be described in section 3.3 after the descriptions of the policy and practice deliverables provided in the next sections 3.1 and 3.2.

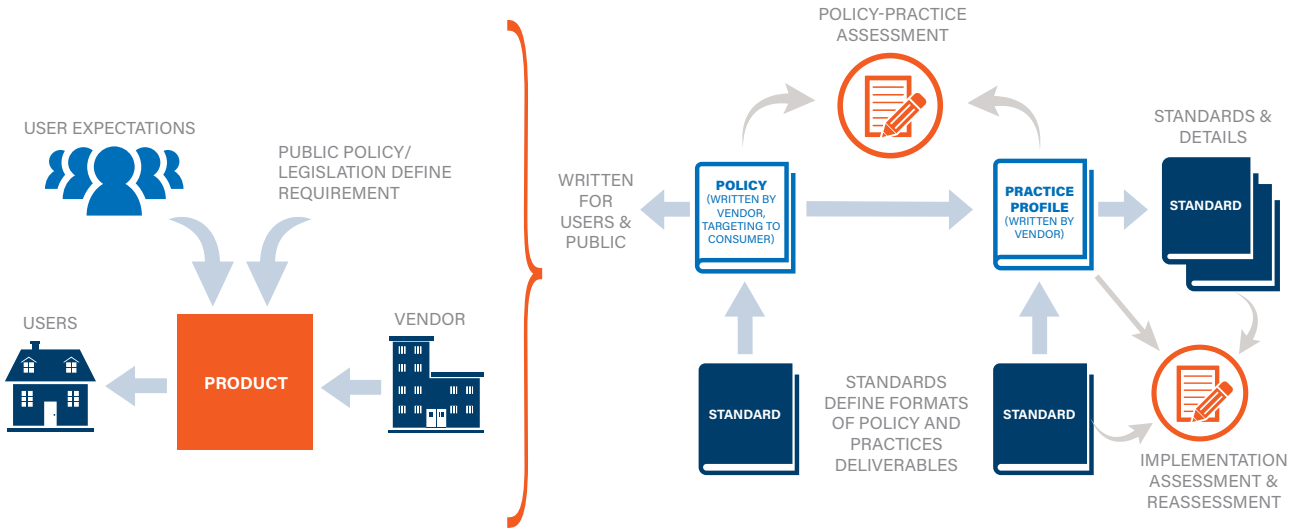
3.1 Policy descriptions

Policy descriptions already exist in part today, often forming part of the agreement[23] the user is expected to approve prior to using a product or service. They also share some similarities to the "voluntary codes" which were previously mentioned in section 1.3. The main difference between these existing agreements and codes, and a policy description are that:

- The format and content of this document would be defined by a standard, and
- Additional details related to the promises made by the product or service provider to the user and to meet public policy requirements, must be included.

Such descriptions will need to address both legal and technical issues, requiring experts in multiple fields. Policy descriptions, defined prior to product or service

Figure 2: *Proposed framework for emerging products and services*



[23] Most if not all online services require the user to agree to a "terms of service"[6].

delivery, are expected to be stable, and would remain largely stable over the life of the product or service.

Policy descriptions should be available at no cost to allow wide user and public review. This facilitates their endorsement by other parties since many end users may not fully read these documents, relying instead on regulator, peer or trusted third-party endorsements[24].

Policy descriptions should be standardized and significantly extend existing "terms of use" agreements. By defining a standard format, it becomes easier to assess completeness, and permits the comparative assessment of similar products and services.

A standard defining how policy descriptions are written would require flexibility to allow a range of potential products and services to be described to a general audience. One size is unlikely to fit all, but general categories of products and services may be amenable to similar formats. The recent European GDPR (see annex B.1) provides an interesting example of some of the required content that would be provided in policy descriptions.

The standardization of policy descriptions must meet both the requirements of end users and public policy and must be capable of being assessed against a corresponding practice profile as will be discussed in section 3.2.

3.2 Practice profiles

One or more practice profiles[25] would identify how the vendor meets the policy description[26]. These would provide an interface between the public facing commitments of the vendor (defined in the policy description) and the internal technical operation of the product or service. Their content may be confidential, and made available only to an assessment organization.

Profiles must be written by vendor experts with wide knowledge and expertise. Vendors must avoid creating new standards. These documents should profile existing standards and identify the levels and degrees of compliance needed[27]. Practice profiles would also identify whether performance-based methods are expected to be used to meet some policy commitments.

The format of these profiles should be aligned with the policy description format to allow an assessment of the adequacy of the practices and associated controls. However, as noted earlier, the specific practices needed will typically be unique based on risk assessments and the technology being employed. Furthermore, practice profiles may need to be updated to meet evolving threats or to accommodate evolving technology.

3.3 Assessment standards

In Figure 2, two assessments were identified. These are required to confirm:

a. That the practices and associated controls are sufficient to meet the policy description; and

b. That the service or product implementation faithfully implements the practices and associated controls defined in the practices profile.

A range of assessment approaches may be needed depending upon the type of performance profile promised. For safety, privacy and security profiles, high confidence will be required, calling for correspondingly highly reputable assessments. For less significant profiles, e.g., promises related to service availability, less stringent assessments may be sufficient.

[24] These freely available descriptions would be available for general public review and comment. For critical elements, regulatory entities may endorse certain relevant clauses of the policy description. Less critical elements might be the subject of traditional consumer reviews.].

