A trustmark for IoT

Building consumer trust in the Internet of Things by empowering users to make smarter choices.

A ThingsCon Report commissioned by Mozilla's Open IoT Studio.

THINGS

moz://a
Open IoT Studio

A TRUSTMARK FOR IOT

Building consumer trust in the Internet of Things by empowering users to make smarter choices. A ThingsCon report commissioned by Mozilla's Open IoT Studio.

ThingsCon is a global community of IoT practitioners that fosters the creation of a human-centric & responsible IoT.

Mozilla's Open IoT Studio seeks to advance responsible open IoT through professional practices and a network of IoT practitioners who conduct research, make prototypes and build meaningful collaborations.

Author: Peter Bihr (ThingsCon, The Waving Cat).
Cover design: Martin Skelly
Version 1.0, 13 September 2017

Published by ThingsCon

Table of Contents

"A lack of transparency results in distrust and a deep sense of insecurity."
— Dalai Lama

EXECUTIVE SUMMARY

We are increasingly surrounded by connected devices that have an impact on every aspect of our lives. This Internet of Things (IoT) thrives on data. It brings us a great many services, but it also provides new and significant challenges. As the Internet reaches into our physical world, so does the fight for Internet health. We now essentially live inside a computer—and it is essential that we can trust it.

All the marks of a healthy Internet also need apply to the Internet of Things: Openness, inclusion, decentralization, privacy and safety, as well as literacy. However, in the world of IoT, some of these aspects are in ever stronger danger than in the rest of the Internet. And here, users are even less equipped to make smart, healthy and sustainable choices.

We propose a trustmark for IoT, a label for consumers to decide which devices they choose to trust and—more importantly—which devices deserve their trust. This empowers consumers to make informed decisions on how to vote with their money and for producers of IoT products to show their commitment to good practices and IoT health.

Why a trustmark for IoT, and why now?

The Internet of Things with its dizzying array of connected products and services is hard to navigate. **Consumers have little insight into what any one connected product does, what it even might be capable of, or if the company employs good, responsible data practices. This is not an oversight on the consumers' side.** Rather it has to do with the way connected products work (they're complex hybrids of hardware and software), as well as an overall lack of transparency in both data practices and business models.

A trustmark for IoT offers a way to empower consumers to make better decisions.

IoT faces a number of specific challenges and risks that go beyond other digital services, including surveillance, risk to physical safety, and that a remote software update can change devices in unexpected ways. **Having these risks in mind**

allows us to better consider IoT trustmarks.

The discussion around consumer IoT trustmarks is extremely salient right now, and it moves quickly. Consumer trustmarks are discussed at all levels, from the European Commission to industry and grassroots initiatives. The term *trustmark* is often used interchangeably with other terms like *certification mark*, or *consumer label*: We recommend using the term for a consumer label with the explicit intent of increasing (justified) consumer trust.

Trustmarks are effective and enjoy high levels of trust by consumers. From other critical consumer protection areas like food and electronics safety we know that **trustmarks can both increase consumer trust and provide an incentive for responsible organizations to clearly communicate their commitment to a higher standard**. They enjoy high levels of trust by consumers. For commercial and non-commercial entities alike, an easy-to-understand labeling system for responsible IoT would allow them to make better, more responsible product and business decisions.

We believe that the current situation poses significant challenges to consumers—and see a tremendous opportunity for Mozilla and its community to have a massive positive societal impact and provide thought leadership. Maybe more importantly, in this debate Mozilla is in a unique position to host this debate and demonstrate leadership as a trusted organization. **Mozilla's input and leadership is both possible and very much needed.**

The special trust challenge of IoT

> *"Trust is a critical challenge and a necessity for a thriving Internet of Things ecosystem."*
> *—Gérald Santucci (DG CONNECT)*

The capability of IoT products to remotely receive software updates are one of IoT's biggest strengths, but it is also one of its biggest weaknesses because a) if there are changes to the producing company (e.g. change of ownership, new strategy, bankruptcy), the products can cease operation and b) software updates can significantly change the product itself, for example by enabling or disabling features or sensors. Increasingly, consumers even face "hidden IoT" devices: Products that are not sold as "smart" yet are ready to be connected and/or contain sensors that could be activated with the next software update.

For consumers it's nearly impossible to know the exact capabilities of the connected products in their lives. This extends to professional product reviewers, too. To make matters worse, even a comparatively secure device can be compromised if it is paired with a less secure one. Hence, **the health of IoT is only as strong as the weakest link in the network.**

Consumers must be able to make an informed decision on IoT products, and transparency is an essential first step. We believe that a much higher level of transparency is both essential and possible.

At any given time, consumers should have a clear answer to four simple questions:

1. "Does it do what I expect it do do?"
2. "Is the organization trustworthy?"
3. "Are the processes trustworthy?"
4. "Does it do anything I wouldn't expect?"

An IoT trustmark can help answer these questions.

It's worth taking a moment to ask **what constitutes trustworthy technology**. **We consider tech trustworthy when it considers all stakeholders, takes a long view and sustainable approach, focuses on value creation rather than extraction, and if in doubt, it errs on the side of openness and empowerment.** In IoT, a device's trustworthiness doesn't depend only on the device itself: It also depends on other factors like the device's readability and understandability, the trustworthiness of the producing organization and their business model, societal impact, service and maintenance guarantees, and others. The multi-dimensional nature of IoT is part of why it is such a challenging space for consumers and producers alike.

> *"Trust arrives by foot and leaves by horse." —Dutch saying*

Trustmarks have beneficial side effects that go beyond the primary intent of verifying and promoting consumer trust. They can increase consumer awareness and literacy, and they offer producers of IoT services and products a way to distinguish their products. Furthermore they have shaping power by highlighting best practices for others to follow and by validating good design decisions and data practices.

A trustmark creates a virtuous cycle. The trustmark allows developers of IoT products to differentiate themselves by "doing the right thing". It allows consumers to make smarter choices and to put pressure on all developers to follow suit. This creates a virtuous cycle in favor of a trustworthy IoT.

What to label & how to verify

There are many different possible approaches to labeling, so it is essential to answer what to label for, who verifies and how, and how can the trustmark be communicated. **In order to be effective, the IoT trustmark needs a clear focus. In our research we identified the following core themes:**

- **Good data practices:** privacy, security, data protection, putting users in control over data capture and processing
- **Good security practices:** checklists, openness, giving users control over fallback mechanisms
- **Openness:** transparency, hackability, open source, compatibility
- **Lifecycle management:** service guarantees, repairability, ease of reverse-engineering and/or hacking, having a strategy in place for end-of-life
- **Establishing that the producing organization is trustworthy** and knows how to handle itself

At the core, transparency helps consumers understand and navigate the complexities of networked technologies. This can only work if a label is verifiable, and trustworthy. In the literature we reviewed as well as in many conversations with experts we encountered a great range of characteristics, principles, or aspects to consider for labels, which we explore in the chapter "What to label & how to verify". **There is a wide spectrum of types of consumer protection labels or trustmarks, from self-labeling to third party certification.** A successful IoT trustmark needs to balance between widespread adoption (promoted by a low barrier-to-entry in terms of cost and bureaucracy) and trustworthiness (promoted by a reliable verification process). Based on our research, **we recommend aiming for a relatively light-weight trustmark approach. We believe an IoT trustmark should tend towards the self-assessed and voluntary while being verifiable through context-appropriate "View Source" privileges.**

We recommend weighing the label slightly towards the device level, but taking into account at least the most salient aspects of a more systemic nature. Especially where data processing happens in the cloud, this is highly relevant for users to know. How exactly this can be implemented should be based on further research and input from a user survey and workshops with partner organizations.

Given the context of Internet of Things, where the information underlying any label will have to be flexible enough to account for future software updates, a dynamic mark seems most promising. If the mark links to deeper background content on the open web, then all relevant information can be publicly accessible and updated as needed. The information displayed on that URL should include the "top level" mark (for example, binary or traffic light) as well as the underlying information, like further documentation. In addition to being pragmatic and flexible enough, such **an open web based model seems a particularly good fit for this context as well as Mozilla's culture.**

The success of a consumer label also depends on how easy it is to understand, and how actionable it is, without oversimplifying. Striking the right balance between accessibility and density is key for a successful, useful implementation of a trustmark. The look and feel of the final trustmark draft will require designers' input. Nutritional labels and laundry labels can serve as inspiration from which the consumer IoT space can learn a lot.

Optimally, the IoT trustmark should convey at a glance the level of trustworthiness and allow for retrieval of more detailed background and context information.

The Landscape of existing relevant certifications, labels & marks

Trustmarks for IoT do not, and could not, exist in a vacuum. In the chapter "Landscape" we highlight several existing approaches. None of them solve the challenges we see for the IoT space, but all are for one reason or another particularly relevant for the context of IoT trustmarks. We looked at a wide range of labels and certifications including OSHWA's Open Source Hardware Certificate, Creative Commons' content licensing, the FCC's Broadband Nutrition Labels, Carnegie Mellon University's Privacy Nutrition Labels, the iFixit Reparability Score, CE certification, the German Blue Angel environmental label, Fairtrade, and laundry labels.

The open web was so successful because it was built on open interoperable layers. The same applies to labeling in the consumer IoT space: **Trustmarks are one layer to apply alongside other layers and building blocks**. Some of these building blocks might be other consumer labels or certifications, others might be technologies or protocols.

Current proposals and initiatives for IoT-related labels

The chapter "Current proposals" looks at proposals, drafts, and initiatives specifically for the realm of IoT. The landscape today looks relatively scattered. The majority of proposals focus on information provided by the producer of IoT products, but a few take a more centralized, top-down, regulatory approach. **This seems to be representative of the equally scattered landscape of organizations and initiatives. We believe that Mozilla can play an instrumental role in convening these scattered initiatives and hosting this global conversation. Mozfest and the Internet Health Report both seem to be natural starting points.**

As part of Europe's push for a Digital Single Market, the European Commission identifies the need for consumer trust in IoT and proposes a labeling system. Europe emerges as a fierce proponent of consumer protection when it comes to digital services, and has been doubling down on IoT especially. With the General Data Protection Regulation (GDPR) about to go into effect in 2018 and the "Trusted IoT" initiative we see ever-stronger efforts to protect European consumers from commercial data exploitation. **It seems that just like Silicon Valley is a global hotspot for disruptive innovation and for providing the means for global scaling of digital services, and like Shenzhen, China, is the world's manufacturing epicenter, Europe increasingly claims a global leadership role in consumer rights, privacy, and data protection.**

Potential collaborators

In our research, we identified a number of promising emerging proposals and initiatives, as well as potential collaborators and allies. The #iotmark initiative, Doteveryone, The Repair Project, Projects by IF (all UK), Just Things (Netherlands), Consumers International, The Digital Standard, and ThingsCon (all global) are all organizations and initiatives we strongly recommend working with.

About this report

This report is based on extensive research in and around the ThingsCon network, a community of IoT practitioners that fosters the creation of a responsible & human-centric Internet of Things. It aims to serve as a starting point for proposing and implementing a labeling system from which further feedback from consumers and industry can be gathered. Written by Peter Bihr, ThingsCon co-founder and managing director of research & strategy firm The Waving Cat, the report is based on interviews and workshops with expert practitioners including designers, developers, researchers, entrepreneurs and activists, conversations at relevant conferences like the London 2017 founding event of the #iotmark initiative (that the author is involved with), as well as extensive literature review.

RECOMMENDATIONS & OPPORTUNITIES

Based on our research, we strongly recommend Mozilla to take a leadership role in proposing a trustmark for IoT.

There is a lack of trustworthy, credible, scalable initiatives for responsible IoT that have primarily users' interest at heart. At the same time, the issues at stake are of high salience, which is why we recommend moving quickly and taking advantage of the early mover advantage. **There's currently an open window to have an outsized impact** and significantly move the needle, but likely not for long.

Now is the time to act, and Mozilla is in a unique position to take the lead.

It is essential for success to **leverage Mozilla's strengths**. Concretely, this includes:

- An active and diverse community
- A highly trusted brand
- A culture of openness and transparency
- Good data practices
- Experience with large-scale open web efforts
- Aspects of data ownership and use, as well as privacy and data protection
- Openness, transparency, inclusion, and opportunity for participation

Furthermore we strongly recommend to focus efforts on consumer IoT as opposed to industrial IoT.

Mozilla will have to identify which approach to implementing a trustmark is the best fit for the organization in relation to specific goals. We recommend matching this as closely as possible onto existing goals and initiatives.

Concretely, we recommend the following strategies, tactics, and activities:

More research

- To fully develop the labeling system, it's highly advisable to gather more data first from both consumers and industry partners. We recommend gathering more data—qualitative or quantitative—both from consumers through a Mozilla user survey campaign, as well as from industry partners. It's essential that consumers can find the information they deem most relevant in IoT trustmarks and that industry partners can use the trustmarks to differentiate themselves sufficiently with a manageable overhead. Only after insights from these surveys are available should the final development of an IoT trustmark take place.

- We recommend working with existing value-aligned organizations like the #iotmark through collaborations and/or to commission more research as needed.
- We recommend determining how the 10 principles of trustworthy technology laid out by Doteveryone can be applied to IoT specifically. This should be done by the Open IoT Studio, potentially with support by Doteveryone and/or external commissioned research.
- IoT poses some specific and unusual challenges for trustmarks. We recommend tapping into Mozilla's user and developer community to explore creative solutions (like a "best before" date that might help indicate for how long an IoT product is "stable" in its current build). This effort should especially seek out input from the global South.
- We recommend the trustmark be tested in public for a trial period (12-18 months), then re-evaluated for further improvement and/or formalization.

Less is more

- Identify the minimal viable set of characteristics/aspects to label and verify. If in doubt, less is more. We recommend an approach for the IoT trustmark that does a few things right rather than trying to solve too many things at once.
- We also recommend to involve partners who complement Mozilla's profile and whose involvement will be instrumental in promoting trust in IoT globally.
- Given Mozilla's culture and strengths, that means building the trustmark around openness, diversity, good data practices, and an open web approach, aiming to promote internet health and user empowerment. Especially at the start, the more clear-cut the profile, the better to start gathering insights and experiences.

Leverage existing programs and infrastructure

- Mozilla has a clear opportunity to feed the IoT trustmarks into their advocacy and research programs. This can and should start immediately.
- We recommend the IoT trustmark be considered for immediate inclusion in Mozfest, the Internet Health Report, and ongoing collaborations.

Develop an easy-to-understand trustmark

- Ease-of-use is essential for successfully establishing a system of trustmarks. We recommend exploring which communication would work best for IoT trustmarks: Visual markers embossed on devices and/or printed on boxes are an obvious path forward, but as outlined before, they are not without restrictions in terms of updatable connected products. QR codes linking to an open web registry or database might offer the required flexibility, and given their ubiquity in large parts of Asia, QR codes seem like a promising approach.

- In parallel to the research phase, development of proposals for a visual mark should begin. The look and feel as well as appropriate mechanisms for the IoT trustmark will have to be developed with designers' input. This could happen with in-house resources (for example within the Open IoT Studio network) or through external commissions. The trustmark needs to codify complex information in a way that is based on substance, easy to skim, actionable for consumers, and dynamic to account for the potentially ever-changing nature of connected products.
- The proposals should be prototyped and user-tested rigorously, with explicit attention given to if and how the trustmark works in emerging markets as well, preferably backed up by externally commissioned research, for example by Quicksand (India).
- To successfully communicate the trustmark later on, a snappy title and visual identity should be developed.

Mozilla needs to lead the rebel alliance

Having initiated working groups around topics like Web VR and others in the past, Mozilla is in a better-than-most position to convene an alliance around an IoT trustmark. Leveraging the organization's wide-ranging and diverse network, Mozilla would be a perfect leader of a "Responsible IoT Rebel Alliance" (#RIoTRebels). Building this alliance should begin immediately.

Concretely, we recommend building an alliance of 10 large players and 20 small organizations to support this initiative out of the gate. (ThingsCon and Just Things in Europe, both of which feature heavily among the experts in this report, are obvious candidates.)

The IoT trustmark will provide creators of IoT products a way to differentiate themselves on the market. With the right launch partners using IoT trustmarks might even become a desirable marketing tactic, which would further drive adoption. Startups and other "cool" smaller, more lightweight organizations are excellent vehicles who could drive this as early adopters.

We believe that Mozilla can play an instrumental role in convening the scattered initiatives that have been proposing ideas relating to IoT trustmarks, and in hosting this global conversation. Mozfest and the Internet Health Report are natural starting points.

When building an alliance to promote the IoT trustmark, make the case for all of the many beneficial side effects of an IoT trustmark, including the ability for producers to set themselves apart in terms of quality and user rights; increasing consumer awareness and literacy; and the network effects of highlighting and establishing best practices. This allows for a broader alliance and hence more impact.

Collaboration is key. We recommend a highly collaborative approach for the IoT trustmark and beyond. Concretely, we recommend reaching out to potential collaborators and discuss how to mutually support each other. Depending on the partner, this could mean joint projects, amplifying ongoing work, or supporting existing initiatives financially or through promotion, commissioning work, or other creative uses of existing resources.

We particularly recommend working with the #iotmark initiative to align the IoT trustmark and the #iotmark initiative's certifications, both of which take slightly different approaches but appear compatible.

Take a lightweight approach

We recommend aiming for a relatively light-weight trustmark approach and building it with and around an alliance of trustworthy organizations. For a light-weight approach, the IoT trustmark should tend towards the self-assessed and voluntary, backed up with "View Source" privileges. (Depending on context this could happen by making source code, documentation, or human-readable explanation of algorithmic decision-making accessible.)

We recommend weighing the label slightly towards the device level, but taking into account at least the most salient aspects of a more systemic nature. Especially where data processing happens in the cloud, this is highly relevant for users to know. How exactly this can be implemented should be based on further research and input from a user survey and workshops with partner organizations.

The light-weight implementation should help to keep the barrier to entry low, allowing for wider, quicker adoption. This allows especially smaller organizations and professional makers to join the movement more easily.

For all aspects of the trustmark, wherever possible, information should be provided to be verifiable. Best practices from the open source world (view source, Github, etc.) can serve as inspiration for appropriate mechanisms.

After a trial period, with more experience gathered, it might be worth formalizing the efforts and potentially getting government and industry bodies (like the European Commission) involved. It seems quite possible that further down the road IoT trustmarks will mature to the point where third party certification becomes viable. However, at the outset this appears to be too bureaucratic an approach.

