IoT Security and Consumer Trust

Dr. Hosein F. Badran

Digital Transformation Consultant

Badran Digital Consulting, Ottawa, Canada, hbadran@badranconsult.com

ABSTRACT

The adoption and usage of IoT devices is on the rise, globally, with consumers already owning smart devices planning on purchasing more devices. Consumers are generally concerned about their personal information being leaked, but are not equipped with knowledge to help them purchase products with adequate security and privacy measures. Manufacturers focus on rushing more products to the market, and do not systematically communicate information about the security features devices possess that would need to be evaluated to assess their level of security.

This paper provides and overview on recent developments in the domain of IoT security frameworks, IoT device security certifications and device labeling. Key proposals from the United Kingdom, the European Union, Australia and Canada are presented. A proposal for a IoT device security label is provided.

KEYWORDS

IoT Security, Consumer Trust, Security and Trust Framework, Device Labels

ACM Reference format:

Dr. Hosein F. Badran. 2019. IoT Security and Consumer Trust. In *Proceedings of dg.o 2019: 20th Annual International Conference on Digital Government Research (dg.o 2019), June 18, 2019, Dubai, United Arab Emirates*. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3325112.3325234>

1 Rising Usage of IoT Devices

The usage of IoT devices (also commonly referred to as “smart Devices”) is on the rise, globally. Recent survey conducted by the Internet Society (ISOC) in the Asia Pacific region identified key trends as well as consumer trust and concerns [1].

Figure 1: IoT Device usage in APAC [1]

A large portion of consumers (70%) already own IoT devices and plan on purchasing more. Consumers want to own IoT devices, but are also deeply concerned about their security and privacy. Consumers’ trust and their concerns about security and privacy do not match their ability to protect themselves, and they would like to be informed and have control over their privacy and security. Consumers highly value measures to protect against security and privacy threats, and believe that government should help ensure that these measures are in place.

The report identified two key risks. Firstly, consumer security, privacy and safety is being undermined by the vulnerability of individual devices; and secondly that the wider economy faces an increasing threat of large scale cyber attacks launched from large volumes of insecure IoT devices.

2 Trends in IoT Device Security and Privacy

This section provides and overview on recent developments in IoT security frameworks, and IoT device security certifications. Key proposals from the European Union, the United Kingdom, Australia and Canada are presented. In particular, the Canadian Multi-stakeholder Initiative on IoT Security [11][12] provides the foundation for the research presented in this paper.

2.1 IoT Product Certification in the Netherlands / The European Union

As part of the EU negotiations, the Netherlands is strongly promoting the rapid adoption of the Cybersecurity Act (CSA) and the active development of a European Cybersecurity Certification framework for ICT products and services [2].

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

dg.o 2019, June 18, 2019, Dubai, United Arab Emirates

© 2019 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-7204-6/19/06.

<https://doi.org/10.1145/3325112.3325234>

Figure 2: The Netherlands: Roadmap for Hardware and Software Security [2]

Moreover, the Dutch government supports the swift adoption of mandatory certification for specific product groups, i.e. products that present the greatest risk or the most problems in practice. In the long term, mandatory certification or compliance with a **CE marking** for all products with Internet connectivity should be implemented through gradual expansion.

Figure 3: Key Elements of the Dutch Roadmap for Hardware and Software Security [2]

2.1.1 EU Framework: Security Certification of ICT Products and Services. The proposed Cybersecurity Act (CSA) is the European Commission's attempt to create, amongst others, a harmonized framework for the cybersecurity certification of ICT products and services within the EU. The absence of reciprocal agreements on standards and certification systems forms a barrier to creating an European market for cybersecurity products and services. It limits the scale for providers, and reduces choice and creates increasing uncertainty for consumers and businesses alike.

This can be changed through common European certification of products and services, indicating that they are resilient (at a specified security level) to threats to their availability, authenticity, integrity and reliability of data or of the functionalities and services being offered. The CSA aims to target fragmentation and foster the harmonization and reciprocal acknowledgement of cybersecurity certification at European level.

Once an European certification framework has been adopted for a product or service, national government schemes will become redundant and Member States will no longer need to develop their own certification programs.