[25] There may be multiple profiles cited for a single product or service. For example, vendors may choose to define "information privacy" issues in separate documents to more flexibly meet regional legal requirements.

[26] As indicated earlier in footnote 25, the Certification Practice Statement (CPS) is used to define the practices associated with a public key certificate service. Thawte combines policy details with their corresponding practices in a combined CPS. See https://www.thawte.com/cps/

Note however that it is expected that most Practices documents will be confidential.

[27] Degrees of compliance refers to the extent of the measures taken. This often depends upon a risk and security assessment of the planned product or service. Many standards offer options on the extent of the measures required and these must be selected based on a risk assessment.

"For safety, privacy and security profiles, high confidence will be required, calling for correspondingly highly reputable assessments."

Splitting the assessments into two steps aligns these functions to the product or service lifecycle.

- The first step, assessment of compliance between the policy and practices can be carried out prior to product or service deployment, and reassessments would be limited to any changes made in the policy or practices.
- The second step, assessment of an implementation is more complex since it must have a wider scope, to verify that the vendor is deploying suitable staff and putting into place the management structure needed to ensure full lifecycle compliance with the practices profile. Performance-based methods, as described in section 1.4 might be applied in more complex cases. Implementation upgrades and changes would also need to be monitored to ensure continued compliance.

4 Conclusion

During this study it became clear that for these new ICT products and services:

A new framework is required to identify the needed standards and assessment services.

Section 3 provided an initial suggestion for a framework to address the concerns of each stakeholder type. Significant input would be required from all stakeholders, especially regulatory, assessment and standards development stakeholders to validate and refine the framework. A key portion would be the validation of this framework's ability to provide the levels of trust demanded by each stakeholder type. Each component of the framework needs to be supported by an appropriate business case.

Funding models are required to support the development of standards, the provision of policy descriptions and profiles by vendors, the development of assessment methods and tools, and the assessments themselves. Traditional funding from component manufacturers and large user groups, such as those in the electrical utility sector, may be significantly reduced for these new ICT intensive products and services. For these services, service delivery systems are constructed using custom assemblies of components, with component manufacturers only indirectly involved with the service provider's system design and operation. Standards and assessments will need to concentrate on the service provider's design of the service delivery system and its ongoing operation.

New ICT products are being bundled with technical support systems which must be assessed along with the products themselves. For example, some home lighting and appliances integrate ICT and wireless technologies that allow internet access, vendor post-delivery support must be present to meet the expectations and policy promises of the vendor, especially related to ongoing safety, security and privacy.

A gap exists in the availability of globally acceptable criteria applicable to the new products and services.

Users and legislators, in Canada and world-wide, are expressing high levels of distrust in the new generation of products and services being deployed [3][13]. With globally provided services, and concerns which bridge national jurisdictions, there is a strong case to be made for the need to define globally acceptable criteria. There will likely be significant international interest on the part of vendors to develop such internationally acceptable criteria, since their absence would likely result in the creation of multiple national or regional criteria with less coordination (as has been the example of the EU GDPR) and resulting in higher overall implementation costs.

These criteria could be constructed in the form of voluntary standards, much like voluntary standards today, leaving jurisdictions the option to mandate their use. These standards would define the required content for policy descriptions if implemented using the framework of section 3.

This is not meant to imply that such criteria have not been developed in the past. Rather the use of the international standards system to reach consensus on such criteria is possibly not being fully exploited. Traditionally some international standardization parties have objected to the development of standards aimed at being cited in regulation[28]. However, increased emphasis on addressing societal needs has been identified[29] and international work has already begun to develop global ethical standards[30].

There is a need to extend the kinds of assessments available and to ensure that assessment products become available more quickly to match the rapid pace of development and deployment of ICT products and services.

The ability to quickly deploy new products and services has stressed existing assessment and regulatory systems. Systems need to be created whereby assessment services for corresponding standards are available quickly, possibly even before the corresponding standards are fully mature. Assessment organizations will need to be more involved in the development of standards so that both the standards and the corresponding assessment programs are available earlier than is the typical case today[31].

New assessment services should be considered which are not directly driven by regulatory demands. For example, the pre-qualification of designers or opinion-providers, such as those providing consumer reviews, might be considered. This would allow some level of trust to be established for subsequent self-provided or third-party-provided product or service opinions[32]. These new assessment services would include the assessment of the capabilities of an organization, as well as the full life cycle assessment of a product or service.

[28] In the past, some vendors tended to avoid the development of standards that could be mandated by legislation. However, public demand for regulatory oversight may encourage increased vendor involvement to ensure that corresponding standards are not unreasonably restrictive.

[29] The current (2018) IEC Masterplan identifies the need to better address societal needs. See http://www.iec.ch/about/brochures/strategy.htm

[30] The Institute of Electrical and Electronic Engineers (IEEE) has a "global initiative on ethics of autonomous and intelligent systems. See https://ethicsinaction.ieee.org/. The IEC Standardization Management Board has established ad hoc group 79 *Autonomous Systems – Ethics* (with IEEE and ISO participation) on how to address these issues across IEC sectors.

[31] Traditionally, conformity assessment designers did not get directly involved with standards-setting. Thus, assessment programs for specific standards were delayed. Recent decisions within the IEC between the Conformity Assessment Board (CAB) and Standardization Management Board (SMB) are promoting the increased cooperation between standards developers and conformity assessment designers.