Creative Commons-style label picker

Creative Commons (CC) offers valuable guidance for the implementation of the practicalities of label picking. With their three-tiered system (human-readable, lawyer-readable, machine-readable) and easy-to-use label picker, CC's modular guided system is both proven and well-respected enough that this general approach holds promise for IoT trustmarks.

- We recommend Mozilla launch a Creative Commons-style label picker for different versions of the IoT trustmark.
- We recommend working with Creative Commons or other parties who are familiar with their approach, like Mozilla board member Ronaldo Lemos, to help adapt and apply this model for an IoT trustmark.

One foot in Europe

As Europe emerges as a global leader in consumer, privacy, and data protection, we recommend leveraging Europe's position of strength and credibility in this space for the trustmark and related IoT efforts by strengthening partnerships within Europe and building out Mozilla's European footprint. As a rule of thumb, thanks to Europe's strict data protection rules, if a digital service passes the data protection rules in Europe, it is likely to pass them in other regions, too.

Compatibility is key

- To maximize impact while minimizing redundancy across the industry, we recommend identifying existing (or soon-to-be-existing) labeling and certification approaches that might be leveraged through compatibilities. For example, the IoT trustmark should consider one indicator for good data practices to be compatibility with the European data protection regulation GDPR, or an indicator for security to be fulfillment of the OWASP IoT Attack Surface Areas checklist.
- We recommend aligning the IoT trustmark to be compatible with the six principles for a trusted IoT as laid out by the European Commission in order to give the trustmark extra weight and leverage.
- We recommend working with the larger Mozilla developer community and advocacy team to identify the best external labels, certifications, and checklists for collaborations.

Explore collaborations with external high-impact organizations

- We recommend working with Consumer Reports to include the IoT trustmark as part of their evaluation framework.
- Insurances as well as city & national governments could be powerful partners for adopting and leveraging the IoT trustmark.

Make IoT health a central part of the Internet Health Report

- IoT health should become part of future iterations of the Internet Health Report. The IoT trustmark can serve as a useful indicator of shifts across the industry landscape.
- Allied organizations like ThingsCon and others can be tapped for further support in this area.

An aggregator site for relevant trustmarks

If Mozilla's IoT trustmark constitutes one essential mark of consumer trust for IoT (for example, for good data practices), then it would be even more powerful alongside other relevant trustmarks. Mozilla could, alone or as part of a larger alliance, launch a website that aggregates the most relevant trustmarks for each product. This site would track on the meta level which other allied labels a product has earned. For example, it could list an open source seal of approval ("check!"), the most relevant security marks for a product's category ("check!"), iFixit's reparability score ("8/10"), Restart Project's software lifecycle mark ("7/10"), etc. This would allow for more experimentation at the ecosystem level, and for synergies to organically surface.

Activities beyond the trustmark

Mozilla's experience with large-scale, global open source projects and campaigns offers opportunities to advance IoT health beyond labeling in way that would allow for more makers and producers of connected devices to comply with the IoT trustmark:

- **Adapt the Firefox plugin security approach for IoT.** Regarding how best to deal with IoT software updates that might alter the device and its security, the Firefox browser plugin or extensions practice might offer inspiration. As Solana Larsen, editor of Mozilla's Internet Health Report explains (Larsen 2017, pers.comm.), Mozilla has experience with browser plugins that could, through a software update, be modified to contain security flaws or even malware. There might be an opportunity for Mozilla might be able to develop a tool that automatically helps check for security of IoT software updates.
- **Lint for good data practices.** Lint is a software tool for programmers which flags suspicious code. A "Lint for good data practices" that highlights

potentially problematic security practices in code and nudges developers towards better practices would be a powerful tool in the fight for a trustworthy IoT. (Thanks to David Ascher for the original suggestion.) We recommend exploring commissions for a "Lint for good data practices" tool that David Ascher proposed and scaling it under Mozilla's roof to a global open source tool.

- **Checklists for trustworthy IoT.** Following the same line of thinking, for non-developers like product managers, designers, or entrepreneurs checklists are powerful tools. Rather than highlighting faulty code, a checklist might probe if a connected product would share data with third parties, if cameras could be physically blocked, or if selling user data was part of the business model.

ABOUT THIS REPORT

Summary: This report is based on extensive qualitative research including literature review as well as interviews, conversations, and workshops within and beyond ThingsCon's network of IoT practitioners and experts. The report aims to serve as a starting point for the development of an IoT trustmark.

This report aims to serve as a starting point for proposing and implementing a labeling system, for which further feedback from consumers and industry can be gathered.

Its structure is optimized for ease of reading and to allow for quick skimming:

1. The executive summary and our core recommendations summarize core ideas and findings, and lay out actionable recommendations.
2. The following chapters offer the densely sourced and referenced main report. It's the "View Source" that the recommendations are based on. Each chapter in itself also has a short summary of key findings at the top.

The redundancy between both sections is on purpose and serves to increase the transparency of the research.

Our research includes…

- Consumer labels 101: What types of labeling systems already exist and might serve as inspiration? Why trustmarks? What to label for, and approaches for verification.
- Landscape analysis: Overview of current approaches in adjacent fields, as well as first approaches in or around IoT labeling.
- A glimpse ahead: What other approaches and early stage proposals are out there that are relevant to IoT trustmarks? What other ideas go above and beyond, and which organizations are actively working on them? Who are potential allies and collaborators?
- Recommendations: Based on our findings we develop recommendations for the most promising and effective approaches and next steps to use IoT labels for

fostering a responsible, healthy, human-centric IoT.

Methodology

Our research is based on extensive literature review and desk research (for details, see the list of references), as well as expert interviews with practitioners—designers, developers, entrepreneurs and activists—from the ThingsCon network and other communities. This report also includes findings and insights from a workshop on the potentials and challenges of IoT trustmarks in July 2017. To broaden the input further, a small-scale qualitative online survey was active from late June to mid-August 2017 within the ThingsCon online community. Through this survey, input from several more experts and practitioners from the ThingsCon community informed this report. Last but not least, a large number of backchannel conversations across the ThingsCon network informed this research. These backchannel conversations—some of which took place under Chatham House rules —happened across a number of channels including Twitter, various ThingsCon-related Slack and social media channels, and in the context of various conferences. Finally, as part of our own active contributions to the London #iotmark initiative, insights and opinions from many experts within that initiative found their way into this research through numerous informal conversations.

Thanks

We'd like to thank the following experts whose insights contributed to this reports through conversations online and offline, public and in private. Also and especially we'd like to thank the larger ThingsCon and London #iotmark communities for sharing their insights.

Alaisdair Allan (freelance consultant and author), Alexandra Deschamps-Sonsino (Designswarm, IoT London, #iotmark), Ame Elliott (Simply Secure), Boris Adryan (Zühlke Engineering), Claire Rowland (UX designer and author), David Li (Shenzhen Open Innovation Lab), Dries de Roeck (Studio Dott), Emma Lilliestam (Security researcher), Geoffrey MacDougall (Consumer Reports), Gérald Santucci (European Commission), Holly Robbins (Just Things Foundation), Iskander Smit (info.nl, Just Things Foundation), Jan-Peter Kleinhans (Stiftung Neue Verantwortung), Jason Schultz (NYU), Jeff Katz (Geeny), Jon Rogers (Mozilla Open IoT Studio), Laura James (Doteveryone, Digital Life Collective), Malavika Jayaram (Berkman Klein Center, Digital Asia Hub), Marcel Schouwenaar (Just Things Foundation, The Incredible Machine), Matt Biddulph (Thington), Michelle Thorne (Mozilla Open IoT Studio), Max Krüger (ThingsCon), Ronaldo Lemos (ITS Rio), Rosie Burbidge (Fox Williams), Simon Höher (ThingsCon), Solana Larsen (Mozilla), Stefan Ferber (Bosch Software Innovation), Thomas Amberg (Yaler), Ugo Vallauri (The Restart Project), Usman Haque (Thingful, #iotmark).

About the author

Peter Bihr is the founder and Managing Director of The Waving Cat, a boutique strategy, research & foresight company where he explores impact and opportunities of emerging technologies—especially Internet of Things (#iot). As an advisor, he helps organizations excel in an environment shaped by digitization, connectedness and rapid change.

Peter co-founded and chairs the the board of ThingsCon e.V. which fosters the creation of a human-centric & responsible Internet of Things. He has co-founded and chaired many acclaimed emerging technology conferences including ThingsCon, UIKonf and Cognitive Cities Conference, and served as co-chair of Interaction16.

Peter is the author of *View Source: Shenzhen* and *Understanding the Connected Home* (with Michelle Thorne). He has provided research and policy recommendations to governments and global tech companies, supported automotive clients with R&D strategy, and helped organizations embrace innovation opportunities as an external radar and sparring partner.

His projects, thoughts and other antics have been featured in Forbes, New York Times, The Guardian, ZDF, ZEIT and many others. He was named a Top 100 Influencer in IoT in 2016 (Postscapes). He blogs at thewavingcat.com.

Full disclosure: The author is married to Michelle Thorne of Mozilla's Open IoT Studio.

ThingsCon fosters the creation of a human-centric & responsible IoT. To this end we provide practitioners with an open environment for reflection & collaborative action. ThingsCon is a global community of practitioners around Internet of Things (IoT), as well as a global event platform for activists and practitioners in IoT.

We believe that technology should be empowering, respectful, and inclusive. Currently in IoT, not all voices are heard equally, and not all services and products are designed in a way that is human-centric and with the public good in mind. We are convinced that good ethics equal good business. Learn more at thingscon.com.

The Waving Cat is a boutique consultancy that explores the impact and opportunities of emerging technologies—especially Internet of Things (#iot). We offer strategy, research and foresight with a focus on #IoT, emerging tech & innovation to help organizations excel in an environment shaped by connectedness, uncertainty and rapid change.

We work with organizations who strive to shape their field rather than follow. We help identify opportunities to do just that—and have a global network of leading experts by our side. In everything we do, we take a responsible & human-centered approach to technology, business and culture. Learn more at thewavingcat.com.

INTRODUCTION: WE NEED A TRUSTWORTHY INTERNET OF THINGS

Summary:
IoT poses a number of specific challenges that allow consumers—and even experts—very little insight into how a connected product works and what it might be capable of, like which types of sensors it contains or uses, what data it captures and shares, if its producers employ responsible data practices, etc. Trust is a critical challenge and a necessity for a thriving Internet of Things ecosystem, but how can users trust IoT? To add to the complexity, a remote software update might change the product fundamentally by activating or deactivating features or sensors, and just like with other software, users cannot meaningfully control this dynamic.
With its physical components that live in our homes, IoT is susceptible to all the well-known software security issues, but it additionally faces even worse challenges and risks including, surveillance, risk to physical safety, sunsetting, selling/sharing of user data, and many more.
Consumers must be able to make an informed decision on IoT products, and transparency is an essential first step. We believe that a much higher level of transparency is both essential and possible. We propose a number of questions to evaluate IoT products and highlight ten areas of challenge & opportunity that Doteveryone identified for evaluating responsible, trustworthy tech.

The Internet of Things (IoT) with its dizzying array of connected products and services is hard to navigate: Consumers have little insight into what any one connected product does, or what it even might be capable of—nor if the company employs good, responsible data practices.

This is not an oversight on the consumers' side. As a buyer of connected products you simply cannot really know. This has to do with the way connected products work (1), and with an overall lack of transparency (2).

(*Please note that for the purpose of this document, we use "connected products and services" more or less interchangeably with "IoT", unless otherwise specified.*)

At the same time, technological change is accelerating, while literacy does not necessarily keep up equally across different sections of society. During his time as an advisor for cross-cutting policy and research issues at the European Commission's Directorate-General for Communications Networks, Content & Technology (DG CONNECT), Gérald Santucci was in charge of DG CONNECT's IoT unit. In an interview (Santucci 2017, pers.comm.) he explains: "The main challenge today—for the Internet of Things but also for all digital technologies—is what we can call the 'acceleration of change'. (...) We are on the crest of a big wave of disruptive change."

> ***"Trust is a critical challenge and a necessity for a thriving Internet of Things ecosystem."*** *—Gérald Santucci*

Santucci (2017, pers.comm.) shares parallels he sees between the challenges of RFID technology in the mid-2000s and IoT today, namely a "widespread sense of uncertainty and anxiety" requiring further building of trust. He notes that the same is true for IoT today: "But [in IoT] the challenges are even greater. First, because our relationship to objects changes—objects talk to each other and to us. Second, because advances in ICT are pulling true intelligence from the cloud to the 'edge' of the network, i.e. where people are, thus creating a new class of applications that enable natural user interfaces—smart, connected objects think on our behalf."

(1) How connected products work

Connected products and services (or IoT) consist—roughly speaking—of a *hardware* part (the device) and a *software* part (often a cloud-based online service). The capabilities and features of IoT products depends on both.

A smart home hub might include hardware elements that exist primarily to allow for future updates: For example, it might by default ship with only the connectivity features (wifi, Bluetooth) activated, but it also contains a microphone, a speaker, and an accelerometer. The microphone and speaker might lie dormant until activated by a later software update intended to enable voice control. The accelerometers might not serve any function at all but simply be included because certain chipsets (due to economies of scale) are cheaper to buy with accelerators than without them.

This update-ability is one of the biggest benefit of IoT. It means that products can improve over time. They can learn, adapt, and be personalized through use. Features can be added or refined. Security patches can be applied as needed.

However, there is a flip side to ongoing updates. First, **many products require the central server** (or cloud service) of a company to function **and hence have a single point of potential failure**. As part of a company acquisition, users can be forced to sign a new end user license agreement (EULA) that changes the relationship between user and provider. If a company goes bankrupt or simply decides that a particular product isn't worth maintaining anymore, their service will stop working. The consumers might be stuck with a dysfunctional ("bricked") product. (There are strategies against this, most notably decentralization and open source.)

Second, **for consumers it's nearly impossible to know the exact capabilities of connected products** they are about to invite into their lives. This extends to professional reviewers, too: Product testers and consumer rights organizations have been struggling with how to test IoT products. If a product can change overnight, traditional testing procedures are inherently inadequate. (See the chapter *Other Research* for a promising approach.)

Third, as Solana Larsen, editor of Mozilla's Internet Health Report points out: In the context of IoT, security often is not just an issue of the device itself but also of other devices you pair it with (Larsen 2017, pers.comm.). Hence, **even an otherwise secure device might not offer real security once it is connected to another, less secure one**. The chain is only as strong as its weakest link.

(2) Lack of transparency

It is anything but simple to learn what exactly a connected product is capable of and even what its exact features are at any given time.

As Thomas Amberg, founder of IoT platform Yaler and organizer of the IoT Zurich community points out (Amberg 2017, pers.comm.), IoT products are also intransparent in their workings because they contain many invisible parts and processes, and they can change through software updates. Short of reading—and trusting—the software release notes for every single update there is currently simply no way of knowing that is reasonably accessible to consumers.

Usually **there is no opportunity for users to opt out of a service during software updates**. If a company decides to push a major update to your smart home hub, and you didn't agree with that update, the only option would be to throw out the product altogether. From a consumer point of view, this is unacceptable.

Consumers must be able to make an informed decision on IoT products, and transparency is an essential first step. We believe that a much higher level of transparency is both essential and possible.

For inspiration on how to best approach this issue, this document examines a range of existing and potential approaches to increase transparency through labeling, from certification to self-assessment. These existing or proposed labeling systems approach IoT from different angles, like making transparent a product's capabilities, origin, or data practices. Each approach has different strengths and weaknesses, and a different focus.

What all of the approaches have in common is that they **aim to increase transparency through human-readable labels.**

This document aims to give a top-level overview of existing and proposed labeling systems—the lay of the land rather than a comprehensive catalog—and relevant related approaches we see emerging. Furthermore, we make recommendations for increasing transparency, and empowering users, in ways that build on and leverage Mozilla's unique position and credibility in the open web ecosystem.

Challenges of the Internet of Things

The Internet of Things (IoT) faces and poses a number of specific challenges and risks. Some of these concerns are inherent in any IT system, like security or privacy. Others are more particular to IoT, for example that the capabilities of a physical product can be changed substantially through a software update.

In our research we identified a set of main challenges of IoT products:

- Security breaches
- Risk to physical safety
- Surveillance
- Sunsetting
- Selling/sharing of user data
- Bugs & licensing
- Products can change through a software update
- Issues with device re-use
- Lifecycle and maintenance
- Unintended consequences

Having those risks in mind allows for better analysis of IoT labeling approaches.

Security breaches are the bane of IoT products. Lack of security, especially in consumer-grade IoT products, is often a result of market pressures. Consumers usually don't pay premium for security—at least not yet.
As security expert Bruce Schneier (2016a) summarizes: "The market can't fix this because neither the buyer nor the seller cares. Think of all the CCTV cameras and DVRs used in [a recent attack]. The owners of those devices don't care. Their devices were cheap to buy, they still work, and they don't even know [the attacked]. The sellers of those devices don't care: they're now selling newer and better models, and the original buyers only cared about price and features. There is no market solution because **the insecurity is what economists call an externality: it's an effect of the purchasing decision that affects other people. Think of it kind of like invisible pollution.**"
Other sources of weak security are lax data and security practices like simple-to-crack default passwords or insufficient software maintenance, which means security updates are not provided in a timely manner or throughout the full product lifecycle.

The type of security incidents we have seen either in the wild or as part of demonstrations include hacked microphones in connected toys, like the connected doll Cayla which was made illegal in Germany (see Bihr 2017), IP-based security cameras becoming part of a botnet (Schneier 2016b), cutting a car's transmission remotely (Greenberg 2015), and holding thousands of computers of San Francisco's public transport system hostage for Bitcoin (Gibbs 2016).

In many cases, owners of infected IoT devices are not even aware that their devices are infected and contributing to this issue.

Risk to physical safety is a real concern when issues of digital security start to leak over into the physical world. This becomes manifest when a car's transmission is cut remotely (Greenberg 2015) or when sensors start capturing our physical movement through the world (OTA 2017:1): "Risks to one's personal and physical safety have become reality. All too many connected devices sold, ranging from automobiles and thermostats to children's toys and fitness devices, have insecure remote access and controls. By default many collect vast amounts of personal and sensitive information which may be shared and traded on the open market. The majority of these devices do not have the functionality (or an easily discoverable method) to easily remove ones personal data."