2.2 IoT Device Certification in the United Kingdom

In March 2018 the United Kingdom Government's Secure by Design review announced a series of measures to make connected devices safer to use [3]. The Kitemark builds on these guidelines by providing ongoing rigorous and independent assessments to make sure the device both functions and communicates as it should, and that it has the appropriate security controls in place. Manufacturers of Internet connected devices will be able to reassure consumers by displaying the Kitemark on their product and in their marketing materials.

There are three different types of *BSI Kitemark for IoT Devices*, which will be awarded following assessment according to the device's intended use: residential, for use in residential applications; commercial, for use in commercial applications; and enhanced, for use in residential or commercial high value and high risk applications [4].

The assessment process involves a series of tests that help ensure the device is fully compliant with the requirements. Before being awarded the Kitemark the manufacturer is assessed against ISO 9001, and the product is required to pass both an assessment of functionality and interoperability, as well as penetration testing scanning for vulnerabilities and security flaws. Once the BSI Kitemark is achieved the product will undergo regular monitoring and assessment including functional and interoperability testing, further penetration testing and an audit to review any necessary remedial action. Importantly, if security levels and product quality are not maintained the BSI Kitemark will be revoked until any flaws are rectified.

The BSI Kitemark™ provides comfort and confidence to users of products or services across a whole range of sectors. Recognition of the BSI Kitemark™ is high. Two thirds of all UK consumers associate it with quality, assurance, reliability and trust. 93% of adults believe BSI Kitemark™ products are safer and 75% say the BSI Kitemark™ will help make choosing between products easier.

2.3 IoT Product Certification in Australia

Another example for IoT product testing and certification is the process identified in Australia. IoT product manufacturers may wish to submit their products for testing by an accredited test laboratory, either under the National Association of Testing Authority (NATA) scheme or under the Australian Government in the Australasian Information Security Evaluation Program (AISEP) [5]. Formal testing will, if successful, result in the award of a test certificate and provide evidence of independent security assurance to customers.

Currently there is no mandated requirement for security testing, but the high profile of cyber attacks involving internet of things devices makes this a key area of consideration for users. Having evidence that a device has been security tested will be a competitive advantage.

In order to provide security and privacy confidence in IoT devices designed, manufactured, or deployed in Australia, the

IoTAA will release a security testing procedure based on the Online Trust Alliance Framework which will be available for accredited organizations to use to recommend the issue of an IOTAA Security and Privacy Trustmark.

Figure 4: BSI Kitemark for Residential IoT Devices [4]

There are currently three sets of published criteria that can be used for testing IoT devices:

1- The IoT Security Foundation has proposed a compliance scheme based on evaluation against their Security Compliance Framework [6]. In addition, the IoT Security Foundation has proposed a compliance regime for demonstrating security in IoT

devices and systems. This positions an IoT product into one of five classes – Class 0 to Class 4 - as shown in Table 1.

2 - The Open Web Application Security Project (OWASP) [7] has developed a testing guide for IoT products. It covers sixteen IoT Principles of Security and provides a framework for testing ten different vulnerabilities.

3 - The Online Trust Alliance (OTA) framework provides measureable requirements, which can be used as a starting point for selecting security testing requirements [8]. The framework consists of eight categories of actionable principles. These principles include; authentication, encryption, security, updates, privacy, disclosures, control and communications. It also considers stakeholders who will have a collective responsibility for developing a secure solution.

IoT device manufacturers could select the relevant criteria for their device from these three documents, in addition to any device specific functionality not otherwise covered. These criteria will then form the Initial Claims Document for the security testing.

Table 1: IoT Security Foundation Classes [5].

Class	Impact of Compromise	Confidentiality	Integrity	Availability
0	Minimal	Basic	Basic	Basic
1	Limited impact on an individual or organisation	Basic	Medium	Medium
2	Significant impact on one or more individuals or organisations	Medium	Medium	High
3	Significant impact to sensitive data	High	Medium	High
4	Personal injury or damage to critical infrastructure	High	High	High

2.4 Canadian Standards Association (CSA) Group Cyber Verification Program

The CSA Group is currently developing a program and standard that is aiming to address the product and organization security aspects. The Cyber Certification Program (CVP) consists of several aspects including a self-assessment, onsite audit, and formal product testing and evaluation. This program is built on the premise that an insecure organization cannot build a secure product. Security practices must be embedded into the organization's operations and development processes.