[32] As discussed in Section 4.3.1, some less critical elements of policy descriptions may be reviewed by traditional consumer rating entities. The methodologies used, and ratings assigned, by these entities could themselves be assessed to ensure that they meet minimum public trust requirements.

Annex A: Topics for further investigation

A.1 New framework for standards and assessments

Relevant discussions will be required with regulator, assessment and standards development stakeholders. This work should concentrate on the overall feasibility of the approach, identifying example cases where similar methods are in use and where such experience can be used to refine the proposed framework. For example, as indicated earlier, volunteer codes and performance-based regulation appear suited to this approach.

Validation and adjustment of the framework will be needed, including the scope and character of:

- Policy description standards;
- Practice profile standards; and
- Assessment tools and approaches, noting that three types of assessments are identified:
  - Assessment of the policy description to the standards that define policy descriptions;
  - Assessments between policy descriptions and practice profiles, and
  - Assessments of compliance between practice profiles and the actual design and operation of a product or service.

Policy descriptions are likely to become complex and most end users may wish to rely on opinions provided by volunteer reviewers. Therefore, it will be important to determine whether a population of such volunteer reviewers exists to provide these services[33].

Pilot projects might be considered to test applicability, such as those identified in subsections A.2 and A.3.

A.2 Globally accepted criteria for new products and services

Identification of critical subjects that require the development of international consensus on public policy criteria applicable to the new generation of products and services is needed. A survey of candidate topics should be carried out. These topics could then be prioritized and linked to current international activities in corresponding areas. Support should then be provided that would accelerate the development of consensus criteria with the ultimate objective of reaching international agreement.

Potential topics include:

- All ethics as discussed in section 2.2;
- An extension to one or more voluntary codes (see Section 1.3) based on an existing code; and
- An extension based on the EU GDPR to address its international use

A.3 Assessment flexibility

An opportunity exists to investigate the provision of a wider range of assessment services. The range of services can be extended to include the provision of full life cycle system level assessments of organizations, and products and services[34]. This is a very large topic

[33] It is not clear that just providing more comprehensive policy descriptions and expecting end users to evaluate them is sufficient. It is likely that consumer-driven peer reviews of these descriptions will be required (in addition to regulatory reviews for important aspects).

[34] The IECEE has already introduced the optional CB-FCS (Certification Bodies - Full Certification Scheme) to cover product manufacture [7]. However, the assessments identified in the proposed framework would require further extensions to cover more phases of a product or system lifecycle. For example, adding assurances related to post-delivery support by the vendor. See https://www.iecee.org/about/cb-fcs-scheme/

since many new types of assessment services might be considered.

Potential assessment topics include:

- Assessments against privacy and security standards[35];
- Assessments against safety standards, and their coordination with security standards[36]; and
- Assessment of evolving standards before they are fully mature, e.g., evolving data misuse and product and service trustworthiness[37] standards.

[35] Many relevant security and privacy standards are still being refined and need assessment designer input if companion assessment services are to be provided promptly.

[36] Security standards were originally developed primarily to protect information; however when applied in safety-sensitive situations, additional considerations are required. In these situations, safety and security requirements are sometimes in conflict, complicating their application. Since this impacts consumer safety and security, regulatory oversight is expected.

[37] Trustworthiness has many interpretations, but the sense here is that the need to ensure that the product or service actually delivered is the one expected to be delivered, including counterfeit prevention. Several working groups in the IEC and ISO are contemplating the development of trustworthiness standards.

Annex B: Analysis of stakeholder concerns in emerging technologies

More than 20 stakeholders were interviewed from the emerging technology sectors as part of the initial analysis phase. Their responses and concerns are documented in this annex. Additional information was gathered from related literature and by drawing on the experience of the authors. Representatives from different sectors expressed similar concerns, since they are all leveraging new technologies with similar impacts.

We noted that concerns mainly differ depending upon the stakeholder's role. For example, end users of a product or service have concerns different from those of the supplier. While addressing user and regulator concerns is a key aspect of this report, it is important to also recognize that these systems must address vendor concerns as well (e.g. intellectual property rights, and the potential delays and costs related to implementation). An approach was used which is loosely based on the initial steps of the systems engineering approach for the identification of system requirements[38].

Note: the "system" in the context of this report is the system of standards and supporting assessment and accreditation components necessary to ensure public and societal acceptance of future complex ICT based systems, products and services. It does not refer to a specific technical physical system.

Any product or service has many stakeholders who have concerns informed by their experience in the sectors where they work. For example, city planners will tend to emphasize concerns related to smart city deployment and operation. Also, some stakeholders fulfil multiple roles, e.g. a stakeholder may be a user of some products and services while being a vendor of other services.

Subsections B.1 through B.7 identify concerns related to the following specific emerging technology sectors:

- Social media services (section B.1);
- Artificial intelligence (AI) (Section B.2);
- Electronic commerce and cryptocurrencies (Section B.3);
- Internet of things (IoT) (Section B.4);
- Cloud computing (Section B.5);
- Healthcare monitoring and information sharing (Section B.6); and
- Smart "everything" (Section B.7).

These concerns are expressed from the viewpoint of each relevant stakeholder of the system. In section 2.1 of the main report these concerns are summarized and organized from the viewpoint of five system stakeholders:

- Users;
- Regulators;
- Assessors;
- Standards developers; and
- Vendors.