Surveillance is one of the potential "side effects" of lacking security. Criminals of all stripes, as well as governments, can potentially break into connected products and activate microphones or cameras for surveillance purposes. The levels of sophistication required to do so vary, as do the motivations. However, even the possibility that an internet-connected microphone or camera might be compromised is understandably worrying to many consumers. Research suggests that even the perceived chance of surveillance has a self-censoring impact on individuals (Penney 2016), and it undermines trust in IoT.

Sunsetting/bricking: Sunsetting is an industry term that describes discontinuing support for a connected product. Reasons for sunsetting include bankruptcy but also strategic re-orientation and/or lack of revenue from a product line. The term sunsetting is mostly used if the product itself will not work anymore, also known as "being bricked". If the service or software is not open-sourced so that it might be continued to be operated by a third party, this otherwise fully functional hardware is turned into junk.

Selling/sharing of user data is, like on the World Wide Web, increasingly a business model for IoT services. Depending on the type of data, and how it is aggregated and anonymized, this may be less or more problematic. Harvard Business Review gives an example of a car company selling usage data to local government (Lewis, McKone 2016): "Toyota, the master of assembly line efficiency, has built a new business that takes advantage of the GPS navigation devices it installs in cars sold in Japan. It captures the speed and position of cars and sells traffic data to municipal planning departments and corporate delivery fleets at prices that start at $2,000 a month." Using aggregate data for urban planning sounds like a benign example. It's possible to make a business case for selling data without exposing customers to risks. But truly anonymizing usage data of a connected product is not trivial, especially given that **advances in machine learning can be expected to make analysis—and de-anonymization—of large data sets ever easier.**

Software bugs, restrictive licensing and other *de facto* malfunctions are a fact of life in the 21st century. IoT products are no exception. A connected product requires hardware, software, and frequently an online service to work hand in hand flawlessly. Frequently, it will also be part of a larger networked arrangement of connected services, which amplifies the complexity and hence the potential for issues to emerge. Yet, unlike with historically analog tools like home appliances, consumers can rarely fix these issues themselves. **Due to proprietary software as well as software licensing agreements that users are forced to agree to**

upon first activation, frequently it is impossible or even illegal for users and third party experts to repair or modify a connected product they bought, or *licensed*.

Products can change through a software update. A software update—installed remotely as a so-called *Over the Air* (OTA) update can add or remove, enable or disable, or change features of a connected product. This means the very nature of an IoT device might change over night, and consumers would have little recourse. An update that fixes a security vulnerability on a smart watch or improves energy efficiency of a connected fridge is generally welcome. However, what if a software update means that a smart car would from now on only allow driving on local roads unless unless the driver pays to "unlock" highways?

Issues with device re-use. As far as personalized devices are concerned, device re-use is awkward at best. Wiping even something as common as a smartphone or laptop completely and reliably from personal data is not trivial. In scenarios of connected products—like for example a smart home setup—this gets exponentially trickier. Users don't want their data to fall into another person's hands, nor do they want to inherit someone else's data—or algorithms trained with that data. As connected products become more ubiquitous, they need tools, processes, and the skills to prevent and avoid data shadows.

Lifecycle and maintenance. Due to the high speed of innovation, the lifecycle of connected products tends to be relatively short. This is especially pronounced in the space of smart appliances: Where a fridge might have traditionally lasted 10+ years, a smart fridge is likely outdated within just a few years. Long-term maintenance is a cost factor that especially startups, but also other companies, are often unwilling or unable to commit to. The practice of *sunsetting* of services (i.e. withdrawing support for them) undermines user trust and is highly unsustainable. In order to trust in adequately long lifecycles, service guarantees and a strategy for enhancing lifecycles on the side of producers seem necessary.

Unintended consequences and unexpected dependencies are hard to avoid. Life is messier than the clean product videos of cloud computing companies suggest. In a real-life smart home scenario, a family might daisy-chain a whole range of connected products together.
These dependencies might lead to unintended consequences. For example, if Amazon's cloud offering AWS goes down—as it rarely, but not never—does, then it might take IFTTT down with it. IFTTT in turn is used widely to program simple behaviors of connected products, like switching on smart lights if a certain light level is measured. AWS goes down, IFTTT goes down, the light stays off.

Companies cannot control how their products are deployed and used in real life. They can however design services to be less reliant on centralized cloud services and assume that in the messy real world their consumers will find their own ways of making their products work for them.

At any given time, consumers should have a clear answer to four simple questions:

1. "Does it do what I expect it do do?"
2. "Is the organization trustworthy?"
3. "Are the processes trustworthy?"
4. "Does it do anything I wouldn't expect?"

This is where IoT trust labels come in.

What makes tech trustworthy?

Before moving on to the labels themselves, it's worth taking a moment to ask what constitutes trustworthy technology. This is not easy to define, as it's mostly a case of *you know it when you see it*. That said, for the purpose of this research we consider tech trustworthy when it considers all stakeholders; takes a long view and sustainable approach; focuses on value creation rather than extraction; and if in doubt, it errs on the side of openness and empowerment.

British digital literacy non-profit Doteveryone have shared some of their early thinking around what it means for digital technology to be responsible. This is written with all digital technology in mind—not just IoT—but we support the areas they identify as a canvas against which to analyze technology, including trustworthy IoT. Doteveryone identifies these ten areas (James 2017b, quoted in full):

- ***Business models, ownership and control***
The business model and organisational structure should be appropriate for the tech in question, and the value given and received by different stakeholders should be reasonable. Organisations should be established in appropriate locations, and should of course follow local and international law, pay their taxes, etc.
- ***Employment and working conditions***
Everyone involved in producing tech should have fair pay and conditions, and work in environments free from exploitation. Workplaces should be inclusive in terms of gender, age, ethnicity, etc. CEO to worker pay ratios should be

reasonable. All the above should apply to the supply chain, including subcontractors, hosting providers and so on, not just those directly creating or operating the tech in question.

- ***Reward for contributions***

Services that use people's labour or information should reward those people fairly for their contributions. (This could include anything from data analysis to microtasking to Google's "I'm not a robot" reCAPTCHA.) Rewards could take many forms — pay, shares, in kind benefits, discounts, etc. — but should be fair for the value generated by the information or effort contributed. Materials which are reused should be attributed appropriately.

- ***Societal impact***

Technology should add something to the world — or, at the very least, not take anything away. In addition to a product or service's actual function, organisations should consider contributing to public or commons infrastructure, and their impact on public services.

- ***Unintended consequences***

Not all risks can be avoided, but they should be anticipated, and actions to avoid them — or to mitigate their consequences — should be planned. During both design and maintenance, systems effects, side effects, and potential harms for different people, stakeholder groups or the wider environment should be considered. This should not be limited to what happens if things go wrong; plans should also include what happens if a product or service becomes overwhelmingly successful.

- ***Maintenance, service and support***

Responsible technology needs to work tomorrow as well as today. All products and systems should offer help and support to users, and offer service including access to necessary updates for a reasonable period, and graceful degradation when necessary. This means that at the design stage there should be consideration of what happens to customers if the product or service doesn't take off, or if the business fails, or if the business is acquired by someone else.

- ***Understandability***

People should be able to easily find out and understand how a product or service works. This includes clear, understandable terms and conditions, but goes beyond that; costs, service levels, and specifics such as data sourcing, storage, management and sharing, etc., should all be accessible and comprehensible. Users should understand how to raise concerns or complain about the service, and know what to expect if something goes wrong or changes.

- ***Best practice***

Responsible technology is useful technology, that interoperates with other *things as far as possible and is designed for real people and situations. In whatever technology is being developed, appropriate standards and best practices should be used, and any particular technology-specific guidelines around ethics should be followed. To ensure the technology is useful, good design practices such as human-centric design and systems design should be used throughout development, testing and operations. Depending on the product or service, sustainability considerations may also be relevant — that might mean hardware designed for reuse, repair or recycling, or energy use. Reusing appropriately licensed code is also good practice!*

- ***Usability***

Especially if a broad range of users are expected, or if people will be compelled to use a product or service, accessibility and support should be appropriate. This includes conventional accessibility considerations — for example, designing for screen readers — but goes much deeper. Does a product or service work for someone with mental health issues, or memory problems? Someone who relies on a carer? Someone who does not have access to a smartphone, or an old phone, or limited or filtered internet access? Enabling support staff to work around exceptional cases is key.

- ***Context and environment***

Nothing operates in isolation. The context technology operates in should be appropriately considered and addressed — including who may use or encounter it, and how it may be interpreted. A service that offers support and guidance should be clear that it's offering advice, not dictating choices; ambient home technology should consider what happens if it's used by children, guests, etc.

TRANSPARENCY & TRUST: THE CASE FOR TRUSTMARKS

> *"Trust arrives by foot and leaves by horse." —Dutch saying*

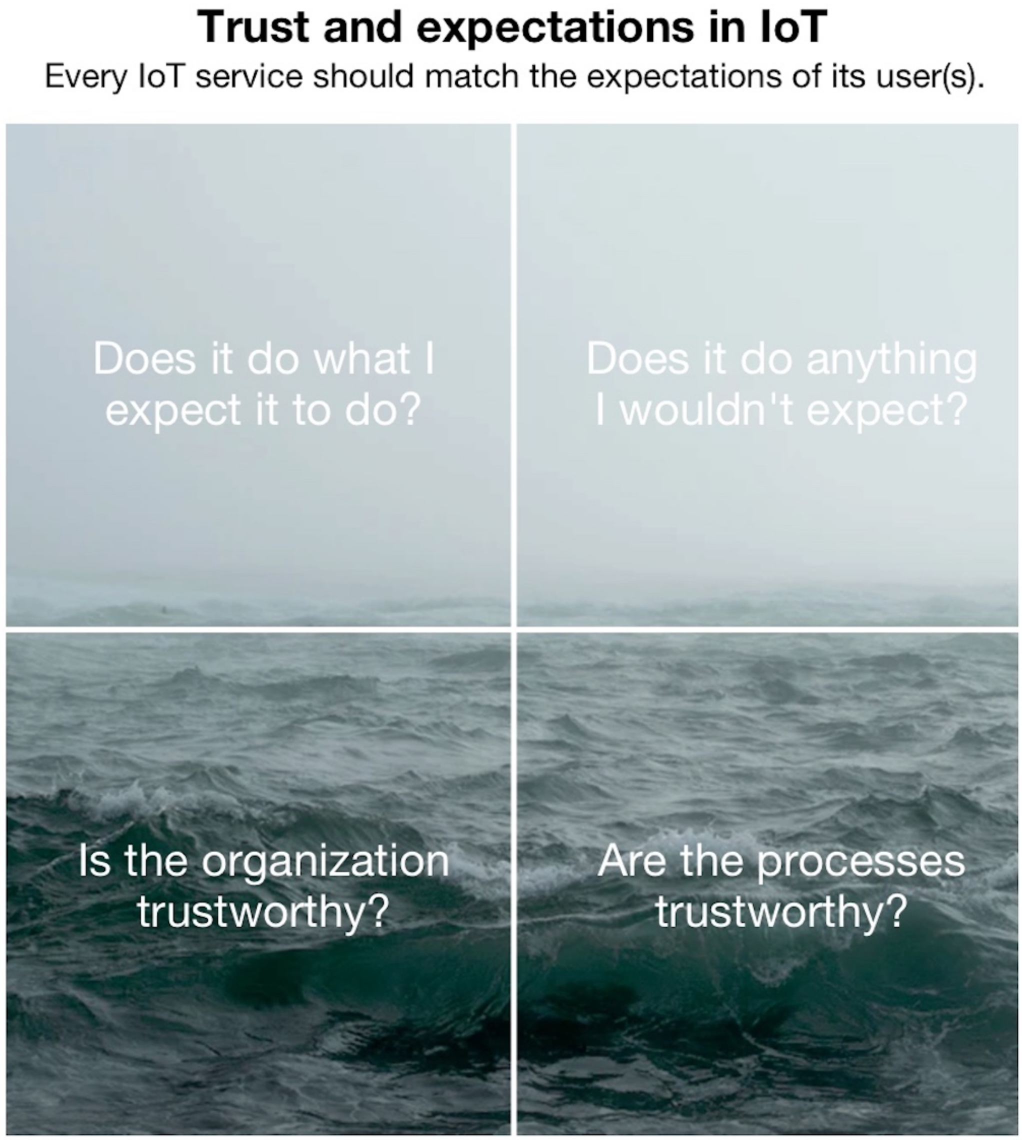
Summary:
Transparency gives users agency and autonomy. To help consumers make informed decisions, it is essential to increase consumers' abilities to understand and evaluate IoT products. From other areas like nutritional labeling, we know that consumer labels are powerful and help consumers make healthier and more sustainable choices. Currently, consumers lack the tools to make these smart choices for most IoT products. As an expert put it: "The public wants to buy secure products. But they can't, because they can't tell the difference between Internet of Things and Internet of Shit."
We propose a consumer label, more specifically a trustmark for IoT, because it increases transparency and expresses the explicit intention of increasing—and deserving!—consumer trust. Research shows that trustmarks are effective and enjoy high levels of trust by consumers. They allow consumers to make informed decisions and also allow producers and makers a way to differentiate themselves on the market. They have other beneficial side effects, too, like highlighting best practices and validating good design decisions and data practices.

Recommendations:

- *The trustmark allows developers of IoT products to differentiate themselves by "doing the right thing" and consumers to make smarter choices and put pressure on all developers to follow suit. This creates a virtuous cycle in favor of a trustworthy IoT.*
- *When building an alliance to promote the IoT trustmark, make the case for the many beneficial side effects for all of an IoT trustmark including the ability for producers to set themselves apart in terms of quality and user rights; increasing consumer awareness and literacy; and the positive network effects of highlighting and establishing best practices.*

Trust is one of the key challenges for Internet of Things (IoT) in the consumer space, and it boils down to expectation management: For consumers it's unreasonably hard to know what to expect from any given IoT product or service. But if they knew what to expect, trust would follow where appropriate.

Any user should be in a position to answer these four questions to determine trustworthiness of an IoT product:



Trust and expectations in IoT

Every IoT service should match the expectations of its user(s).

Does it do what I expect it to do?

Does it do anything I wouldn't expect?

Is the organization trustworthy?

Are the processes trustworthy?

Trust and expectations in IoT by Peter Bihr (image available under CC by)

Does it do what I expect it do do? This should pretty straightforward for most products: Does the fitness tracker track my fitness? Does the connected fridge refrigerate? Does this smart home hub's digital assistant let me order groceries from the vendor of my choice?

Is the organization trustworthy? This question is always a tough one to answer, but it comes down to building, earning, and keeping the trust of your consumers and clients. This is traditionally the essence of brands. Mozilla, for example, has established a long-standing track record of openness and inclusion. Hence new products launched by Mozilla enjoy a certain trust credit.

Are the processes trustworthy? Internal processes are hard to interrogate. Organizations could differentiate themselves positively by being as transparent as possible. For example, a producer of IoT products should publicly and in an easy-to-understand form communicate if they follow best practice data and security practices.

Does it do anything I wouldn't expect? This question is essential. Connected products often have features that may be unexpected to the layperson, sometimes because they are a technical requirement, sometimes because they are added later through a software update. Whatever the reason, an IoT device should never do anything that their users would not reasonably expect them to do. To pick a toxic example, it seems unreasonable to expect that a smart TV would be always listening and sharing data with a cloud-service.

We recommend going beyond merely meeting consumer expectations and instead aiming to exceed them, a notion echoed by Iskander Smit. In all parts of his work, trust in IoT is of paramount importance: In his role as innovation director at info.nl, he oversees the designing and making of IoT products; as organizer of ThingsCon Amsterdam, he and his team aim to provide designers with relevant knowledge; and in the research environment of his role of a visiting professor at TU Delft, ethics in design plays an essential role. Smit proposes (2017, pers.comm.) that **products should respect the perceived privacy and security but also go further and respect levels of privacy and security that consumers do not—or would not know to—explicitly ask for.**

Trust vs. "hidden IoT"

Smit applies trust, or rather trustworthiness, broadly as he points to a new trend: **"Hidden IoT" refers consumer products describes appliances that are IoT ready or even already connected, even though they are not sold under the label of IoT or "smart".** According to Smit (2017, pers.comm.), this brings "new challenges in 'protecting' users from unintended or unwanted functions and risks." He points to the example of smart TVs, which in some cases spy on their users, presumably without proper consent, or implement such poor data security practices that they pose a risk to users:

- In 2015, Samsung smart TVs sent users' voice searches and data over the internet unencrypted, allowing hackers and snoopers to listen in on their activity" (Gibbs 2015).
- More recently, the FTC filed a complaint to the New Jersey Attorney General about Vizio (who settled the case for USD 2.2m), which had been tracking and also selling consumers' watching habits to advertisers: "Starting in 2014, Vizio made TVs that automatically tracked what consumers were watching and transmitted that data back to its servers. Vizio even retrofitted older models by installing its tracking software remotely. All of this, the FTC and AG allege, was done without clearly telling consumers or getting their consent." (FTC 2017)

Smit recognizes the inherent tradeoff between functionality and intrusion for connected products like personal assistants and connected speakers, and he stresses: "As humans we need a personal free space for living without the potential danger of being listened to or data captured, etc. Losing this personal space will harm individuals' well-being, and **violating products will create distrust in the category as a whole**." (Smit 2017, pers.comm.)

Trustmarks have beneficial side effects

There are benefits to a trustmark that go beyond the primary intent of verifying and promoting consumer trust:

A trustmark or consumer label can increase consumer awareness and literacy in certain areas (like data capture and processing, or security).

A trustmark can offer producers of IoT services and products a way to distinguish their products from less wellmade others. A key issue according to experts including Lilliestam (2017, pers.comm.) is that there are currently no economic incentives for cheap devices to be secure. This is in stark contrast to other areas where we know that security is a premium that's worth paying for. Trustmarks have the potential to change that dynamic for the better.

A trustmark has shaping power, as Thomas Amberg (Yaler, IoT Zurich) points out (2017, pers.comm.): By highlighting best practices it can establish a reference model for others to follow. Furthermore, recognizing responsible design practice validates good work, creating incentives for producers and designers (Smit 2017, pers.comm.) and elevating the industry to new levels of best practice.

A trustmark can create a virtuous cycle. The trustmark allows developers of IoT products to differentiate themselves by "doing the right thing" and consumers to make smarter choices and put pressure on all developers to follow suit. This creates a virtuous cycle in favor of a trustworthy IoT.