The assessment aspects consider 6 domains and 18 practice areas within these domains. The current self-assessment consists of 198 binary questions that once completed in connection with audit will provide a maturity rating for the organization.

3 IoT Device Labeling

This section addresses experience and recent research in product labeling, how it applies to the case of IoT device security label, and recent proposals for IoT device labels as well as IoT consumer code of practice. The usage of the QR code as a product label is investigated, identifying relevant use cases.

In order to provide more insight into the relative merits of the different types of labeling, it is useful to refer to critical research performed on well-established labeling schemes, particularly on the food labels and the energy efficiency labels. This research is summarized in the recent report of PETRAS IoT Hub and Dawes Centre for Future Crime at UCL as part of the Consumer Security Index project in the UK [9].

3.1 The need for a labeling scheme for consumer IoT devices

At present, consumers cannot distinguish between devices that offer good and inadequate security when making purchasing decisions. Actually, they have to research the security features and capabilities of the product themselves before deciding. This would involve evaluating technical information such as security standards compliance, what data is collected by the device and how it is shared, the length of support coverage, and whether the device ships with a default password.

Awareness campaigns and behavior change interventions can encourage consumer behavior and motivate consumers to routinely assess the security of IoT devices they consider purchasing. However, research has shown that such intervention will not be sufficient to have real impact on consumer decisions

when buying an IoT product [9]. A key reason is that manufacturers do not systematically communicate information about the security features devices possess that would need to be evaluated to assess their level of security. Also, the average consumer will not have the expertise required to evaluate this information, and typically is inclined to avoid cognitively demanding tasks, as per relevant research [10].

A label that consumers can relate to and that would inform their decision making in a meaningful way is a more achievable intervention that could impact consumer choice.

As mentioned, manufacturers do not provide correct or accessible information to inform consumers and retailers about the level of security their devices offer. A labeling scheme would likely encourage manufacturers to compete on security as a form of market differentiation. It would also hold manufacturers to account by promoting attention to be directed to the security of devices and for this to be done against clear criteria and guidelines. Finally, a labeling scheme would allow market oversight and consumer protection authorities to assess compliance to IoT security in a more consistent and transparent approach.

3.2 Types of labeling formats

There are three different types of labeling formats:

- Descriptive information label: it details security-related information.
- Seal of approval label in which a product is certified to a standard.
- Graded scheme label that allows more critical comparisons of security-related compliance.

3.3 Code of Practice for Consumer IoT Security

Recent research, including research by the Internet of Things Security Foundation [6], as well as the UK's Department for Digital, Culture, Media, and Sport (DCMS) report titled "Code of Practice for Consumer IoT Security" [14] published in Oct. 2018, have identified key information and best practices that is critical to be followed and documented by the manufacturer, service provider, retailer, and the consumer.

The thirteen principles identified in the Code of Practice for Consumer IoT Security [13] published by the UK's Department of Digital, Culture, Media and Sport are presented in Figure 5.

Similar guidelines have been provided by the U.S. Department of Homeland Security in the "Strategic Principles for Securing The Internet of Things" report [14]. The IoT Alliance Australia (IoTAA) published a comprehensive report titled "Internet of Things Security Guidelines" [5]. The IoTAA report identifies "the Trust Framework", which requirements form the basis for evaluating an IoT system for best practices in security and privacy, and form the basis of the IoTAA Security and Privacy Trustmark.

Figure 5: UK IoT Consumer Code of Practice [13]

3.4 ETSI Cyber Security for Consumer Internet of Things Standard

The European Telecommunications Standards Institute (ETSI) published the "Cyber Security for Consumer Internet of Things" or the TS 103 645 V1.1.1 standard, in Feb. 2019 [22]. This is certainly a major development into the direction of specifying globally applicable high-level provisions for the security of consumer devices that are connected network infrastructure such as the Internet or home network.

The standard document provides basic guidance for manufacturers involved in the development and manufacturing of consumer IoT on how to implement those provisions.

The thirteen high-level provisions identified in the standard document closely follow the principles identified in the Code of Practice for Consumer IoT Security [13] as shown in Figure 5.