B.1 Social media services

Probably the most visible and newsworthy ICT-intensive emerging technology today social media services. Many of these social media services have shown explosive growth in recent years. Global deployment of these services is fundamentally challenging the trust that users place in the social media services they use.

[38] This approach is popularized in a number of standards such as ISO/IEC/IEEE 42010:2011 [10], *Systems and Software Engineering – Architecture description,* and The Open Group's TOGAF work. Specifically, in TOGAF 9.2 it represents the initial steps of the "Architecture Vision" phase.

Social media services are often based on the creation of large data sets and the expanded ability to analyze and use this data in new ways. Recent news articles, such as Facebook's apologies[39] have highlighted end user and government stakeholder concerns that these "new ways" may violate the trust users place in these services.

Companies, both national and international, can now collect vast amounts of data, often gathered without the user's specific knowledge. Routine activities can be monitored to obtain accurate replays of day-to-day activities, explicit or implicit interactions with others, mobility histories, online search and social media activity, chats, emails and many other details which enable highly accurate modeling of the user's psychological profile. This is a level of privacy loss never seen before.

The ability of these new systems to reach large populations of users, to assemble large volumes of data, and to derive conclusions from this data, have led to widespread concern. While some of the use of this data may benefit end-users, e.g. by providing "user experiences" tailored to specific user interests, it also raises concerns about data privacy and security, and how this information could be used for targeted manipulation of users and populations. There are obviously big questions about who has access to this information and how it might be used.

Recent experiences have also made it clear that not only do most users often not understand the ramifications of the usage of these services, but also many legislators may not understand the technology, and many vendors appear to have great difficulty communicating what they are doing. While the visible day-to-day use of the service may be known, less obvious aspects may be unclear, and may not be been fully understood even by the vendor. "Terms of Use" agreements are usually too complex, are not easily understood by users and do not clearly address all user concerns. They are often accepted without much thought.

Furthermore, vendors may not fully realize how sensitive end-users can be when those users are apprised of the full ramifications of the service. Vendors may also be concerned that this public concern, coupled with the societal concerns identified by governments, may result in the imposition of regulations[40] which they consider incompatible with the technology or business models upon which their services are based.

The European General Data Protection Regulation (GDPR)[41] represents the first major attempt to regulate some aspects of these new services. These high level requirements are significantly impacting the way these services are provided globally. Vendors world-wide have been forced to address GDPR requirements as they deploy global services to global users.

B.2 Artificial Intelligence (AI)

Artificial Intelligence and machine learning, while promising benefits to end-users, also leave many complex social, political, and ethical questions unanswered. AI systems improve performance by making new decisions based on huge volumes of data and continually adapting by incorporating new data partially resulting from those decisions[42]. After a period of time, it becomes difficult to fully understand how such systems will react, since their behaviour is based on a complex history of learning. This lack of understanding is already a significant issue for economically critical and safety-critical systems since systems like this cannot currently be comprehensively evaluated and tested.

If a smart system, like an autonomous car, is compromised, the consequences can be disastrous. However, since the technical understanding of how these systems operate will often be unclear and based on a complex learning history, the presence of

[39] "Facebook's Zuckerberg apologizes to U.S. Congress, vows to do better", Associated Press, April 10, 2018.

[40] "Facebook's Zuckerberg says regulation of social media firms is 'inevitable'" Associated Press, April 11, 2018.

[41] General Data Protection Regulation (GDPR). See https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[42] In classical analog electronics, positive and negative feedback in amplification systems like this can be highly unstable and require great care to ensure stability.

compromise may be almost impossible to detect using traditional methods. Thus, high priority must be given to securing the perimeter around these systems to prevent compromise.

AI–based automation can make critical decisions in real-time. Although the right decision can often be determined by objective analysis, there are some examples where significant ethical and moral issues will arise. For instance, an autonomous car which knows that it is about to hit a pedestrian, must decide if it will try to avoid the pedestrian using a risky (to its passengers) maneuver. This decision may need to be decided in milliseconds and the "right" decision may depend upon who influences it (the pedestrian community, the driver community or the passenger community). The AI-based system must decide based on a complex learning history where matching data and events may never have been seen before.

Considerable investments are being made today in the development of AI, both at the scientific/engineering level, at the commercial level and at the product development level. Technology giants with massive data sets have a significant advantage, as they have access to large volumes of information describing a wide range of human activity (searches, communication, content creation, social interaction and more), in many different formats (text, images, audio, video). Much of this research and development can result in effective AI-based technology which can provide their owners with tools that can be used to significantly influence public opinion. A similar concern was discussed in the previous subsection regarding the misuse of large social media data sets.

Regulators and legislators will likely face significant challenges in defining standards for the acceptable ethical behaviour of technical systems. Even if such standards are developed[43], compliance assessment will be an ongoing challenge. This assessment challenge occurs because it is not clear that AI systems will have stable and predictable behaviour, because, like humans, their behaviour is modified by experience.

B.3 Electronic commerce and cryptocurrencies

Electronic commerce refers to the wide range of tools and techniques utilized to conduct financial business in a paperless environment. ICT systems have long underpinned this sector. For example, EMV (Europay, Mastercard and Visa)[44] is a global standard for chip-card transactions. EMV is a generally accepted industry standard which supports interoperability between all host systems, payment devices, and cardholder devices.