LANDSCAPE OF EXISTING RELEVANT CERTIFICATIONS, LABELS & MARKS

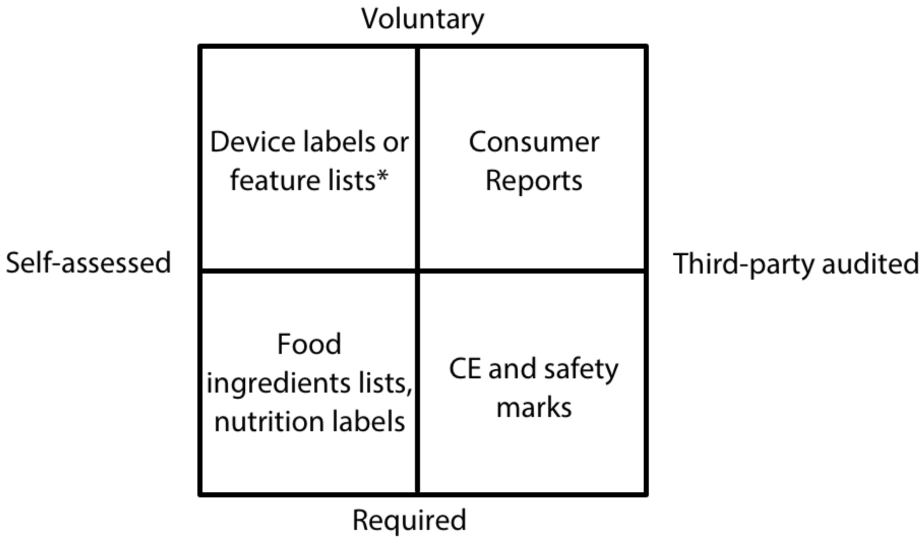
Summary:
Trustmarks for IoT do not, and could not, exist in a vacuum. We surveyed the landscape of existing labeling approaches from a wide range of areas from electronics safety, to nutritional and textile labels, to Creative Commons licensing. None of them solve the specific set of challenges we see in IoT, but all are relevant for this context and can guide the development of a trustmark for IoT.

Recommendations:

- *The IoT trustmark should tend towards the self-assessed and voluntary, backed up with "View Source" privileges. (Depending on context this could happen by making source code, documentation, or human-readable explanation of algorithmic decision-making accessible.)
- We recommend weighing the label slightly towards the device level (as opposed to focusing primarily on organizational or legal aspects), while taking into account at least the most salient aspects of a more systemic nature. Especially where data processing happens in the cloud, this is highly relevant for users to know. How exactly this can be implemented should be based on further research and input from a user survey and workshops with partner organizations.*
- Creative Commons' approach offers valuable guidance for an IoT trustmark: Aiming to complement rather than replace existing frameworks, granting rather than restricting the freedom of producers, making licenses accessible through the lawyer/human/machine readable layers, as well as the simplicity of the license picker all combine into a blueprint for an IoT trustmark.

Trustmarks for IoT do not, and could not, exist in a vacuum. The following pages highlight several existing approaches that are relevant for the context of IoT trustmarks. Some are relevant because they might apply to a subset or superset of the products that IoT trustmarks might apply to. Others because their processes, structure, or approach can inform the development of a trustmark for IoT.

From a 10.000 foot perspective, the overall landscape of labels, certifications and reviews looks roughly like this:



Voluntary

Self-assessed

Third-party audited

Required

Device labels or feature lists*

Consumer Reports

Food ingredients lists, nutrition labels

CE and safety marks

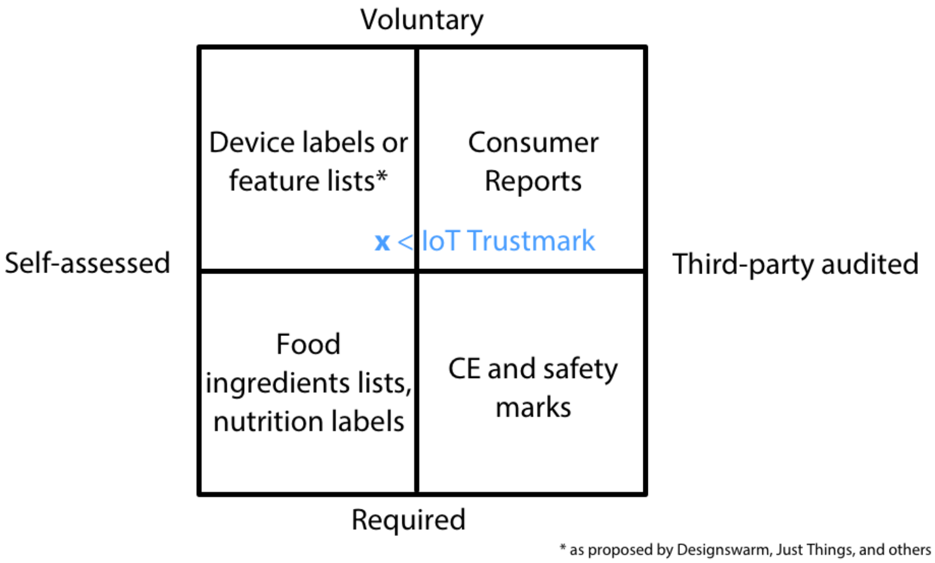
* as proposed by Designswarm, Just Things, and others

Landscape of labels, certifications & reviews. Where does the IoT trustmark fit in?

The two axes denote...

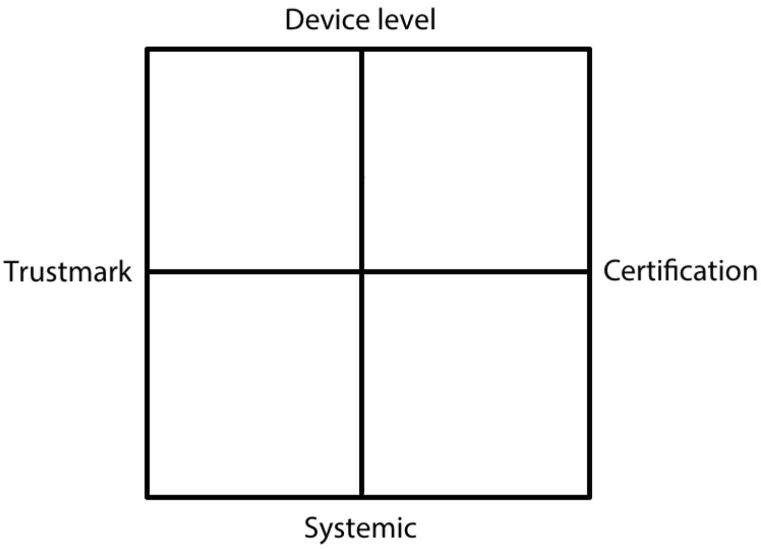
- **X: Self-assessment vs. third-party assessment**
  Does the producer provide the relevant information or is there an external party to assess, verify, or certify data? This is highly relevant for trustworthiness as well as the required bureaucratic overhead.
- **Y: Voluntary vs. required**
  Are the labels, and all involved information, verification, certification, etc. voluntary additions initiated by the producer, or a requirement (legal or otherwise) to enter a certain market?

For example, nutrition labels and ingredients lists are a legal requirement for selling food in many jurisdictions like Europe. The information is provided by the producer. Hence, the label is in the quadrant "self-assessment/required". In the quadrant "3rd-party assessment/voluntary" we see consumer review services like Consumer Reports: A Consumer Report rating or test is not legally required, and the testing happens entirely independently from the producer or manufacturer. Safety-related marks like safety marks and CE certification are legally required to sell certain categories of products and are to a larger or lesser degree based primarily on producer-provided information or on external assessments (that require a range of overhead and costs, depending on category, assessment location, etc.).


Voluntary
Self-assessed
Third-party audited
Required
Device labels or feature lists*
Consumer Reports
x < IoT Trustmark
Food ingredients lists, nutrition labels
CE and safety marks
* as proposed by Designswarm, Just Things, and others

A proposed positioning for a IoT trustmark.

But in order to develop an IoT trustmark, there's also the question whether to target the device level or to take into account a more systemic perspective, like networking features, cloud computer aspects, and organizational structures:

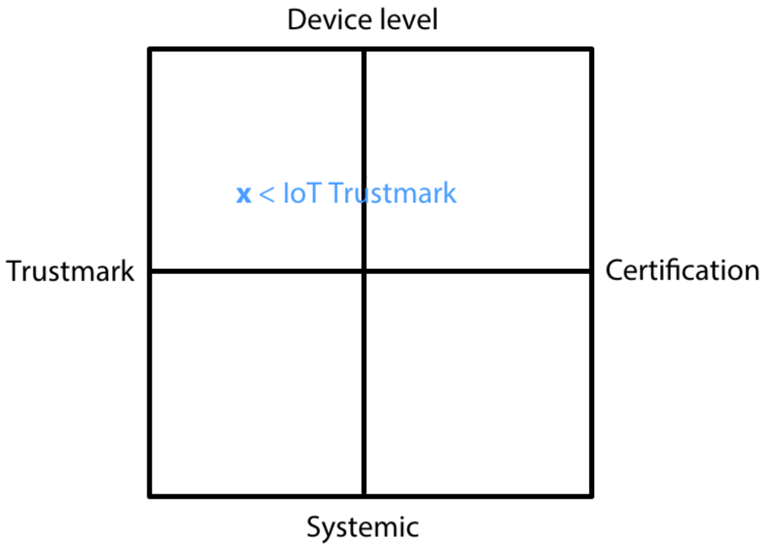


Where and how to target an IoT trustmark?

Fairphone's arguments for a systemic approach are strong (Fairphone 2015):

"Certifications can be granted to a specific product or to a company as a whole. While product certifications are probably easier to understand for consumers (eg, the coffee I buy is Fairtrade Certified) we believe a more systemic, company approach is necessary (eg, B Corp certifies a company in its entirety). (...) An example that illustrates the shortcomings of the process followed by some auditors is the Rana Plaza disaster in 2013 in Bangladesh. Eight floors of a sewing workshop collapsed killing 1100 people and leaving 2000 injured. This production site had been certified following well-known standards on international labor and safety standards, but the auditors failed to identify the structural problems of the building."

We recommend weighing the label slightly towards the device level, while taking into account the most salient aspects of a larger ecosystem. Especially where data processing happens in the cloud, this is highly relevant for users to know.



A proposed positioning for a IoT trustmark.

Scott Jenson, the lead for Google's Physical Web project, explores how much a layered approach has helped the open web thrive (Jenson 2017, highlights added):

> ***One of the reasons the web has been so successful is that it's open and layered. Everything from lower-level transports to higher-level content are their own open layer, so they can each grow and improve independently.*** *The web has used this approach for more than 25 years, and while it hasn't always been rapid, it has resulted in quite a bit of trust and*

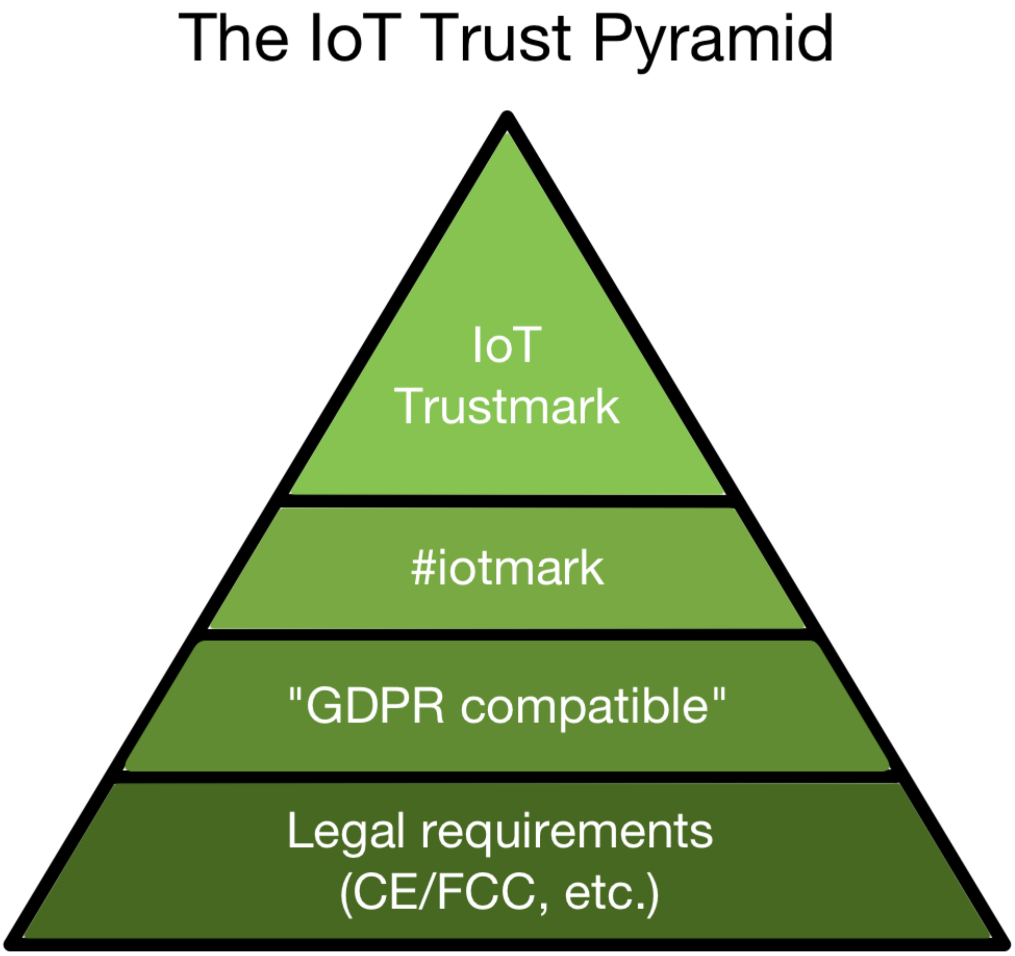
> *growth as no one company or organization owns the entire stack. The IoT could greatly benefit from a similar approach. Imagine one company controlling the API of every smart device on the planet. It's too vast a space for this to be possible.*

Writing about his experience as CEO of Creative Commons, Joi Ito, too, emphasizes the role of interoperable layers of standards—especially those that emerge organically from the bottom up (Ito 2009):

> *TCP/IP and the Web are successful because they are open standards shepherded by non-profit organizations which are custodians of a bottom-up process taking inputs from and creating consensus from a wide variety of stakeholders. (...) Having 100 Internets or 100 World Wide Webs governed by incompatible "standards" would suffocate the network effects that we enjoy on our one interoperable Web. Having a single set of copyright licenses and a single metadata format is key to creating the network effect of interoperability at the collaboration/legal layer. (...) In the early days, those of us who were proponents of TCP/IP had to argue with regulators, lawyers and technologists who for a variety of reasons did not support TCP/IP. (...) Just as we have seen with each new layer of the Internet stack, I believe that Creative Commons will soon become, in hindsight, an obvious thing and that all of the yet to be imagined innovations will have a dramatically positive effect on business, society and the environment.*

These lessons are highly relevant for the IoT trustmark. Here, too, we need a shepherd and custodian of an open, emerging standard. Here, too, we are faced with regulators, lawyers, technologists and lobbyists who find reasons why this effort is doomed to fail. And last but not least here, too, **the IoT trustmark will in hindsight become an obvious thing with dramatically positive effects on society.**

Trustmarks are one interoperable layer—in this case a trust layer—to apply alongside other layers and building blocks. Some of these building blocks might be other consumer labels or certifications, other might be technologies or protocols.



The IoT Trust Pyramid. Peter Bihr / The Waving Cat

A possible IoT Trust Pyramid: The various relevant layers of trust credentials stack up. From minimum legal requirements (like CE/FCC marks) through regional-but-valuable quality seals (like compatibility to GDPR), through quality certifications like the proposed London #iotmark initiative all the way to an aspirational, progressive trustmark for IoT that keeps pushing the boundaries of what a responsible, healthy and trustworthy IoT can look like.

Below we look at a few existing approaches for labels and certifications and how they might be beneficial inspiration for the development of an IoT trustmark.

Open Source Hardware Certificate

The Open Source Hardware Association's approach for certifying the open sourceness of hardware is built on self-certification (OSHWA 2017):

> *"Any producer may self-certify at any time that their products meet the requirements for an Open Source Hardware Association Certification. In order to do this, the certifying party must submit a completed Certification Mark License Agreement by completing the process here. Completing this process signifies that the certifying party meets the requirements outlined in this document and binds the certifying party to follow the Certification Mark Usage Guidelines."*

It is in the nature of open source software that the openness in terms of access to source code is comparatively easy to evaluate: If the source code is not accessible, this will be apparent right away. Some aspects related to hardware as well as legal questions might pose more serious challenges.

About enforcement, OSHWA (2017) as this to say:

> *"To encourage use of the certification and safeguard good-faith users of the certification mark, OSHWA's enforcement policy is designed to make it easy for certifying parties to maintain compliance or withdraw from certification without fine or forfeiture. Persistent violators, however, will be subject to increasing penalties. Note that in many cases, good faith actors can avoid penalty merely by removing the certification mark from their product."*

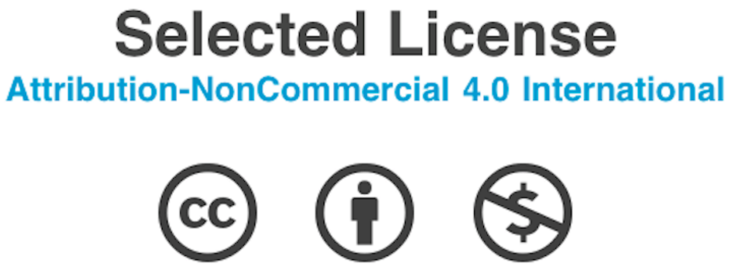
This is a comparatively soft approach based on carrot rather than stick, although the possibility of penalties is pointed out.

Creative Commons content licensing

Creative Commons (CC) provides a content licensing system that—while fully respecting existing copyright frameworks—allows creators to license their content more freely: Others can them to—as per the creator's stated preference—use, distribute, or remix this content in a wider range of ways than the default applicable copyright regime might otherwise allow for.

Creative Commons thus didn't aim to replace any existing legal frameworks, but to complement them. CC licenses work through modules (attribution, non-commercial use, share-alike) that allow for multiple configurations and comparatively granular license-granting: This means more flexibility and freedom for creators as they allow their content to be used far more freely than "all rights reserved". It also reduces friction for those intending to use content by inverting the default from "ask for permission" to "permission granted".