3.5 IoT Device Security Label

In terms of the possible IoT device security label formats, as explained above, each of the known three labeling schemes has its strengths and weaknesses.

The colored graded scheme would attract the attention of consumers and help them compare the security of different devices. For this implementation to be effective the display of the graded label needs to be mandatory for manufacturers.

The Binary or "seal of approval" label is typically preferred by consumers due to its simplicity, but is less effective in guiding attention and informing consumer choice [15]. Care should be given as the use of the binary label may lead consumers into a false sense of security or assume that it requires no intervention from them to keep secure.

The descriptive information label communicates critical information to consumers and may provide helpful indicators of a device's security readiness. The label needs to communicate the most relevant information only and not burden consumers with unnecessary information. This type of label is more suitable for the voluntary label introduction.

3.6 Mandatory and Voluntary Labels

The Department of Digital, Culture Media and Sport (DCMS) of the UK, released their policy review for Secure by Design for consumer "Internet of Things (IoT)" products, in March 2018 [3].

A key measure in the report is a voluntary code of practice for manufacturers to ship products with features that make them “Secure by Design”. The report also proposed exploring the role of a voluntary labeling scheme to communicate important information to consumers that is otherwise invisible to them, or difficult to find, such as how data collected by devices is shared and the support period for the product [3].

More recently, the UK’s DCMS announced a consultation process on the government’s regulatory proposals regarding consumer IoT security [23]. In this consultation process, initiated in May 2019, a proposal for the “top three” guidelines of the Code of Practice [3], be made mandatory in the UK. These critical guidelines are that all IoT device passwords shall be unique and not be resettable to any universal factory default value; that the manufacturer shall provide a public point of contact as part of a vulnerability disclosure policy; that manufacturers will explicitly state the minimum length of time for which the product will receive security updates.

A voluntary labeling scheme would be useful as an initial step, but for a sustainable market growth and to ensure manufacturers adherence, as well as to maintain consumer awareness, it will be necessary for the label to be mandatory to be effective. It is feared that manufacturers may be unwilling to display a label that indicates poor security of a product.

3.7 QR Codes

A QR code is a type of matrix bar code or two-dimensional code that can store data information and designed to be read by smartphones. QR stands for “Quick Response” indicating that the code contents should be decoded very quickly at high speed. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL or other data [16] [17]. The QR code was designed to allow its contents to be decoded at high speed.

The popularity of QR codes is growing rapidly all around the world. Nowadays, mobile phones with built-in camera are widely used to recognize the QR Codes.

QR Codes are created by the Toyota subsidiary Denso Wave in 1994, and was initially used for tracking inventory in vehicle parts manufacturing [18].

3.7.1 QR Codes Usage Statistics. The use of code scanning has gone up during the past years, as awareness and adoption of QR Codes grow exponentially. QR code stats done by ScanLife show that 23 million QR codes are scanned during the first quarter of 2015, which is nearly 10 million more than during the first quarter of 2012, and the first quarter of 2012 had posted a 157 percent increase as compared to the first quarter of 2011 [19].

According to a recent survey by Statista, in the US alone, an estimated 11 Million households will scan a QR Code in 2020, as shown in Figure 6. This is an increase from an estimated 9.76 Million scans in 2018 [19]. Hence there is a huge potential for US manufacturers and marketers who are considering adding a QR Code to their print media campaigns.

In Canada,

- 27.4 million Canadians are online representing 80% of the population
- 93% go online to view and verify product information

These figures have changed the way Canadian marketers and retailers engage their audience. To strike a chord with the young generation, marketers, retailers, manufactures and even the police have adopted QR Codes in Canada [20].

Table 2: Global QR codes usage by ScanLife [19].

Users who scan QR codes in the first quarter of the several years	
Year	Users
2011-Q1	7.5 millions
2012-Q1	13.3. millions
2013-Q1	18.2 millions
2014-Q1	21.8 millions
2015-Q1	23.1.millions

3.7.2 Relevant Use Cases for QR Codes. The use cases of QR codes vary widely and cover different areas from marketing, product packaging, advertising, special causes, customer surveys, and much more.

Below, three use cases of QR codes that focus on providing product information particularly in the ICT (information and communications technology) domain, are presented [21].