Traditional payment systems are expected to continue to advance, with the deployment of distributed financial systems. PayPal, Apply Pay, Google Pay, Samsung Pay[45] are all examples of these new approaches.

Users have traditionally relied on card issuers and their banks to enforce and guarantee the security of their transactions. This traditional trust model may come under threat as users must transfer their trust to other providers or to equipment (e.g. smartphones) from other sources.

New "cryptocurrencies", are being offered which no longer rely on traditional financial infrastructures. Cryptocurrencies such as Bitcoin[46] are decentralized

[43] Several standards developers are embarking on projects to define ethical behaviour standards for automation. The IEEE has a website dedicated to "Ethics in Action": https://ethicsinaction.ieee.org/

[44] Though EMV are the initials of the original creators of the standard that underpin this technology, the standard is now managed by a consortium including Visa, MasterCard, JCB, American Express, China UnionPay, and Discover. This EMV standard references a number of other standards, including ISO/IEC 7816 *Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange and ISO/IEC 14443 (Cards and security devices for personal identification—Contactless proximity objects—Part 1: Physical characteristics)* for chip-based payment (e.g. credit) cards.

[45] PayPal with over 200 million accounts, primarily supports online web payments. See www.paypal.com
Apple Pay provides a contactless payment service for smartphones. See www.apple.com/ca/apple-pay
Google Pay provides a contactless payment service for android phones. See pay.google.com
Samsung Pay also provides a contactless payment service. See www.samsung/ca/Samsung-Pay

[46] Bitcoin is one of a number of blockchain-technology based financial systems. It is based on the use of open source software (see Subsection 1.5). See www.bitcoin.org

digital currencies with no central banker or single administrator. Rather than relying on strong financial enterprises and governments to ensure trust and security, this technology relies on a distributed international trust model which depends on public acceptance of its underlying crypto-technology. This is one of the ultimate tests of public acceptance.

National governments and international decision-making bodies are still coming to grips with the impacts of the introduction of cryptocurrencies. This technology can potentially circumvent international laws and agreements and can become vehicles for increased criminal activity. Furthermore, governments often impose controls on national currencies to stabilize their national economies. Significant cryptocurrency use may ultimately limit some of the economic levers available to governments.

Regulators and governments are concerned that the use of the new financial instruments may no longer come under their jurisdiction.

Assessors who participate in existing schemes (e.g. EMV) are concerned that they will be asked to assess the trust of attached systems which they traditionally do not examine. For example, online credit card payments may be processed by consumer-owned components traditionally outside their domain of responsibility. They may also be concerned about the need to expand beyond the current single integrated scheme (e.g. EMV) into new areas such as cryptocurrencies, and the assessment of end user devices (e.g. smartphones).

SDOs will face new challenges in developing the standards necessary for the new cryptocurrency technology[47].

Vendors of traditional security services, i.e. existing financial institutions, are concerned about the security of the external systems to which they need to interface.

Vendors of new services will likely need to address regulatory/legislative requirements if they are to provide financial services to the public.

B.4 Internet of Things (IoT)

The term "Internet of Things" is generally used to refer to the ability to cost effectively deploy large numbers of devices which can send information to, and receive information from, related devices over global networks such as the internet, and react to this information by altering the physical world[48]. A wide range of devices is included under the IoT category, including human-wearable sensors to home automation devices, environment sensing devices and actuators. Key drivers of the technology are advances in information processing (computers) and cost effective and ubiquitous communications technology. IoT is expected to play major role in supporting a range of "smart" sectors, to be discussed later in section B.7.

There are many challenges related to the deployment of IoT. Clearly safety, security and privacy are major issues.

The introduction of IoT devices extends the perimeter of traditional networks and introduces new targets for exploitation. As consumers, businesses and governments begin to deploy seemingly "innocent" IoT devices, which are then connected to the internet, additional vulnerabilities may be exposed. Since these devices are expected to be deployed in large numbers, the exploitation of a single security flaw could have widespread impacts. Such flaws have already been exploited to generate a number of world-wide attacks.[49]

Many current standards are not well suited for application to products and services which employ IoT technology. Most current system designs with critical performance requirements have assumed that when used they will be physically isolated from the outside world[50]. The interconnection of many devices, such as

[47] ISO has established a new technical committee, TC 307, to standardize blockchain technology, which forms the basis for cryptocurrencies (and other applications). However, their success in developing standards actually used by these new cryptocurrency vendors is difficult to predict.

[48] A more formal definition of "Internet of Things" can be found in Clause 3.28 of ISO/IEC DIS 20924.

[49] The availability of millions of devices with a common flaw lends itself to denial of service attacks, although other attacks are also possible.

[50] The past 60 years abound with techniques to permit computational systems to show guaranteed performance when sufficiently simplified and restricted. This applies to real time systems [1], specialized network protocols, aviation systems, etc.

happens with IoT, can violate the premises used to verify the critical properties and can open failure paths and attack vectors.

The proliferation of low cost IoT components within such architectures introduces concerns since low-cost ubiquitous devices are generalized, and have superfluous functionality not required by the particular use of the device. Such functionality cannot be disabled by a particular instance, presents a larger attack surface, and may be more susceptible to responding to unexpected triggers. Work is on-going in a number of standards committees to examine the impact of the wider use of IoT devices[51].

Tomorrow's networks are likely to be highly interconnected as IoT devices become more common. The widespread availability of these devices to the general public[52] will increase the exposure of the technology to both good and bad actors.