To make this approach as frictionless as possible, Creative Commons implemented a license picker tool that walks creators through a series of questions ("Allow adaptations of your work to be shared?", "Allow commercial uses of your work?") to arrive at a license fitting their preferences. Every license module is represented by a simple icon:



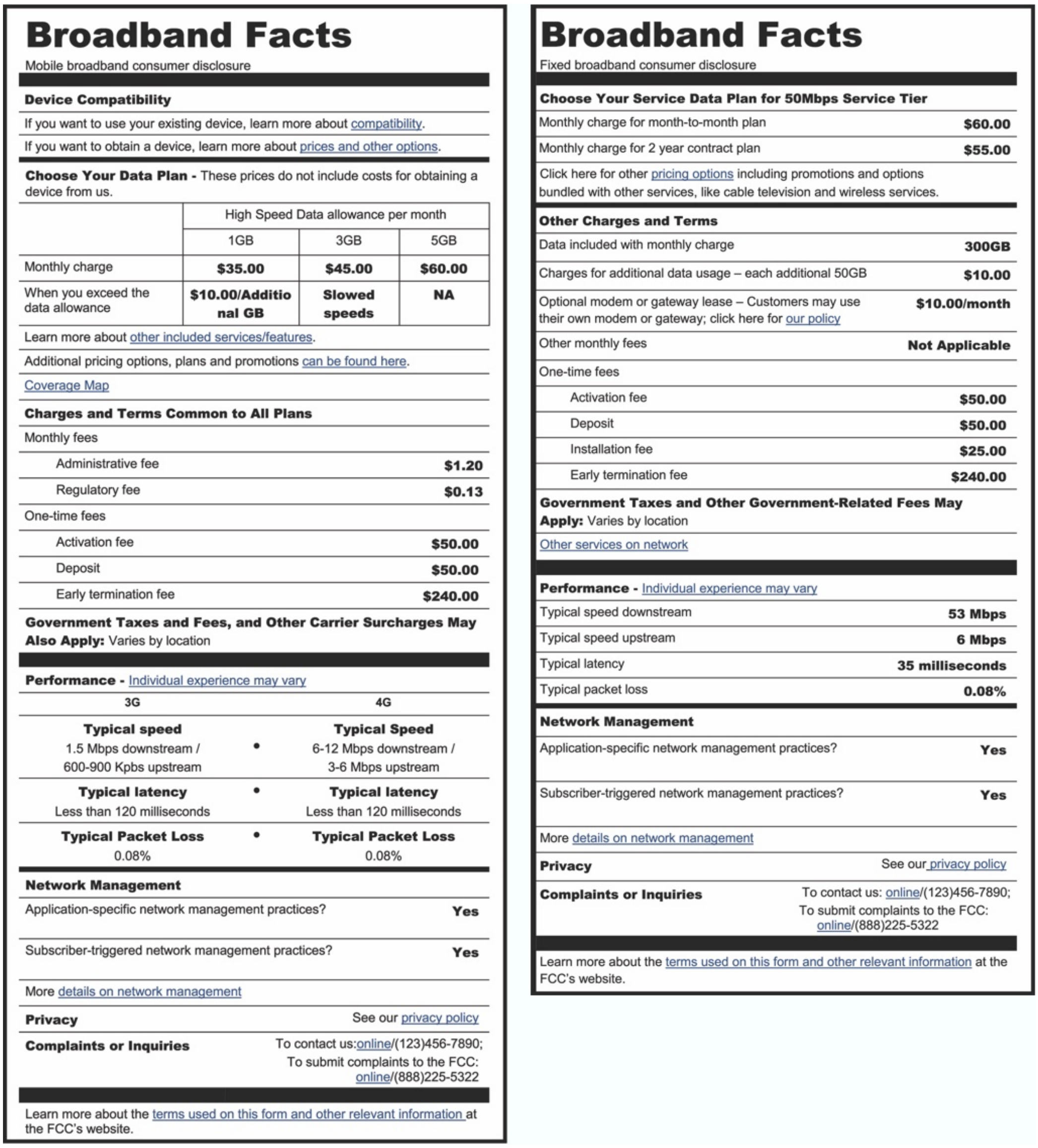
Selected License

Attribution-NonCommercial 4.0 International

An example of the visual representation of a Creative Commons license.

All CC licenses are layered: The base layer is "lawyer-readable", ie. the legal text of the license. This is the legally binding license. A "human-readable" layer explains in layperson terms what is allowed to do with content and what isn't. Finally, the "machine-readable" layer wraps the license in code so developers can use this for digital search, to build APIs, etc.

Creative Commons' approach seems highly relevant for an IoT trustmark: Aiming to complement rather than replace existing frameworks, granting rather than restricting the freedom of producers, making licenses accessible through the lawyer/human/machine readable layers, as well as the simplicity of the license picker all combine into a true benchmark.



Broadband Facts

Mobile broadband consumer disclosure

Device Compatibility

If you want to use your existing device, learn more about compatibility.

If you want to obtain a device, learn more about prices and other options.

Choose Your Data Plan - These prices do not include costs for obtaining a device from us.

	High Speed Data allowance per month		
	1GB	3GB	5GB
Monthly charge	**$35.00**	**$45.00**	**$60.00**
When you exceed the data allowance	**$10.00/Additional GB**	**Slowed speeds**	**NA**

Learn more about other included services/features.

Additional pricing options, plans and promotions can be found here.

Coverage Map

Charges and Terms Common to All Plans

Monthly fees	
Administrative fee	**$1.20**
Regulatory fee	**$0.13**
One-time fees	
Activation fee	**$50.00**
Deposit	**$50.00**
Early termination fee	**$240.00**

Government Taxes and Fees, and Other Carrier Surcharges May Also Apply: Varies by location

Performance - Individual experience may vary

3G		4G
Typical speed 1.5 Mbps downstream / 600-900 Kpbs upstream	•	**Typical Speed** 6-12 Mbps downstream / 3-6 Mbps upstream
Typical latency Less than 120 milliseconds	•	**Typical latency** Less than 120 milliseconds
Typical Packet Loss 0.08%	•	**Typical Packet Loss** 0.08%

Network Management

Application-specific network management practices?	**Yes**
Subscriber-triggered network management practices?	**Yes**

More details on network management

Privacy	See our privacy policy
Complaints or Inquiries	To contact us:online/(123)456-7890; To submit complaints to the FCC: online/(888)225-5322

Learn more about the terms used on this form and other relevant information at the FCC's website.

Broadband Facts

Fixed broadband consumer disclosure

Choose Your Service Data Plan for 50Mbps Service Tier

Monthly charge for month-to-month plan	**$60.00**
Monthly charge for 2 year contract plan	**$55.00**

Click here for other pricing options including promotions and options bundled with other services, like cable television and wireless services.

Other Charges and Terms

Data included with monthly charge	**300GB**
Charges for additional data usage – each additional 50GB	**$10.00**
Optional modem or gateway lease – Customers may use their own modem or gateway; click here for our policy	**$10.00/month**
Other monthly fees	**Not Applicable**
One-time fees	
Activation fee	**$50.00**
Deposit	**$50.00**
Installation fee	**$25.00**
Early termination fee	**$240.00**

Government Taxes and Other Government-Related Fees May Apply: Varies by location

Other services on network

Performance - Individual experience may vary

Typical speed downstream	**53 Mbps**
Typical speed upstream	**6 Mbps**
Typical latency	**35 milliseconds**
Typical packet loss	**0.08%**

Network Management

Application-specific network management practices?	**Yes**
Subscriber-triggered network management practices?	**Yes**

More details on network management

Privacy	See our privacy policy
Complaints or Inquiries	To contact us: online/(123)456-7890; To submit complaints to the FCC: online/(888)225-5322

Learn more about the terms used on this form and other relevant information at the FCC's website.

FCC Broadband Labels. Image: FCC.

Broadband Nutrition Labels

In another attempt to build on the concept of nutrition labels, the FCC introduced consumer labels for broadband internet (which were formally approved in April 2016). The FCC's model is built around voluntary labels for wired and mobile broadband to help consumers make more informed choices. These labels include aspects like pricing details (monthly fees, etc.), data allowances, broadband speed, and network management practices, "namely, precautions providers may take to manage heavy traffic on their networks" (FCC 2016).

Privacy Nutrition Labels

In 2010, Carnegie Mellon University's CyLab Usable Privacy and Security Laboratory (CUPS 2010) proposed Privacy Nutrition Labels (Kelley at al 2010:1): "Many surveys have shown that consumers are concerned about online privacy, yet current mechanisms to present website privacy policies have not been successful. This research addresses the present gap in the communication and understanding of privacy policies, by creating an information design that improves the visual presentation and comprehensibility of privacy policies. Drawing from nutrition, warning, and energy labeling, as well as from the effort towards creating a standardized banking privacy notification, we present our process for constructing and refining a label tuned to privacy."

Emulating successfully implemented consumer trust labels from other areas seems promising, as do CUPS' early research results (Kelley at al 2010:1) that demonstrate that "compared to existing natural language privacy policies, the proposed privacy label allows participants to find information more quickly and accurately, and provides a more enjoyable information seeking experience."

Please note that this example just serves as inspiration: We are not aware of any privacy labels that have worked and/or have been established in the market.

iFixit Reparability Score

iFixit offers a fairly straightforward way of evaluating how reparable consumer devices like smartphones and laptops are: A repairability score of 1-10 stars. This score is calculated following a checklist of factors that makes repairs easier, including the following (iFixit 2017):

- Repair information/diagrams are included with device, or freely available on the internet
- No proprietary screws or self-destructing fasteners are present
- Disassembling the device does not require substantial prying effort
- Battery is easily removable (no strong adhesive, not soldered in place)
- Components are not tightly packed together, making disassembly easy
- Full device disassembly takes less than half an hour
- Discretionary feel after having taken apart the device

Note that some of these aspects are "hard facts" based, making them testable, like "are repair diagrams included". Others are more subjective, relying on the experts' opinions rather than testing ("discretionary feel after having taken apart the device"). This hybrid approach seems sensible especially in areas that are not always testable but "you know it when you see it."

What iFixit's repairability score does not include is the software side of things, which in IoT increasingly becomes a relevant factor for a product's lifecycle.

Consumer protection & safety for electronics: CE certification

For completeness' sake, and because in our research it frequently came up as a point of comparison, let's take a quick look at Europe's CE certification. (Analogs exist around the world, like the FCC Declaration of Conformity in the US.)

The CE marking provides (European Commission 2016:64) "the first indication that the necessary controls can be assumed to have been carried out, before the product in question is placed on the market, in order to ensure its compliance to the legislative requirements. (...) Member States must provide in their national legislation for appropriate measures both to prevent the abuse and misuse of CE marking, and to redress the situation if such abuse or misuse takes place."

The letters "CE" as a trust mark "signify that products sold in the EEA have been assessed to meet high safety, health, and environmental protection requirements. (...) CE marking also supports fair competition by holding all companies accountable to the same rules." (European Commission 2017).

This highlights the dual nature of certification: A protection of minimum quality standards as well as a level playing field for commercial competition. The CE mark was created to protect and inform consumers and businesses alike.

Understandably, the requirements for using the CE mark are strict.

To be allowed to use the CE marking on a product, as the maker of that product you must provide "a technical dossier proving that your product fulfills all the EU-wide requirements. As the product's manufacturer, you bear sole responsibility for declaring conformity with all requirements. (...) For some products, special conformity assessment bodies ('Notified Bodies') must verify that your product meets the specific technical requirements. (...) If your product doesn't need to be verified by an independent body, then it is up to you to check that it complies with the technical requirements. (...) The marking must be visible, legible and indelible." (European Union 2017)

The CE mark is not without criticism: According to security researcher Emma Lilliestam (2017, pers.comm.), the CE mark is a great example to learn what *not* to do: For example, no matter what type of updates (if any) have been made, re-certification is required every 5 years. The pre-approval process of the CE mark is not flawless in practice, and the process is relatively opaque. She sees the EU's General Data Protection Regulation (GDPR) as a more hopeful example. The GDPR's strong stick for failure to comply might turn out to be helpful: Depending on the context, fines can run up to 4% of the company's annual worldwide revenue.

Blue Angel environmental label

Germany's The Blue Angel environmental certification, started in 1978, covers over 80 categories.

In 2016, Fairphone was the first smartphone ever to be certified with the Blue Angel certification (Fairphone 2016). Their Fairphone 2 model received the Blue Angel based on a wide range of criteria including low electromagnetic radiation, product lifetime extension, and active promotion of take-back programs and recyclable design.

This example demonstrates that existing labels could well be integrated as a building block for an IoT trustmark.

Fairtrade

In an interview Solana Larsen (2017, pers.comm.), who has researched Fairtrade in the past, recommends looking into how it works, and especially how it has also failed in the past. The overall model is straightforward: Fairtrade defines indicators and licenses its mark to organizations or products that meet these criteria. But in some circles the organization has lost credibility and is met with charges of hypocrisy, inefficiency and whitewashing. There are competing initiatives and even copycats. On the other hand, Fairtrade has become synonymous with a fairer way of consumption. It might be useful to look at the overall ecosystem rather than only Fairtrade in isolation—especially since IoT looks like a similar type of ecosystem with similar vulnerabilities.

Laundry labels

Researcher Holly Robbins (2017b, pers.comm.) points to laundry labels as a source of inspiration. They are particularly clear in communicating all relevant information visually and clearly, and have been adopted worldwide after being introduced by Ginetex in 1963. According to Robbins, they recognized the need for this type of communications and created a system that the industry adopted readily. Textile care labels solved a concrete problem and were easy enough to implement.

However, she also notes that while laundry labels work on a 1-to-1 ratio of object and labeling ("this piece of clothing requires this temperature of washing"), multi-nodal and complex questions make labeling much harder. That's why for example carbon impact studies (which are as a rule of thumb fact-checkable, but notoriously hard to interpret) often don't offer easy answers. Similar challenges are to be expected for IoT as well. **A trustmark for IoT made for consumers rather than power users, will have to be very accessible and offer actionable advice.**

WHAT TO LABEL & HOW TO VERIFY

Summary:
There are many possible approaches to labeling, most of which revolve around the questions what to label and how verification works. For example, should the label focus on hardware and sensing capabilities, data practices, or security and safety? Should the device itself, the service backend, or the producing organization be evaluated?
In our research we identify five core themes: Good data practices, good security practices, openness, lifecycle management, and establishing if the producing organization is trustworthy.
How verification works has profound impact on the trustmarks' trustworthiness and chance of adoption. We argue for a relatively lightweight approach with a low barrier to entry and little bureaucratic overhead to optimize for widespread adoption.
It's also important that consumers can easily understand a label, and in the context of IoT, that the label represents the state of the device at any given time. To account for software updates and because it seems a great fit with Mozilla's culture, we recommend a dynamic label: A label that links back to deeper information on the open web, i.e. that allows to "view source".

Recommendations:

- *Identify the minimal viable set of characteristics/aspects to label and verify. Given Mozilla's culture and strengths, that means building the trustmark around openness, diversity, good data practices, and an open web approach, aiming to promote internet health and user empowerment.*
- *Adopt a trustmark approach that is built around an alliance of trustworthy organizations and light-weight implementation to keep the barrier to entry low, but allows organizations to demonstrate that they go above and beyond.*
- *The look and feel as well as appropriate mechanisms for the IoT trustmark will have to be developed with designers' input. The trustmark needs to codify complex information in a way that is based on substance, easy to skim, actionable for consumers, and dynamic to account for the potentially ever-changing nature of connected products.*

There are different approaches for labeling. It's essential to determine what to label and how to implement verification and labeling.

The key questions to map out overall approaches are:

- What to label for?
- Who verifies, and how?
- How does the label communicate this information?

Equally, in order to be effective, the IoT trustmark needs a clear focus. There is a range of aspects that an IoT trustmark could potentially tackle to serve consumer protection. This range includes the following focus areas, or combinations thereof:

- Hardware/software capabilities (sensors, update-ability, etc.)
- Data practices (data collection/ processing/ sharing/ protection, privacy by default, applicable legal data & privacy regime, etc.)
- Security practices (security breach disclosures, compliance, security by default, bug bounty programs, etc.)
- Maintenance practices (service guarantees, etc.)
- Sustainability & sourcing (clean, fair, recyclable?)

At the core, transparency is key to help consumers understand and navigate the complexities of networked technologies. This can only work if a label is credible. Or as researcher Holly Robbins (2017, pers.comm.) puts it, we need a standard "to de-murkify the murky things."

What to label for?

Roughly speaking, a trustmark can evaluate inputs, processes, and outputs. In practice, many consumer labels touch on multiple of these areas.

- **Input:** What goes into making a product? In the textile world, Bluesign is a trustmark that demonstrates that an apparel manufacturer uses sustainable, eco-friendly materials. It's primarily an *input*-based trustmark. It also touches on *processes* in that factors like workplace safety also play into the rating.
- **Processes:** How is a product made and distributed? Fairtrade with their strong focus on sustainable farming practices and good labor conditions is a well-known example of a *process*-based trustmark.
- **Outputs:** CE certification confirms that the final product fulfills certain EU quality and safety requirements. As such it's primarily an *output*-based

assessment.