Figure 6: QR Scans in the US [20]

HP Use Case

HP sought after a practical and interactive way for customers to receive details on their products right from the package. They wanted potential customers to more easily understand what they were purchasing, and what accessories, like ink packages, were required for each.

HP used ScanLife activated codes extensively on most of their consumer printer line around the world (Figure 7). The codes told customers more about the products and gave them details on accessories which made it easier for shoppers to buy products, especially during the busy holiday season when retail associates were difficult to find.

Staples Use Case

Staples had a variety of goals for its mobile marketing campaign: To show value for the consumer while also helping the business achieve key sales milestones. However, their

ultimate objective was to increase overall conversions through the use of an effective in-store campaign. Staples incorporated QR Codes into its in-store displays to let the products do the talking (Figure 8).

Figure 7: QR codes used by HP [21]

Figure 8: Staples mobile marketing campaign [21]

4 Comparison of Types of Labels for IoT Device Security

This section provides a comparison between the different types of labels, focusing on their suitability as a label for IoT device security (Table 3).

Table 3: Comparison of types of labels for IoT device security.

Type of Label	Pros	Cons	Notes
Graded/Color Graded	<ul style="list-style-type: none"> - Attracts the attention of consumers - Helps consumers compare the security of different devices 	<ul style="list-style-type: none"> - To be effective the display needs to be mandatory for manufacturers 	<ul style="list-style-type: none"> - Could be introduced at a later stage in a mature IoT Security market
Binary (Seal of Approval)	<ul style="list-style-type: none"> - Easy for customers to interpret - Preferred by consumers 	<ul style="list-style-type: none"> - Less effective in guiding consumer choice - Gives (false) sense of security and that no additional action from consumer is needed - Does not automatically reflect current security status of new product vulnerabilities. 	<ul style="list-style-type: none"> - Example is BSI Kitemark - Combine binary/seal of approval label with other informative label (e.g. Live Label)
Informative	<ul style="list-style-type: none"> - Communicates critical information to consumers - Provides helpful indicators of a device's security readiness - More suitable for voluntary label introduction 	<ul style="list-style-type: none"> - Need to limit information displayed to most relevant information 	<ul style="list-style-type: none"> - Suitable for market introduction and to help build consumer understanding and trust.

Live Label (e.g. QR code)	<ul style="list-style-type: none"> - A form of informative label - QR codes are gaining adoption from manufacturers as marketing tools - Provides link to current information on product security - Allows consumer to get information beyond security compliance, e.g.: <ul style="list-style-type: none"> - Deployment recommendations, - Data collection/sharing information, - Latest vulnerabilities 	<ul style="list-style-type: none"> - Requires consumer to scan QR code and spend time going through relevant information 	Suitable for market introduction and to help build consumer understanding and trust.
------------------------------	---	---	--

5 Proposal for an IoT Device Label

This section provides a proposal for an IoT device security label. Following the comparison between the benefits of the different label formats, as described in Table 3, the proposed approach is to combine the consumer trust factor of known “trust marks” such as CE in Europe, Kitemark in the UK, CSA in Canada, CTIA in the US, with advanced and critical product security information that are difficult to display on a label, and have the nature to change over time.

Key information to be conveyed by the label:

- Formal testing and certification has been performed on the product.
- Where to get up-to-date critical information on product security features and installation/deployment considerations.

Main aspects to be covered by a security product label are:

1. Identification of the organization overseeing/authorizing the certification and formal testing (e.g. BSI Kitemark, CE mark, CSA mark).

2. A machine-readable code that is linked to a url (web site) providing up-to-date product information (*i.e. a live label or QR code*). The website should include the following:

- Product model and/or version number
- Latest product firmware version number
- Recent vulnerability information
- Certification/testing framework
- Security configuration guide

f. Information on what data is collected and how it is shared

Figure 9: Example of IoT Device Security Label

In the example label (Figure 9), the entity overseeing/authorizing the product certification and testing is the CTIA, while the device tested is the Amazon Alexa smart home assistant. The QR code (a form of a live label) should point to the product site with up-to-date product security information. The product name could optionally be explicitly listed in the label. This presentation is a reference example only, not a working implementation.