Users of IoT components share many of the concerns of users of data aggregation since essentially their information, although potentially resident within their IoT device, may be visible to the world and subject to exploitation. In addition, security concerns arise related to potential outside interference with the operation of these devices.

B.5 Cloud computing

"Cloud computing" generally refers to the movement of traditional processing from within the domain of the user, to an external provider ("somewhere on the internet"). Rather than deploy computing resources in-house, a user may contract with an external provider for the processing required. Cloud computing is popular since external providers can use economies of scale to cost effectively deploy large computer "farms" to provide bulk processing and each user's peak processing demands can be averaged over many users. With these economies of scale, and the ability to deploy the computer farms in multiple locations, enhanced reliability and availability can also be offered to customers.

Cloud computing has become popular with many business and organizations. Depending upon the size of the organization, they may be diligent in assuring that the services they use are secure, reliable, and that their data is not misused[53]. However, some organizations may not have the capabilities needed to fully assess the cloud service, and some cloud service providers may be unwilling to reveal sufficient details of how they provide the service.

Cloud computing is also sometimes offered to augment the performance of products delivered to end users, e.g. to augment processing to support voice recognition. Many home automation systems, for example, rely on a connection to the "cloud" to offload some processing, interconnect to other vendor systems, or provide customers with an "internet portal" accessible when they are away from home. Google Home™ [54] , Amazon Echo™ (Alexa)[55], Apple HomePod™ (Siri)[56], Samsung SmartThings™ [57], and even the Lutron Caséta™ [58] home automation, each use an internet connection to cloud based servers.

The requirement to open a channel to the internet exposes existing systems to additional outside threats. The information stored in the cloud may be vulnerable to alteration or misuse, and its improper manipulation may negatively impact local equipment operation.

[51] ISA 99, responsible the development of most parts of the IEC/ISA 62443 *Industrial communication networks – Network and system security*, series of security standards has a working group examining the impact of IoT on this series.

[52] Low cost IoT devices and software development platforms are available today to the general public. The Adafruit ESP8266 IoT device offers a processor, WiFi radio, and a software environment to deploy a web-capable hosting platform for less than $15.00. See www.adafruit.com/product/2471

[53] Google posts their assurances for Cloud services. See https://cloud.google.com/security/compliance/

[54] Google Home™ speakers contain a microphone allowing access to cloud-based "personal assistant" and can also control some home automation. See store.google.com/product/google_home

[55] Amazon Echo™ uses speakers and microphones to allow access to a cloud-based "assistant" called Alexa and can also control some home automation. See www.amazon.com/echo

[56] Apple HomePod™ uses a speaker and microphone to access a cloud-based "assistant" called Siri and can also control some home automation. See www.apple.com/homepod

[57] SmartThings™ was created to provide an open platform for home automation. Purchased by Samsung in 2014 it continues to offer a development environment for independent developers. Automation functions can run in a home-based SmartThings hub, or in the cloud. See www.smartthings.com

[59] Caséta™ by Lutron has an optional hub device to access cloud based automation to enhance its operation and to interface to other vendor home automation. See www.casetawireless.com

Vulnerabilities in the equipment providing cloud services can put the security of all services being offered to multiple clients at risk. With the advent of multi-tenancy in the cloud, systems from various organizations are placed close to each other and given access to shared memory and resources, creating a more attractive target for attack. The components used to provide the cloud service may not have been designed to offer strong isolation between customer applications, and this can lead to additional vulnerabilities[59].

An accidental deletion by the cloud service provider, or a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data and follows best practices in business continuity and disaster recovery.

The risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.

Users of cloud services must fundamentally trust that the service provider offers the service advertised and does not misuse the data entrusted to them. The details of the implementation of the service will often be invisible to the user. Even the location of the data processing may be unknown and may be subject to the laws of foreign jurisdictions. These challenges lead to many detailed technical concerns, e.g. the security of the computing systems, the legal jurisdiction of the locations where the data is stored, backup systems and their security, and so on.

B.6 Healthcare monitoring and information sharing

ICT is impacting the Health Sector in significant ways. The ongoing digitization of health care records, with the promise that this will provide more seamless heath care services to citizens. Today the growing use of "wearable electronics" is beginning to open the door for more real-time and ubiquitous health monitoring as well as the delivery of this information to both health care providers and to the citizen being monitored.

The growing use of integrated electronic health records is also introducing security risks. Currently administered by the Canadian Medical Association using a policy developed by "Health Infoway"[60], Canada wide coordination remains a challenge. A primary concerns include the need to ensure that data can be shared across clinician, lab, hospital, pharmacy, and patient systems regardless of the application or application vendor, while at the same time maintaining the privacy and security of the information. In addition, each of these various health sector systems including those deployed in large and smaller offices[61], must be designed, built and operated to the minimum standards demanded by citizens.

Advances in ICT in low power sensing, processing and communications has opened additional opportunities for remote patient monitoring (RPM). These technologies are intended to contribute to the prevention of unnecessary visits to hospitals and help drive the healthcare system towards community care and tele-health. The current state of the technology still limits how clinicians can use data collected from RPM tools, as the quality and reliability of the data is often lower than clinical standards.

However as this technology develops, the volume and detail of the data might effectively augment traditional methods. Indeed, even today, "fitness monitors" gather significant information on exercise, heart rate, and a growing number of additional physiological measurements. Although not meeting clinical requirements, such devices can still be used to detect impending problems so that medical attention can be sought at earlier stages.