In the literature we reviewed, as well as in many conversations with experts, we encountered a great range of characteristics, principles, or aspects to consider for labels. Below we include a informative selection of examples:

In our interview, Gérald Santucci (2017, pers.comm.) of **the European Commission's DG CONNECT program highlights six key principles that should guide a "Trusted IoT label"** as part of Europe's Digital Single Market strategy. They focus on giving users more control over their data:

- Privacy by design
- Transparency regarding the collection and use of personal data
- Data minimization in terms of its collection and retention
- A right of access for users to the source of their personal data and a right of recovering that data at a reasonable cost
- Authentication and authorization of any connected object before it collects data
- The possibility to turn off and stop an object from collecting data about the data subject, possibly at a cost, and unless this would jeopardize a legitimate public policy

Dries De Roeck (2017, pers.comm.) speaks from a **UX design perspective that focuses on data capture and processing, and he adds organizational aspects** to the list:

- Where is data captured
- Where is data sent, processed
- How is the "network of actors" that processes data organized
- Lifecycle of products

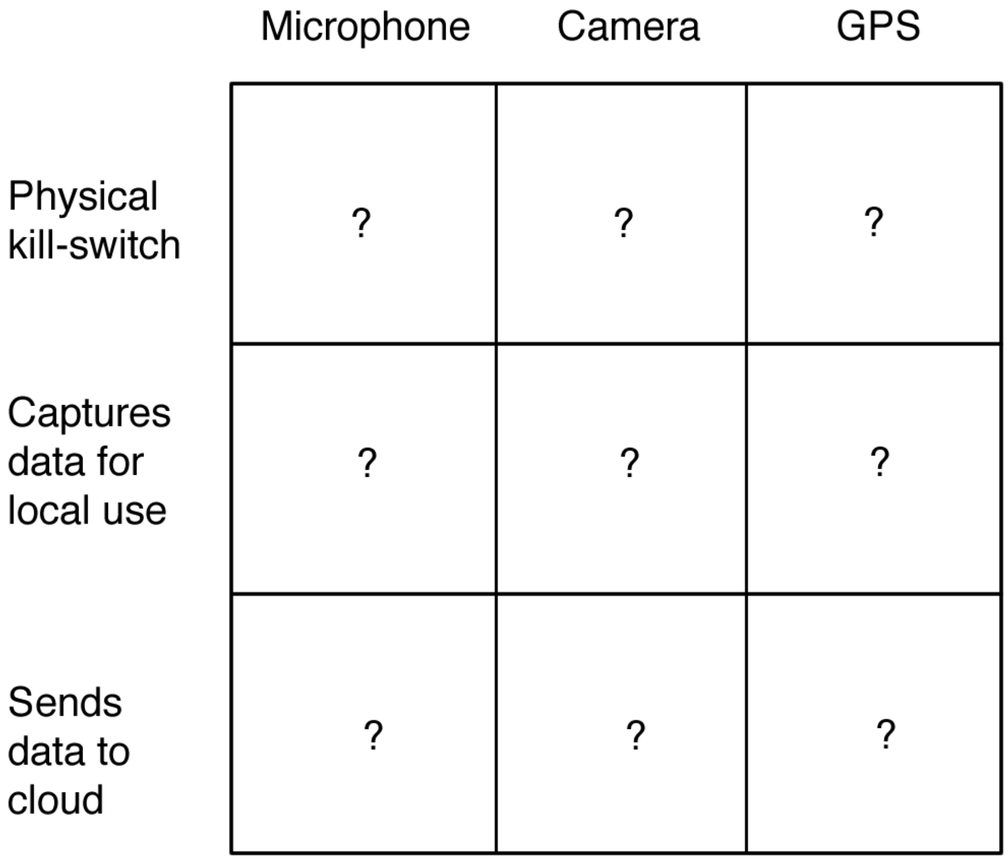
Arguing from a technical background, Yaler founder Thomas Amberg (2017, pers.comm.) identifies three core areas to consider (rather than a concrete list):

- safety
- privacy/security
- ownership (incl. the right to reverse-engineer, to switch clouds, to export data).

David Li (2017, pers.comm.), founder of the Shenzhen Innovation Lab, sees hyperbole and fear-mongering in the discussion of both artificial intelligence and in IoT as undermining consumer trust. According to Li, "IoT labeling is becoming important, especially when we are entering the era of image and voice based interaction where image and voice are captured and send over to the cloud." Li proposes to focus any labeling efforts initially on **three indicators that represent types of sensors, namely microphone, camera and GPS (location)**. He adds three levels of data capture and processing:

- Can the sensor be physically turn off?
- Does the sensor capture the data for local use?
- Does the device send data to the cloud?

This leads to 3x3 matrix:



	Microphone	Camera	GPS
Physical kill-switch	?	?	?
Captures data for local use	?	?	?
Sends data to cloud	?	?	?

Sensor data computation grid based on David Li.

Li sees the base level of trust established by knowing what sensing takes place in IoT devices as essential: "Confidence must be built before the tide turns on the new interactions for the 'fear' of AI" and, by extension, IoT.

Approaching IoT labels from a security perspective, Swedish security expert Emma Lilliestam (2017, pers.comm.) proposes **five categories that a label or security seal should take into account**:

- user communication
- transparency
- data ownership
- operational security
- technical aspects

Lilliestam (2017, pers.comm.) acknowledges that security has the air of being hard, but she asserts it's largely a question of checklists, hygienes, communications, and processes. So process is at the core of the issue. She proposes a reasonably low entry level that might take the following bullet points as a baseline:

- The product cannot be trivially hacked (web application checklist, see OWASP 2015)
- A commitment to handle Vulnerability Disclosure (ISO vulnerability disclosure guidelines, see ISO 2014)
- Update management
- Lifecycle management
- Commitment to the meaning of the GDPR
- Continuously raising the bar as the business matures and old cipher suites get deprecated

The idea of this checklist-based approach and of keeping it comparatively easy is to guarantee that anyone with an interest, time and the right checklists can do this.

Laura James, CTO of UK charity Doteveryone proposes in our interview (2017, pers.comm.) to **take into consideration some core principles (openness, compatibility) but also incorporate already existing trustmarks** if they are relevant.

Other experts frame the individual points slightly differently, but overall the main themes are stable across the board, and most mirror one or several mentioned here that can be sorted under the aspects listed before: *Input*, *processes*, or *outputs*. Some of them focus on the device level, others at the organizational level.

Core themes

We see the following **core themes** pop up over and over again in different forms:

- **Good data practices:** privacy, security, data protection, putting users in control over data capture and processing
- **Good security practices:** checklists, openness, giving users control over fallback mechanisms
- **Openness:** transparency, hackability, open source, compatibility
- **Lifecycle management:** service guarantees, repairability, ease of reverse-engineering and/or hacking, having a strategy in place for end-of-life
- **Establishing that the producing organization is trustworthy** and knows how to handle itself

Considering what kind of labelling approach to take, Laura James (2017, pers.comm.) of Doteveryone proposes a hybrid model: A combination of different types of labels and certifications is most likely going to be most useful. For food, we already see this in practice with complementary labeling systems like ingredients lists, organic and fair trade marks, EU regional provenance labels, and others. Depending on the specific goals of a labeling system, modularity and degrees/ranks within a label are great because they allow for optimizing for different priorities.

As Solana Larsen (Mozilla) backs this up in an interview (2017, pers.comm.), stressing that organic food labels can be especially interesting for IoT, because they also apply to complex and nuanced contexts. She recommends looking at which stages of the production process are targeted and/or certified. Picking the right stages in the process could be essential for the success of an IoT trustmark.

Certification methods

Rosner (2016:10) provides a solid overview of **certification methods** (quoted in full below):

> *There are two methods of certifying that a product, service or organization conforms with requirements that lead to a trustmark: self-assessment and third-party assessment.*

- ***Self-assessment and certification:*** *An organization conducts a review of its own products, services, processes, policies or any other business characteristic and then asserts its conformance to standards, regulations, laws, practices or other external requirements through documentary assertion, legal attestation and/or use of a visible trustmark. Assessment criteria potentially originate from* *within an organization or derive from external sources.*

- ***Third-party assessment and certification:*** *An independent third party assesses an applicant organization and certifies that it conforms with a given set of standards, regulations, laws, practices or other external requirements. This arrangement breaks down into three categories.*

  - *Peer-to-peer: Organizations are assessed by other organizations participating in a certification scheme.*
  - *Independent assessors: Organizations are assessed for compliance by entities specifically tasked with independent assessment. These entities are separate from, but work on behalf of, certifying bodies.*
  - *Certifying body assessment: Assessment is conducted by people or entities who have a direct relationship with a certifying body.*

Drawing on the example of the EU's trustmarks for e-commerce, Gerald Santucci of the European Commission's DG CONNECT reinforces that trustmarks work well for industry and governments alike (Santucci 2017, pers.comm.): "**Trustmarks are by essence a means of self-regulation, which aims at enhancing user trust in online communications.** Therefore, in general, trustmarks can relieve governments of an additional financial burden by making it redundant to regulate some sectors of the Internet and at the same time, they tend to generate significant revenues for governments by boosting e-commerce."

Who verifies? Considerations on trustmark providers

There is a wide range of types of **trustmark providers**. Rosner's outline focuses on the online identity space rather than IoT, but as a structural overview his input (Rosner 2016:9-10, quoted below in full) is valuable for the IoT trust space as well. Trustmarks, according to Rosner, originate from five different sources:

- ***Industry organizations:*** *These are bodies made up of private for-profit and non-profit member organizations. Examples include ETSI, SAFE-BioPharma, the Kantara Initiative and the InCommon Federation.*
- ***Government bodies:*** *Accrediting authorities who are created or led by government institutions. Examples are the NIST Cryptographic Module Validation Program and Germany's EuroPriSe Privacy Seal.*
- ***Public/Private bodies:*** *These are bodies where a clear distinction cannot be drawn between public and private governance of the trustmark certification process. Examples are ISO, IEC and tScheme.*

- ***Private organizations:*** *These are single, private for-profit or nonprofit entities who oversee a trustmark. Examples include the Better Business Bureau, TüvSüd, TRUSTe, and Symantec's Norton checkmark.*
- ***Marks without a traditional accreditation authority:*** *Some marks exist that do not have an accrediting body. Rather, use of the mark is mandated by law for certain product categories, though there is not an accrediting authority in the traditional sense. For example, various European legal instruments specify which products require a CE mark to indicate conformance as well as the acceptable methods of certification (self, third party assessment, etc.); there is no single authority responsible for the CE mark's use.*

Collective marks are a special subset of trademarks. A collective mark indicates that "the goods or services bearing the mark originate from members of a trade association, rather than just one trader" (Intellectual Property Office 2014). The main feature of a collective mark is that it is used as an indication—to the relevant public—that goods or services originate from a member of a particular association. It is a sign of membership that could be implemented, for example, across the members of an industry alliance. For a detailed guideline on how the examination process works in the UK see Intellectual Property Office (2014); for this context suffice it to say that collective marks face a range of grey areas, but the membership-based labeling approach can serve as one source of inspiration for IoT trustmarks.

Even within the same labeling system, there are sometimes significant differences in terms of pricing and implementation. For example, CE certification isn't a *one size fits all* solution:

(1) Depending on where a company chooses to have the certification done, prices might differ wildly. One entrepreneur shared price quotes ranging from €1.500 to €7.500 for CE certification for the same product depending on the certification provider. That's a 5x difference! Anecdotally, CE certification in Europe tends to be much expensive than in Asia.

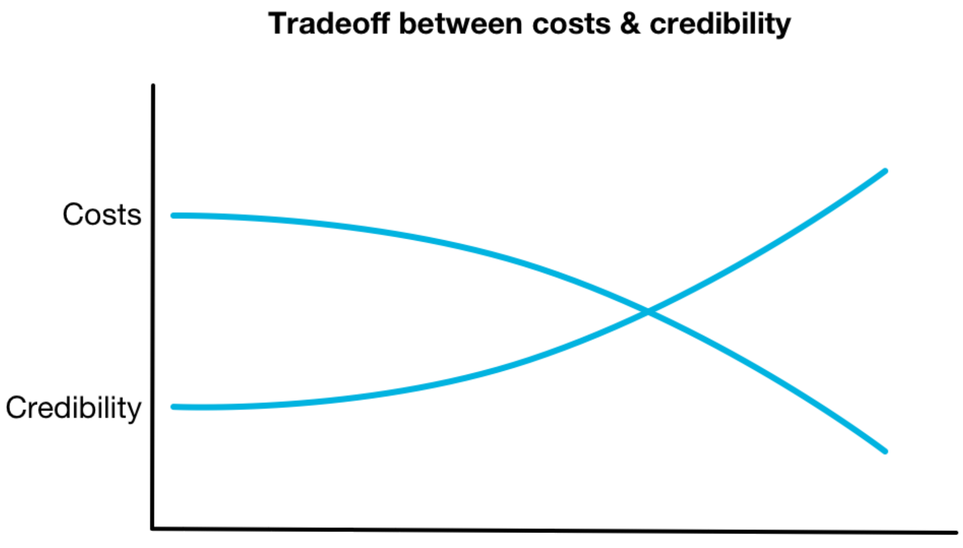
(2) Compatibilities and combinations of standards change complexity and pricing. As Cian O'Flaherty (Managing Director of an Irish IoT company) shares his experience: Price and complexity of CE certification also depends on whether a company requires "CE in line with ENEC and LV directive or need to test EN standards also."
ENEC is a European mark for electric products that is complementary to the mandatory CE mark. It signifies that the product is safe in accordance with the appropriate European directive, like for example LVD (Low Voltage Directive), MD

(Machinery Directive).
These are questions an entrepreneur should be able to answer at the time certification becomes a requirement, but anecdotally that doesn't necessarily mean entrepreneurs can estimate at the outset just how complex and expensive this type of certification might end up being.

Tradeoffs for verification

There is a wide spectrum of types of consumer protection labels or trustmarks. This spectrum goes from unverified self-labeling on one end to third party certification on the other, and many models in between. **The trade-off is between high credibility (i.e. trustworthiness) and high costs (in overhead/bureaucracy)**:

- Self-labeling is comparatively cheap and easy. The downside is that it has inherently lower levels of credibility.
- Third-party certification tends to score higher on credibility. However, it is more expensive and requires a larger bureaucratic overhead, including an organization that does the certification.



Source: The Waving Cat

For every consumer label, there is an inherent tradeoff between costs and credibility.

Painting in broad strokes, a *softer* approach in this context indicates being based on self-assessment, being more bottom-up, and requiring minimal overhead. This would make a softer mark easier to implement than a harder certification, but it has less teeth and hence, lower trustworthiness. It works more through carrot than stick.

A *harder* approach on the other hand indicates a more top-down, centralized approach that requires third-party auditing, potentially even auditing in advance. It has more teeth and hence higher trustworthiness, but it requires more overhead and/or higher costs. It has a bigger stick to punish failures to comply.

The lower barrier to implement the mark, the more uptake can be expected. Inversely, the higher the barrier to implement the mark, the slower the uptake.

In extreme cases, the costs of certification can be prohibitive for smaller organizations. As Solana Larsen (2017, pers.comm.) points out, it's worth considering that a label needs to work for organizations with business interests. Can it offer business opportunities? Is it affordable and practical? In some countries the costs for getting an organic certification can be so high that some farmers actually farm organically but still can't afford to get certified. This scenario should be avoided.

These approaches exist on a spectrum and could come in any number of implementations and configurations. Literature and experts are not unanimous on what might work best for the context of IoT. At the extreme ends of the spectrum, a hard and expensive certification (in terms of money and/or time) risks excluding smaller independent actors altogether whereas a very soft mark might be so watered down as to be essentially meaningless.

Mozilla will have to identify which approach is a better fit for the organization in relation to specific goals (see chapter "Recommendations").

Below we include some considerations from literature and expert interviews on this question. This is not a comprehensive list, but these answers well represent the spectrum of harder vs. softer approaches. The implications here can and should inform any labeling approach: Where does the IoT trustmark fit in?

From *harder* to *softer*, the arguments go as follows:

- Security expert Bruce Schneier suggests a **regulatory approach is unavoidable for IoT security**: "The technical reason these devices are insecure is complicated, but there is a market failure at work. (...) There is no market solution because the insecurity primarily affects other people. (...) The only solution is to regulate."

- A technical VP of a telecoms-backed IoT data platform startup proposes neither fully grass-roots nor fully top-down, but rather **a low barrier to entry combined with a really strong stick**: Easy to adopt but prepared for really harsh fines, not unlike the fine structure as it exists in the GDPR (up tp 4% of a company's revenue). This would make it easy to adopt but hard to mess up.
- Security researcher Emma Lilliestam proposes to take **a voluntary approach for IoT security**. She poses this explicitly as opposed to the centralized, regulation-based approach suggested by Bruce Schneier.
- In order to keep all outputs as applicable as possible, Laura James (Technical Principal at Doteveryone) tends towards a softer "standard". The effort, says James, should **be focused on preventing wide, systemic failure scenarios** rather than countering narrow niche issues.
- Gérald Santucci (DG CONNECT) also backs a softer, industry-led approach, albeit one with strong involvement of the government: "Taking a bird's eye view of the security and cyber security situation, I am inclined to believe that in the IoT scenery **where breath-taking innovations happen at unprecedented speed, 'soft regulation', whether it is self-regulation or co-regulation, is the only reasonable approach.** I think the IoT industry should be encouraged to lead initiatives on designing and managing a Trusted IoT label in a hyper-connected environment, but discussions should be open and transparent. By this, I mean concretely they should involve the Alliance for Internet of Things Innovation (AIOTI), the EU Member States, the European Network Information Security Agency (ENISA) as well as civil society associations such as the European Consumer Voice in Standardization (ANEC) and the European Consumer Organization (BEUC)." (Santucci 2017, pers.comm.)
- Anthropologist and Just Things Foundation board member Holly Robbins draws a comparison to laundry labels and makes the case for a soft approach: The whole industry picked up textile care labels because they **solve a concrete problem and adoption was is easy enough.** They were not formally standardized but found widespread adoption. High levels of accessibility aren't easy to design, but important. Industry best practices need to be able to evolve over time.

Overall, we found that experts have been placing significant amounts of trust in the GDPR not least because of its ability to enforce painful fines. The stick, it seems, is something many experts think we cannot do without in this context.

But how to put this stick to use? How does reporting/auditing and enforcement work? The experts we interviewed didn't have any final answers but gave us some clues:

Belgian product and UX designer Dries de Roeck of Studio Dott believes that it should be possible to enforce a mark bottom-up. Customers, according to de Roeck in a conversation at the London #iotmark event, "should have the opportunity to 'report' issues in the same way, and with the same seriousness, as other organizations can do." He adds that "the entry point should focus on the 'softer' side of things. Ideally there would be a way to go more formal" at the point of enforcement.

In our online survey, founder of IoT platform Yaler Thomas Amberg (2017, pers.comm.) argues for a soft approach "based on publicly verifiable proof, e.g. 'show me the source' with URL links: Device software / firmware / hardware source, BOM, physical designs, API docs, etc." for the product itself as well as the legal, organizational, and policy counterparts that make up the backend, i.e. "service license agreement, privacy policy, security policy, API docs, etc."

The hybrid approach of "soft but verifiable" or rather "self-assessed but verifiable" would open up any source to potential public scrutiny in a similar way that open source software can be peer reviewed and audited. It seems like a good fit for Mozilla's approach and background.