6 Conclusions

With the rising usage of IoT and smart devices, consumers are concerned that their security, privacy and safety could be undermined by the vulnerability of individual devices. At the same time the wider economy faces an increasing threat of large-scale cyber attacks launched from large volumes of insecure IoT devices.

This paper provides an overview on recent developments of IoT security frameworks, IoT device security certifications and device labeling. Key proposals from the United Kingdom, the European Union, Australia and Canada are presented. A proposal for an IoT device security label is provided. The proposed label combines the consumer trust factor of known “trust marks”, with a live label (QR code) providing access to advanced and critical product security information that are difficult to display on a label, and have the nature to change over time.

7 ACKNOWLEDGMENTS

The support of the Internet Society, North American Bureau is hereby acknowledged.

REFERENCES

- [1] Internet Society, 2018 Survey on Policy in Asia-Pacific: “We need to do something about IoT Security”, <https://www.internetsociety.org/blog/2018/11/we-need-to-do-something-about-iot-security/>
- [2] Ministry of Economic Affairs and Climate Policy, The Netherlands, Roadmap for Digital Hard-and Software Security, 2018, <https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digital-hard-and-software-security>
- [3] Department of Digital, Culture, Media and Sport (DCMS), Secure by Design Report, 2018,

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
- [4] British Standards Institution. BSI launches Kitemark for Internet of Things devices, 2018. <https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/>.
 - [5] IoT Alliance Australia, Internet of Things Security Guideline, 2017, <http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf>
 - [6] IoT Security Foundation, Establishing principles for IoT Security, 2015, <https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf>
 - [7] Open Web Application Security Project (OWASP), Principles of Security, www.owasp.org/index.php/Principles_of_IoT_Security
 - [8] Online Trust Alliance (OAT), IoT Trust Framework, https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf
 - [9] PETRAS IoT Hub, Rapid evidence assessment on labelling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf
 - [10] D. Kahneman, P. Egan, (2011), Thinking fast and slow. New York: Farrar, Straus and Giroux.
 - [11] Internet Society, Enhancing IoT Security, *draft report*, Feb. 2019, <https://iotsecurity2018.ca/wp-content/uploads/2019/02/Enhancing-IoT-Security-Draft-Outcomes-Report.pdf>; *Earlier draft*, Jan. 2019: https://iotsecurity2018.ca/wp-content/uploads/2019/01/Labeling-WG-Report-Public-Draft_v1.pdf
 - [12] Hosein Badran, "IoT Security and Consumer Trust", Expert Group Meeting on Cyber Security, United Nations Economic and Social Development Council for West Asia (UN-ESCWA), Beirut, Lebanon, Dec.2018, https://www.unescwa.org/sites/www.unescwa.org/files/events/files/s95_iot_security_and_consumer_trust.pdf
 - [13] Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, <https://www.gov.uk/government/publications/secure-by-design>
 - [14] U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things, (2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL.pdf
 - [15] J. Koenigstorfer, G. Wasowicz-Kirylo, M. Styśko-Kunkowska, A. Groeppel-Klein (2014) Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! Public Health Nutr;17:2115–21.
 - [16] Dong-Hee Shin, Jaemin Jung, Byeng-Hee Chang (2012), "The psychology behind QR Codes: User experience perspective", Science Direct, Computers in Human Behavior 28, pp. 1417-1426.
 - [17] Phaisarn Sutheebanjard, Wichian Premchaiswadi, (2010), "QR Code Generator", IEEE 2010 8th International Conference on ICT and Knowledge Engineering, pp. 89-92.
 - [18] Sumit Tiwari, An Introduction to QR Code Technology, (2016), IEEE International Conference on Information Technology (ICIT), DOI: 10.1109/ICIT.2016.021
 - [19] ScanLife.com, "QR Code Adoption: Trends and Statistics", www.scanlife.com
 - [20] QR Code Statistics 2018: Latest Numbers On Global QR Code Usage, (<https://scanova.io/blog>)
 - [21] Scanbuy, QR Codes Use Cases, <http://www.scanlife.com/case-studies/>
 - [22] ETSI, Cyber Security for Consumer Internet of Things, TS 103 645 V1.1.1, 2019, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf
 - [23] Department of Digital, Culture, Media and Sport (DCMS), Consultation on the Government's regulatory proposals regarding consumer Internet of Things (IoT) security, May 2019, <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security>