Concerns related to RPM also revolve around security and privacy issues, and their interface to other heath information systems. Users will likely be concerned

[59] Meltdown and the two Spectre variants (CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754) are examples of such vulnerabilities. see cve.mitre.org

[60] Canada Health Infoway, www.infoway-inforoute.ca/en/

[61] During this study, it was not possible to determine the level of security assessments used in smaller health offices.

that their information is only provided to those medical entities they choose, since improper disclosure might affect employment or insurance qualifications.

New standards are needed as healthcare moves from acute care to community-based and home-based care. Regulations in the health care sector are currently the main drivers for ICT health care products and services. However, as consumer "wearable" devices become increasingly popular, and as health care providers recognize the value of the data they can provide, new standards will be needed to bridge the gap between highly regulated systems and those available to consumers.

B.7 Smart "everything"

ICT technology is being incorporated into a wide range of components and systems, from simple devices to large complex systems. It is now common to identify this next generation of large complex systems incorporating ICT by adding the word "smart" or "intelligent" to their traditional name.

Several sectors are leveraging the new ICT for their work, as discussed in the following subsections.

B.7.1 Smart cities

Smart cities promise the ability to optimize the operation of suburban areas, e.g. by allowing the dynamic control of traffic, public transportation systems, etc. Smart technology could also play a critical role in cities during significant weather events or emergencies, by earlier detection of critical events, by identification of citizens likely to be affected, by clear and directed warnings to potentially affected citizens, and by guidance on means to avoid the situation. From a general public perspective, considerable concerns will arise if the implementation of this technology does not acknowledge the rights of citizens to privacy. Taking into account the concerns raised in the research, from a public policy perspective, such systems should be trusted to:

- Work in an unbiased manner;
- Be free from interference; and
- Use the information gathered appropriately.

Smart city technologies attempt to address the interconnection of many information sources and to optimize city operation based on this information. Many communication and data systems need to be connected, at a minimum, to autonomous cars and trucks, road infrastructure, other types of vehicles, and even pedestrians and bicyclists. The goal of these systems is not only to provide individual vehicles and users with the information they need, but also to provide authorities with the ability to better manage and optimize traffic flows.

GPS and traffic apps already have a degree of intelligence, but substantial policy, economic, and safety concerns will likely delay implementation of fully integrated systems. Vulnerabilities have been identified in individual components from self-driving cars to traffic lights. The impact of security compromises of urban "smart" infrastructure is similar to the impact for individual autonomous or connected vehicles, but on a larger scale. A miscommunication in the system, whether accidental or intentional, could lead to numerous traffic accidents, cause property damage, injury, and possibly death.

There is also public concern that the social license to implement these systems may be exceeded in order to facilitate greater privacy invasions. Data sharing, even between departments of a single government, may be considered improper by some citizens and may be prohibited in many jurisdictions. There has been a long tradition of concern that "smart cities" might lead to mass surveillance. Issues also exist related to the sharing of business data between governmental and non-governmental organizations, e.g. data from car hire or taxi businesses, although originally shared to optimize traffic flow, might be leaked and misused for anticompetitive business purposes.

B.7.2 Smart manufacturing

Smart manufacturing refers to the next generation of manufacturing, which attempts to address all phases of the lifecycle of a product, from concept to ultimate disposal, plus the associated design, manufacturing, marketing, delivery and support infrastructure. It leverages flexible manufacturing to allow products to

be made on-demand, personalized and customized for each customer. Monitoring of product operation in the field using advanced communications technology will provide data on product performance which can be fed back to improve future designs. Even today, some automobiles can communicate problems back to the manufacturer, and the manufacturer can issue updates to improve performance. Most manufacturers of computer software products issue "updates" to repair problems discovered after delivery.

The sales and delivery plans for smart manufacturing also promise the delivery of "electronic catalogs" which can interface to customer procurement and design systems. The products, and ranges of customization, available from a manufacturer would be offered in compatible formats so that customers can compare products from multiple suppliers electronically and can directly import product details into their own design systems. This is already happening to some extent today[62], providing common dictionaries ("languages of things") to allow each manufacturer to publish specifications using common terminology. Compatible interfaces with design tools will further these goals.

This technology will impact on how organizations buy and sell in the future.

Most of the concerns related to smart manufacturing revolve around the gaps in the standards needed to implement the promises of the technology (e.g. agreements on common language as discussed above). Users may be concerned that manufacturer access to monitor product performance could be misused to derive lifestyle details or to introduce vulnerabilities which can then be exploited to create faults or interfere with product operation. Some products may become reliant on product updates to maintain product performance, and the discontinuance of such support would limit a product's useful life (this is often the case for software products).

B.7.3 Smart energy

"Smart energy" or "smart grid" refers to the modernization of our electricity energy supply, by enabling the dynamic control of energy flows, while at the same time permitting easier deployment of smaller distributed energy generation and storage. This technology also allows end users the ability to better manage their own energy use, by letting them to control and schedule energy use. In addition, as electric vehicles and home-based energy generation and storage become more common, these energy sources and loads can be more effectively integrated into the overall energy plans of the utility.

While such technologies potentially offer future cost savings, the resulting exposure of customer use information can be a concern.