The effectiveness of softer approaches is not easy to gauge. But **anecdotal evidence indicates that a lower barrier to entry can unfold significant positive impact over time**:

For example, at the London #iotmark event (16 June 2017), VP at Bosch Software Innovations Stefan Ferber shared the story of how a document that same group's 2012 event produced on data rights for IoT, the Provisional Declaration of the Open Internet of Things Assembly (Sterling 2012), impacted the corporate strategy of Bosch. In 2012, he helped draft this document alongside other members of this community of IoT experts. He later introduced this, without much fanfare or public visibility, as part of Bosch Software Innovation's strategy and brand guidelines. By 2017, he explained in London, the core principles of said declaration have become part of the foundation of Bosch's IoT activities (Smit 2017).

Two collateral effects Ferber mentioned are worth noting: One, initially there was some internal criticism from the business development teams as the principles laid out in that Open IoT Declaration put heavy restrictions on what would be allowed to do with consumer data without explicit consent. Two, because of these restrictions and principles, which have since then been mirrored in the soon-to-be-implemented European General Data Protection Regulation (GDPR), Bosch's IoT products happened to be ready for the GDPR ahead of time. **Good ethics, this proves once more, are good for business. Something to keep in mind when proposing an IoT trustmark to potential industry partners.**

How to communicate labels?

Typically, consumer labels are printed on, or otherwise affixed to, products and packaging. How to best implement labels for IoT is a question we have seen different proposed answers to, some of which are highlighted in this document.

What makes IoT trustmarks potentially more complicated than other comparable labels is that the underlying issues are complex *and additionally* the labeled products might change with a software update, change in the producing company's ownership, or an updated license agreement. In other words, in **IoT there are more moving parts than in more traditional consumer products.**

While an embossed or printed logo is the most established means to convey the relevant information, maybe **for IoT, a web-based approach than can reflect up-to-date information is more apt**. For example, this could be based on QR codes, scannable via smartphone. There might be other solutions or hybrids.

Translating complicated information into a simple, easy-to-skim visual mark is hard. For example, a mark for environmental impact is very hard to establish because the complexity and density of environmental impact makes it so. The same goes for Terms of Services (ToS) and end user license agreements (EULA), which are hard to read and understand because of complex, dense interactions and implications.

Hence whichever path is chosen for the visual communications, it's key to balance accessibility with density, argues Robbins: A more accessible label is easier to understand, but this comes at the the risk of oversimplification. A label that allows for more density represents complexity better, but at the risk of being inaccessible. The binary character of certification (certified vs. uncertified) brings a particularly high risk that important nuances and depth get lost.

How much complexity can be folded into a label? What degree of liberty is acceptable in its implementation? Striking the right balance between accessibility and density is key for a successful, useful deployment of the IoT trustmark.

The two most well-established flavors of a mark are either binary ("passed the test Y/N") or a traffic light (green/yellow/red for "recommended", "recommended, but conditions apply", "not recommended"). Which model works best for this context is a task to be worked out by a graphic designer in tandem with the group that formalizes the characteristics that will form the basis of the trustmark. Potentially a more unusual and creative solution might be possible if the mark is dynamic. **Optimally, the IoT trustmark should convey at a glance the level of trustworthiness and should allow to retrieve more detailed background and context information.**

Solana Larsen (2017, pers.comm.) points to Stiftung Warentest, Germany's counterpart to Consumer Reports. Their labels are helpful because they are at the same time simple and quick to scan ("Very good", "good", "insufficient", etc.), but also built on substance. Like Consumer Reports', Stiftung Warentest's approach is built on fiercely independent testing, which has thus far been only partially applicable to IoT.

Given the context of Internet of Things, where the information underlying any label will have to be flexible enough to account for future software updates, a dynamic mark seems most promising.

If the mark links to content on the open web, then all relevant information would be available online, publicly accessible. This could be implemented through a QR code or a similar measure. The information displayed on that URL could include the "top level" mark (for example, binary or traffic light) as well as the underlying information, like original sources, comments, etc. In addition to being pragmatic and flexible enough, such **an open web based model seems a good fit both for the overall aim of maximizing transparency as well as Mozilla's culture.**

Note that it isn't just the trustmark itself that needs to be dynamic. As designer Dries de Roeck points out in an interview (2017, pers.comm.) it might not make sense to work with a one-time certification approach but rather the assessment or verification process itself might also need to reflect the potentially changing nature of IoT products. At the very least, it seems that due diligence requires regular re-evaluation. A "best before" approach that indicates how long any given evaluation of the trustmark can be reasonably assumed to hold true seems like a plausible approach (i.e. "This product can be assumed to be stable as-is until 12/2018").

Learning from laundry labels

Fabric care or laundry labels can offer inspiration. They were introduced in the 1960s by Ginetex, the international association for textile care. **Laundry labels were a reaction to new circumstances and newly arisen needs**: At the time, laundry machines were becoming commonplace in homes (Robbins 2017). They have since "practically become an international convention" (ibidem). Laundry labels are not fully standardized and come in a range of flavors, but over time consumers have learned how to interpret them beyond exact instructions (ibidem): "From these recommendations, we develop a sensibility about how certain materials need to be cared for and treated. We can choose what instructions are overzealous and which ones are necessary. We know that one red sock in a white load can have an undesired impact. Here washing technology has become more complex and accessible; and that harmony is being supported by a symbolic language system."

Unlike IoT, laundry labels solve a comparatively simple problem. As Holly Robbins (Just Things Foundation) points out, laundry labels enjoy the luxury of a 1-to-1 ratio of object and labeling, so the relationship is pretty clear and straightforward. Multi-nodal and complex questions make this approach much harder. That is why for example carbon impact studies usually offer no simple answers. For IoT, this complexity poses a challenge.

Yet, **the consumer IoT space has a lot to learn from laundry labels. It, too, creates new circumstances and gives rise to new needs.** It, too, is becoming ever-more complex, and consumers need to develop new sensibilities for how to interpret and apply IoT labels according to their personal preferences and choices.

CURRENT PROPOSALS AND INITIATIVES FOR IOT-RELATED LABELS

Summary:
We examined a wide range of proposals, drafts, and initiatives specifically for the realm of IoT. The landscape today looks relatively scattered, which seems to be representative of the equally scattered landscape of organizations and initiatives with touchpoints to IoT. We highlight some noteworthy initiatives.
We believe that Mozilla can play an instrumental role in convening these scattered initiatives and hosting this global conversation. Mozfest and the Internet Health Report both seem to be natural starting points.
Europe is emerging as a fierce proponent of consumer protection when it comes to digital services, and it has been doubling down on IoT especially. It seems that just like Silicon Valley is a global hotspot for disruptive innovation and for providing the means for global scaling of digital services, and just like Shenzhen, China, is the world's manufacturing epicenter, Europe increasingly claims a global leadership role in consumer, privacy, and data protection.

Recommendations:

- *As Europe emerges as a global leader in consumer, privacy, and data protection, we recommend leveraging Europe's position of strength in this space for the trustmark and related IoT efforts by strengthening partnerships within Europe and building out Mozilla's European footprint.*
- *We recommend aligning the IoT trustmark to be compatible with the six principles for a trusted IoT as laid out by the European Commission in order to give the trustmark extra weight and leverage.*
- *We recommend Mozilla to take an active role in convening the somewhat scattered initiatives and hosting the global conversation around IoT trustmarks—preferably with a focus on Europe with strong input from the global South. Mozfest and the Internet Health Report both seem to be natural starting points.*

Earlier we examined the larger landscape of the types of labels and certifications that form the backdrop to potential new IoT trustmarks. **This chapter looks at drafts, proposals and initiatives that are aimed specifically at the realm of**

IoT.

There are some relatively early drafts of labels for connected products as proposed by product designers. The landscape today looks relatively scattered; a clear winner or dominant proposal does not seem to have emerged yet.

The majority of proposals we see so far, like the ones by design-focused organizations Designswarm and Just Things Foundation, focus on information provided by the producer of IoT products. They assume an incentive in the opportunity to set the product or producer apart from other, less responsible and transparent organizations: A brand exercise of sorts. In other words, they assume an implicit market incentive. Other take a more centralized, enforceable, top-down, or regulatory approach.

European Commission "Trusted IoT" label

Likely the closest approach to the IoT trustmarks discussed throughout this document is the European Commission's Trusted IoT Label initiative.

As part of Europe's push for a Digital Single Market, **the European Commission identifies the need for consumer trust in IoT** and proposes a labeling system (European Commission 2017b): "One of the policy challenges for IoT is to strengthen trust, security as well as end-to-end personal data protection and privacy in the field of IoT. **One possible solution to this challenge could be the development of a 'Trusted IoT' label** (as identified by the European Commission in its 'Communication on ICT Standardisation Priorities'), which will provide consumers of IoT products information about the products' level of security and privacy. Such a 'Trusted IoT' label could be similar to the labelling system used today to indicate energy-efficiency of various appliances across the EU."

In an interview, Gérald Santucci who was at the time in charge of DG CONNECT's IoT unit, provides more background as well as the categories the EC had been considering (Santucci 2017, pers.comm., highlights by the editor):
"Since 2012, and more insistently in the context of the Digital Single Market strategy, the European Commission has shown its commitment to informing end-users on the quality of any IoT device or IoT service in terms of the privacy and security safeguards it provides. This was how the idea of a 'Trusted IoT label' to ensure transparency emerged. **This label would rely on six key principles: privacy-by-design, transparency** regarding the collection and use of personal data, **data minimization** in terms of its collection and retention, entitlement of the

users to a **right of access** to the source of their personal data and a **right of recovering that data** at a reasonable cost, authentication and authorization of any connected object before it collects data, and finally the **possibility to turn off and stop an object from collecting data** about the data subject, possibly at a cost, and unless this would jeopardize a legitimate public policy."

EC Trusted IoT initiative (proposed key principles)
Privacy-by-design
Transparency of data collection & use
Data minimization
Right of access
Right of recovery
Possibility to turn off data collection

Europe is emerging as a fierce proponent of consumer protection when it comes to digital services, and has been doubling down on IoT especially. With the General Data Protection Regulation (GDPR) about to go into effect in 2018 and the "Trusted IoT" initiative, we see ever-stronger efforts to protect European consumers from commercial data exploitation.

It seems that just like Silicon Valley is a global hotspot for disruptive innovation and for providing the means for global scaling of digital services, and like Shenzhen, China, is the world's manufacturing epicenter, Europe increasingly claims a global leadership role in consumer, privacy, and data protection.

Security & safety focused initiatives

Kleinhans (2016:10) provides an overview of existing initiatives in European and the US that focus on security and safety.

Translating from his original writing in German: "Regarding minimum standards for IoT devices, there currently exist different initiatives in Europe and the United States: The Open Web Application Security Project (OWASP) has been working on non-binding IoT security guidelines. The industry-oriented Online Trust Alliance published an IoT trust framework. Also, the global association of GSM mobile providers (GSMA) published security recommendations for the internet of things. The US Chamber of Commerce had a consultation process for IoT security and the role of government, and is now working on further workshops to the central challenges. Furthermore the European Commission is working on 'Trusted IoT Labels' and is considering in workshop what appropriate minimum standards would have to look like. Last but not least, BSI [editor's note: Bundesamt für Sicherheit in der Informationstechnik, the German Federal Office for Information Security] has done important work with its test concept for broadband routers that would be partially applicable to IoT devices."

Kleinhans (2016:11) provides some analysis as to how this might be applied to IoT labeling [translated from German]: "An IoT label would build on such a minimum standard. First, one could require that, analog to European CE marks, IoT devices would only be allowed to operate in Europe if they carry such a label and thereby prove that they fulfill this minimum standard. Second, such a label would offer manufacturers the opportunity to differentiate themselves from their competition through IT security, because they now had the chance to demonstrate their customers that the product delivers on its promise. Third, it would be easier to enforce liabilities for a product because the manufacturer committed to a label that represents a minimum standard. Hence both approaches, product liability and minimum standard including an IoT label, would complement and strengthen each other."

In fact, at the time of writing—as part of a larger cyber security initiative—the German federal government is evaluating the introduction an IT security seal for IoT, or rather on applying an effort for IT security seal to IoT (Deutscher Bundestag 2017).

In the United Kingdom, at the time of writing, BSI (a business standards company and Notified Body that also offers CE certification, among other things) was developing an "IoT Secured BSI Kitemark", as "a new service being developed for manufacturers to demonstrate that they have measures in place to ensure the security and safety of their products when connected to the Internet." (BSI 2017)

Open Web Application Security Project (OWASP)

Focusing primarily on security aspects, the US-based Open Web Application Security Project proposes IoT security guidelines for manufacturers. This guidance is deliberately structural in nature, "giving builders of products a basic set of guidelines to consider from their perspective. This is not a comprehensive list of considerations, and should not be treated as such, but ensuring that these fundamentals are covered will greatly improve the security of any IoT product." (Open Web Application Security Project 2016)

Online Trust Alliance (OTA)

The Online Trust Alliance (2017) published a list of 37 principles that might serve as "a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs. It is the goal of OTA to post and highlight devices which meet these standards to help consumers, as well as the public and private sectors, make informed purchasing decisions." The 37 principles outlined in this "IoT Trust Framework®" are clustered into four key areas, namely (1) security principles, (2) user access & credentials, (3) privacy, disclosures & transparency, and (4) notifications & related best practices.

> *IoT challenges frequently are not just of a technical nature but also have organizational, legal, and procedural implications.*

This clustering reflects well the type and range of challenges involved in IoT products and services, which frequently are not just of a technical nature but also have organizational, legal, and procedural implications.

It must be noted that by definition these principles are fairly top-level and abstract. Principle 1 (security), for example, opens with urging developers to "ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards." While undoubtedly true, for security questions the devil tends to be in the details. That said, if all connected products and services even just consistently applied encryption at all, IoT (and much of the Web) would be in much better shape.

Security Nutrition Labels

Nutrition labels are a popular comparison for any type of consumer labeling, and IoT is no exception. In a Fortune interview (Hackett 2017), chair of the RSA security conference Hugh Thompson makes the case for security nutrition labels for connected products. Hackett expands on Thompson's proposal: "The difference being that these connected gadget labels would reveal the sensory powers of the devices in question, rather than caloric and sodium content. Can the gadget record audio? Can it capture video? Can it sense light, motion, heat, moisture?"

This is an approach also proposed in conversations with David Li of the Shenzhen Open Innovation Lab (SZOIL). Developers (referring to the company that orders the manufacturing) of connected products should include labels on hardware capabilities—especially sensors—on their products.

The US Department of Commerce's National Institute of Standards and Technologies adopts this approach (NIST 2016:29-30):

"The ultimate solution is that all devices should be 'secure to market.' But until then companies must provide information about each product sufficient to enable consumers to make informed and smart security-related decisions about the technology products and services they acquire. Such disclosures should incentivize technology product vendors and service providers to give consumers clear, accurate, and comprehensive information about their cybersecurity and privacy capabilities and practices. A partial goal of this effort should be to make cybersecurity a market differentiator."

Concretely, they outline this as Action Item 3.1.1 (NISt 2016:30): "To improve consumers' purchasing decisions, an independent organization should develop the equivalent of a cybersecurity "nutritional label" for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand."

IoT Security Guidelines

There are a number of security-focused guidelines, toolkits, and checklists that apply to IoT, or could be applied to IoT. A complete list of these guidelines would be redundant, so here are just a few examples that specifically focus on IoT.

The GSMA IoT Security Guidelines (GSMA 2016) promote "a methodology for developing secure IoT services to ensure security best practices are implemented throughout the life cycle of the service" and offers a toolkit for IoT security self-assessment.

The Open Web Application Security Project's IoT Security Guidance (OWASP 2016)—available for manufacturers, developers, and consumers—is a long list of high-level "security considerations." While the list of advice certainly is useful ("Ensure that any web interface in the product has an account lockout mechanism"), the list of categories of security concerns is particularly worth reading. It is, in a nutshell, a great overview of the wide range of security concerns that apply to connected products:

1. Insecure web interface
2. Insufficient authentication/authorization
3. Insecure network services
4. Lack of transport encryption
5. Privacy concerns

6. Insecure cloud interface
7. Insecure mobile interface
8. Insufficient security configurability
9. Insecure software/firmware
10. Poor physical security

This, of course, is just the security lens. Once we widen the scope to include other potentially problematic aspects like data protection, data practices, privacy, security UX, business models, and all the others, the list grows profoundly.

IoT labels proposed by designers of IoT products

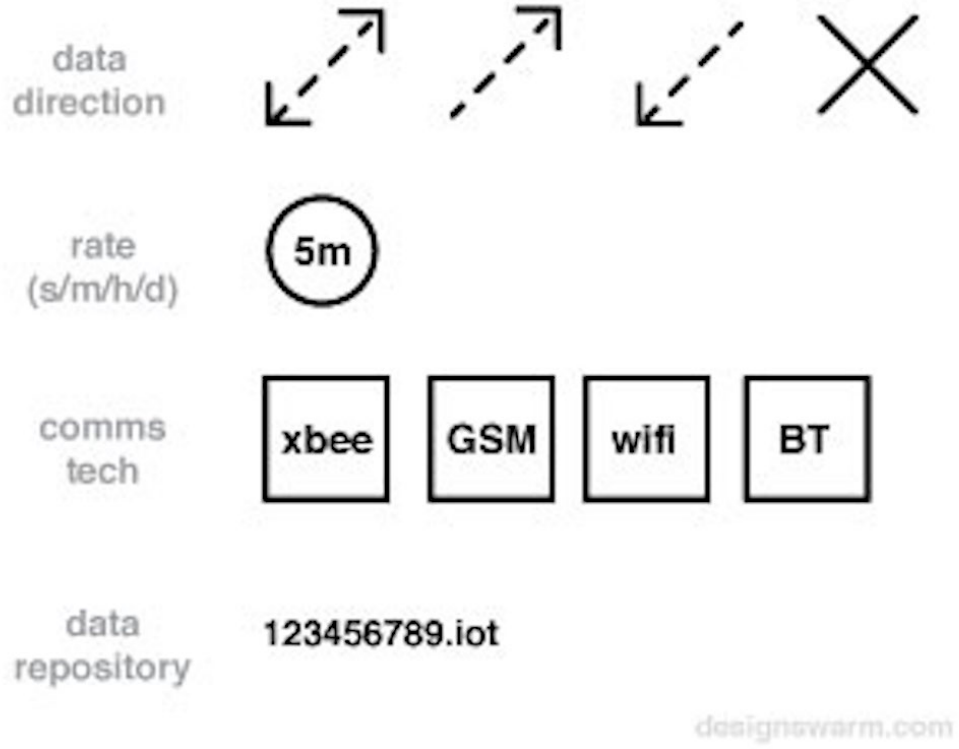
Several groups of designers involved in creating IoT products have proposed labeling systems for connected products.