Grid modernization has evolved to be more inclusive of customer preferences and desires. In many regions, this has translated to infrastructure and process improvements that have facilitated the integration of distributed energy resources (DER) which includes generation and load.

Smart energy must also address the rapid changes forced on the energy sector due to climate change concerns. This has already led to the growing deployment of smaller, often renewable, energy sources such a photovoltaic and wind generation. This in turn highlights the need to address the standardization requirements of smaller players in the energy sector, including home provided energy generators and industry.

The predicted massive move to electric vehicles (EVs) will significantly impact how transportation energy is delivered. Over the next decade or so there will be a need to deploy an EV charging infrastructure of a scale similar to that used by fossil-fueled cars today. While some standards are in place for EV chargers, a common universal standard, and one likely to meet the needs

[62] The eCl@ss consortia with over 3500 industry members is facilitating the common classification and definition of product data. The IEC 61360 *Common Data Dictionary* (CDD) is an online service providing common definitions in some IEC and ISO product areas. Similarly, ISO publishes terms and definitions as part of the ISO Online Browsing Platform.

for fast charging (charging competitive to the fueling time-efficiency of gasoline stations) do not yet exist. These standards must not only address the connector and voltages/current provided to deliver the energy but must also address measurement and user-pay requirements[63], safety and environmental requirements, and must be compatible with the electrical grid.

B.7.4 Smart homes and buildings

"Smart homes and buildings" refers to the increased automation of building systems, both at home and the office. Smart buildings offer the promise of increased convenience and optimization of building operations as well as the potential to be linked to a smart grid and to connect to a smart city. With the ability to remotely control lighting and other building elements, smart buildings could become increasingly vulnerable to outside interference, and if capable of being monitored by others, can be considered a privacy concern.

Using IoT sensors, actuators and data analysis tools, homes and commercial and industrial buildings, eventually cities, can be made more efficient, comfortable, and safe. There is significant market activity in the home automation space, for example some energy-efficient LED lighting is marketed with built-in wireless interfaces to home automation. Concerns related to the connection of such IoT devices to cloud services were discussed earlier in section B.5.

Smart buildings also promise the ability to detect potential maintenance issues and take action to fix them automatically or proactively requesting appropriate directed remedial action. One of the highest security risks in this field will involve safety and security related technologies, such as fire suppression, alarms, cameras, and access control.

B.7.5 Smart appliances

The term "smart appliances" refers to the incorporation of ICT into traditional appliances, for example to allow them to be monitored and controlled remotely. Some newer appliances can connect to the internet to allow the appliance to provide diagnostic information should a failure occur. Smart televisions can access additional content via the internet. The example of the smart refrigerator was given in section 2. While these products can potentially make life easier for the consumer, they also introduce vulnerabilities which could impact the safety and privacy of the consumer.

[63] Metering and payment must meet legal requirements and are subject to regulatory oversight

References

[1] Burns, A & Wellings, A. (2009). Real Time Systems and Programming Languages: Ada 2005, Real-Time Java and C RealTime POSIX. Toronto, ON: Pearson Canada.

[2] Canadian Centre for Occupational Health and Safety. (2017). CCOHS Annual Report. Retrieved from https://www.ccohs.ca/ccohs/reports/annualReport16-17.pdf

[3] Chakravorti, B. (2018). Trust in digital technology will be the internet's next frontier, for 2018 and beyond, *Scientific American*. Retrieved from http://theconversation.com/trust-in-digital-technology-will-be-the-internets-next-frontier-for-2018-and-beyond-87566

[4] CSA Group. (2018). CSA C22.1-18 Canadian Electrical Code (24th Edition), Part I Safety Standard for Electrical Installations. Retrieved from https://store.csagroup.org

[5] CSA Group. (2018). CSA C22.10-18., Québec Construction Code, Chapter V – Electricity, Canadian Electrical Code, Part I (23rd edition) with Québec Amendments. Retrieved from https://store.csagroup.org

[6] Google. (2017). Google Terms of Service. Retrieved from: https://policies.google.com/terms?hl=en&gl=ca#toc-about

[7] International Electotechnical Commission. (2015). The IECEE CB-FCS Full Certification Scheme. Retrieved from https://www.iec.ch/about/brochures/pdf/conformity_assessment/IECEE_CB-FCS_Full_Certification_scheme_LR.pdf

[8] International Organization for Standardization. (2015). ISO 9001:2015 Quality Management Systems – Requirements (5th edition). Retrieved from https://www.iso.org/iso-9001-quality-management.html

[9] International Organization for Standardization & International Electrotechnical Commission. (2013). ISO/IEC 27002:2013 Information technology— Security techniques—Code of practice for information security controls. Retrieved from https://www.iso.org/standard/54533.html

[10] International Organization for Standardization, International Electrotechnical Commission, and Institute of Electrical and Electronics Engineers. (2011). ISO/IEC/IEEE 42010:2011 Systems and Software Engineering – Architecture Description. Retrieved from https://www.iso.org/standard/50508.html

[11] Internet Engineering Task Force. (2003). Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Retrieved from https://www.ietf.org/rfc/rfc3647.txt

[12] Raine, L. and Anderson, J. (2017). The Fate of Online Trust in the Next Decade. Retrieved from http://www.pewinternet.org/2017/08/10/the-fate-of-online-trust-in-the-next-decade/

[13] Certification Practice Statement. (2018). Retrieved from https:/www.thawte.com/cps/

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™