These come from deep experience and workflows of designers of consumer IoT products, and represent that particular perspective. In particular, the examples included here focus on consumer-readability.

Designswarm: What does it do? A proposal for connected product labelling

On the occasion of a conference presentation in Hamburg in 2015, Alexandra Deschamps-Sonsino—founder of both IoT design and strategy consultancy and IoT startup Good Night Lamp—proposed a labeling system for IoT products.

She explains: "Companies should be sharing information on a basic level such as whether data is being sent to the cloud and collected or not. At what rate that data is being sent and using what type of communications technology." (Deschamps-Sonsino 2015)



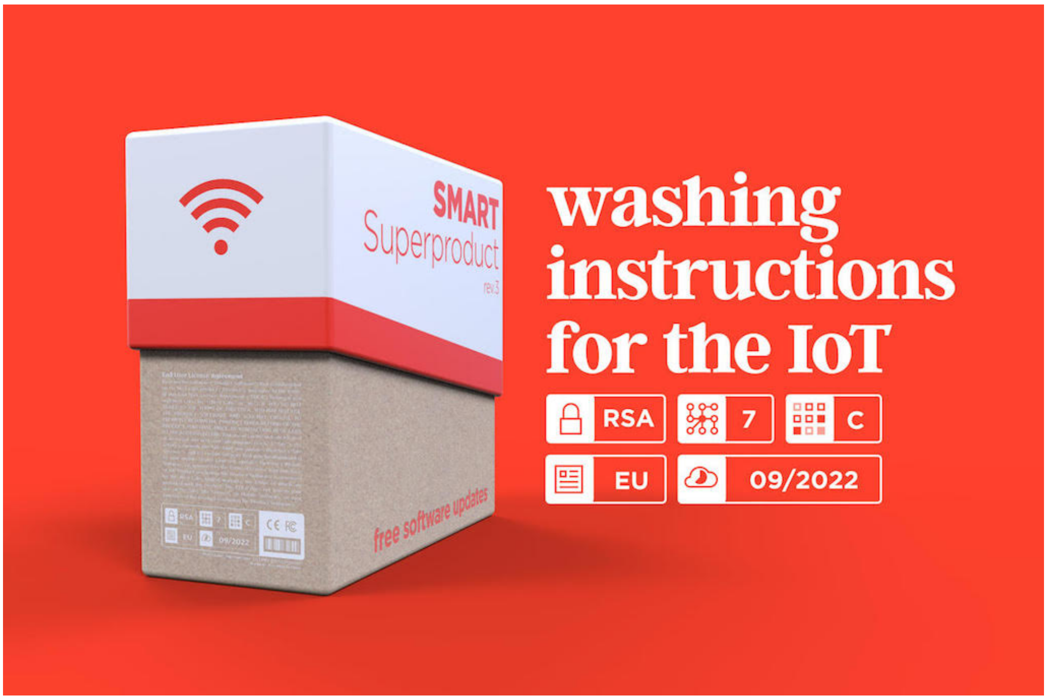
Designswarm: A proposal for connected product labelling

For Deschamps-Sonsino this is a first building block for a larger shift of data transparency and mobility (2015): "Additionally I think we should all have access to the data we share with companies in a human-readable format. We can then decide to archive the data elsewhere or delete it. This is regardless of our technology literacy and mobile phone access. You should be able to pick up an object and see things about it online that relate to you."

Beyond.io: Washing instructions for the IoT

For Dutch Design Week, Belgian experience design studio Beyond.io was commissioned by Just Things Foundation as part of an exhibition called "An Internet of Things We Can Be Proud of!" to create a label concept for IoT.

Their "washing instructions for the IoT" (Beyond.io 2016) focus on data practices and especially data sharing of a fictional smart product:

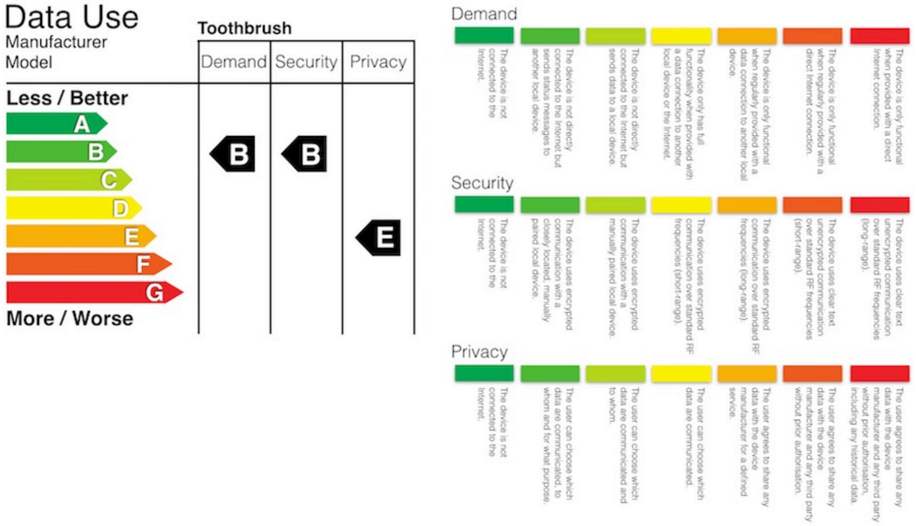


Washing instructions for the IoT by Beyond.io, commissioned by Just Things Foundation

The labels include the type of encryption used (RSA), number of companies are involved in the product and data is shared with (7), overall trustworthiness level (C), the legal framework that governs data protection of this product (EU) and how long the company would guarantee to support the software and servers necessary to keep the product running.

Adryan: Data Use Labels

Coming from a technical background, Dr. Boris Adryan drafted Data Use Labels to "highlight the three pain points of connected consumer products: Data Demand, Security and Privacy." (Adryan 2015)



Demand

The device is not connected to the Internet.

The device is not directly connected to the Internet but sends status messages to another local device.

The device is not directly connected to the Internet but sends data to a local device.

The device only has full functionality when provided with a data connection to another local device or the Internet.

The device is only functional when regularly provided with a data connection to another local device.

The device is only functional when regularly provided with a direct Internet connection.

The device is only functional when provided with a direct Internet connection.

Security

The device is not connected to the Internet.

The device uses encrypted communication with a closely located, manually paired local device.

The device uses encrypted communication with a manually paired local device.

The device uses encrypted communication over standard RF frequencies (short-range).

The device uses encrypted communication over standard RF frequencies (long-range).

The device uses clear text unencrypted communication over standard RF frequencies (short-range).

The device uses clear text unencrypted communication over standard RF frequencies (long-range).

Privacy

The device is not connected to the Internet.

The user can choose which data are communicated, to whom and for what purpose.

The user can choose which data are communicated and to whom.

The user can choose which data are communicated.

The user agrees to share any data with the device manufacturer for a defined service.

The user agrees to share any data with the device manufacturer and any third party without prior authorisation.

The user agrees to share any data with the device manufacturer and any third party without prior authorisation, including any historical data.

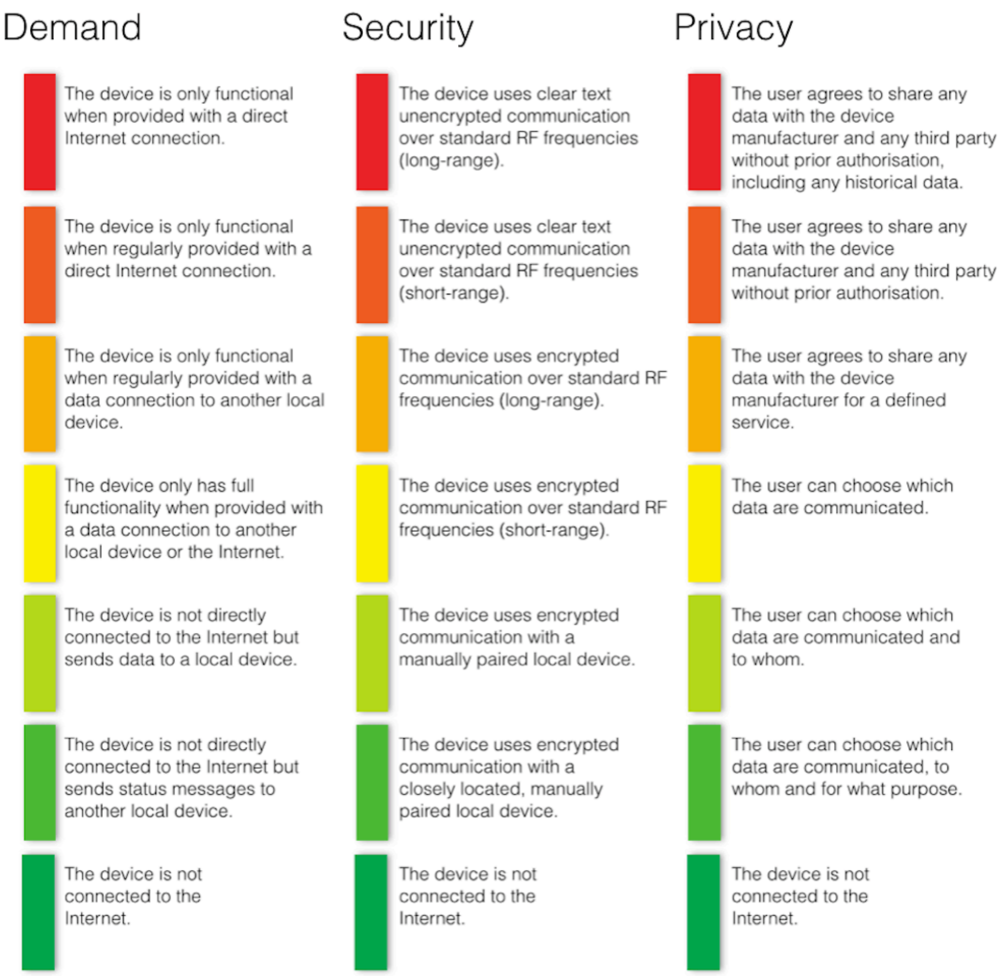
Data Use label, draft by Dr. Boris Adryan (2015)

His explanation of these three pain points is worth quoting in full:

- ***Demand.*** *Is your device connected at all? Is it a data hog? Is it rendered totally useless without a functioning Internet connection or is it happy to occasionally talk to a local hub? In other words, does your web-connected thermostat still work when your communication line is down, or does with the Internet also your heating system fail?*
- ***Security.*** *This covers how save your device is and how resilient to outside attacks. We don't need to have this discussion if your device is not connected, but different communication technologies come with different risks. And while I'm probably (still somewhat) comfortable that my connected kitchen sink sends an unencrypted "Clean me!" via Xbee, there are certain domains in which I would hope for a physical range limit, proper authentication and encryption. The latter two become especially relevant with new technologies such as low-power wide-range networks, where the receiver of a radio message may be many kilometers away, with plenty of opportunities for an attacker to skim your*

information. (Needless to say that also your more locally restricted WiFi should be appropriately protected).

- ***Privacy.*** *Assume your data has safely landed in the hands of your device manufacturer. Are you giving your rights away? In an ideal world, you'd be in complete control over which data is shared with whom and what for. Some data I'd share, but only if it's aggregated with other people's data so the individual data point cannot be traced back to me. On the opposite end of the spectrum, many of us don't even know (or care, or feel helpless) with what major player data companies are doing with our information. Do you want to live in a world where you rather not use a device for fear that the manufacturer sells it and your insurance premium might go up?*



Demand	Security	Privacy
The device is only functional when provided with a direct Internet connection.	The device uses clear text unencrypted communication over standard RF frequencies (long-range).	The user agrees to share any data with the device manufacturer and any third party without prior authorisation, including any historical data.
The device is only functional when regularly provided with a direct Internet connection.	The device uses clear text unencrypted communication over standard RF frequencies (short-range).	The user agrees to share any data with the device manufacturer and any third party without prior authorisation.
The device is only functional when regularly provided with a data connection to another local device.	The device uses encrypted communication over standard RF frequencies (long-range).	The user agrees to share any data with the device manufacturer for a defined service.
The device only has full functionality when provided with a data connection to another local device or the Internet.	The device uses encrypted communication over standard RF frequencies (short-range).	The user can choose which data are communicated.
The device is not directly connected to the Internet but sends data to a local device.	The device uses encrypted communication with a manually paired local device.	The user can choose which data are communicated and to whom.
The device is not directly connected to the Internet but sends status messages to another local device.	The device uses encrypted communication with a closely located, manually paired local device.	The user can choose which data are communicated, to whom and for what purpose.
The device is not connected to the Internet.	The device is not connected to the Internet.	The device is not connected to the Internet.

Data Use label, draft by Dr. Boris Adryan (2015)

This system, while only drafted as his contribution to an online conversation around labeling opportunities, goes fairly deep while staying accessible and straightforward to apply.

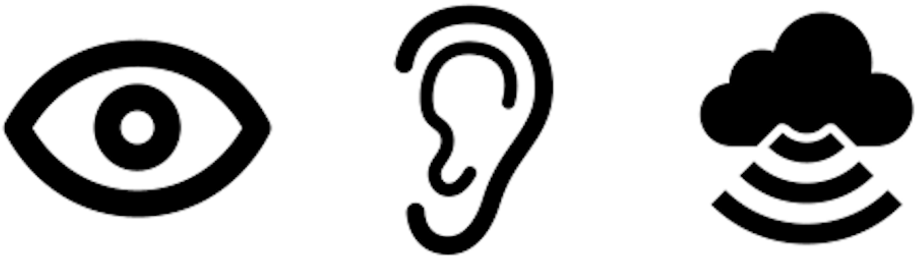
AvantGadget: IoT Identity Brand Guide

AvantGadget's IoT Identity Brand Guide (AvantGadget 2017) appears to be a draft-stage exploration on how to visually communicate certain aspects of IoT devices and services. Described as "an open source project to help the IoT community" this simple system of labels focuses on categorization ("drones, sound, gadgets", etc.), as well as on types of connectivity a device is capable of (Bluetooth, Z-wave, Wifi). The website was not fully functional at the time we accessed it.

Thorne & Bihr: IoT icons

In "Understanding the Connected Home" (Bihr & Thorne 2016), the authors explore so-called interaction layers of connected homes. Borrowing from the three-tiered Creative Commons licensing structure they differentiate between (1) human-readable, (2) machine-readable, and (3) new layers, i.e. environment-readable.

Focusing on the human-readable layer, i.e. consumer-grade labeling, they propose a set of icons that indicate what is collecting data, what is transmitting data, what is analyzing data. "Does this thing listen or watch? Does it share data to the cloud?" (Bihr & Thorne 2016)



Bihr & Thorne: A set of icons that indicate what is collecting data, what is transmitting data, what is analyzing data.

This approach could be interpreted in different ways:

1. Current status: Is this device currently recording video or audio, or transmitting data?
2. Capabilities: Is this device equipped—through software, hardware, or a combination of both— to record video or audio, or transmit data?

3. Potential: Could this device be updated remotely (through a software update) to become capable of recording video or audio, or transmit data?

For consumers, this would make a big difference. It also decides at which production step the labeling would have to be decided: Is it at the hardware manufacturer level, the level of the company that designs the connected service, or the consumer-facing company level? Or a combination of all three? The lines are often blurry.

Hardware capability labels

In conversations about potentials for IoT labels, David Li of the Shenzhen Open Innovation Lab (SZOIL) has been proposing a set of labels that would indicate a base level of what type of sensing the hardware of a product is capable of.

This system, which would be comparatively easy to implement at the manufacturer level, would indicate if a device has a microphone, a camera, or a motion detector for example.

This approach is fairly basic, but it does offer a solution to an inherent characteristic of IoT products. Software updates that might enable new features, and the fact that sometimes due to economies of scale chipsets with additional sensors are cheaper to source than those without them. For example, if a fitness tracker with a built-in motion sensor also had an unused microphone built in (because it was cheaper to source for the producer), this microphone could potentially be activated later through a software update or a security breach. Consumers would not reasonably expect a microphone to be part of a fitness tracker, so a label of the hardware capabilities might clarify by increasing transparency.

Other initiatives, manifestos, declarations, and tools

#iotmark (#iotmark 2017) is a community-driven IoT certification initiative initiated at a London event in June 2017 by Alexandra Deschamps-Sonsino and Usman Haque. This initiative builds on the success of the 2012 Open IoT Declaration (initiated by the same group, see Sterling 2012). At the time of writing, the group convened there still had some foundational decisions to make, but multiple working groups are actively figuring out proposals on how to tackle the numerous challenges in this space.

For the #iotmark initiative, co-founder Deschamps-Sonsino (2017, pers.comm.) explains in an interview that they are considering to aim to separate two core aspects for a certification: The underlying principles and the certification mark that requires licensing. One provides the philosophical underpinnings, the other communicates and confirms compliance to the outside world.

The goal of the initiative is ambitious, the approach is one focused on interoperability (#iotmark 2017): "We would like to push the current and upcoming (GDPR) interpretations of consumer rights in the unregulated space of connected products (or internet of things). We consider the current technical standards that address this space too narrow in their focus and not aiming at the protection of consumers."

Which form the evaluation of compliance would work was not decided at the time of finishing this report (early Sept 2017). The most likely scenario was to ask for documentation to be provided rather than testing; if testing was needed it would most likely be subcontracted through a separate provider of testing services. This might be required particularly if security aspects turned out to be at a core element of the certification. A first public launch of the mark is aimed at end-of-year 2017.

(Full disclosure: The author was part of the group and has been involved in the governance working group.)

Just Things' IoT Design Manifesto (Just Things 2015), a collaborative effort by a group of predominantly Dutch designers launched at ThingsCon Berlin 2015, outlines 10 strategies presented as a checklist for creating responsible IoT products:

1. We don't believe the hype
2. We design useful things
3. We aim for the win-win-win
4. We keep everyone and everything secure
5. We build and promote a culture of privacy
6. We are deliberate about what data we collect
7. We make the parties associated with an IoT product explicit
8. We empower users to be the masters of their own domain
9. We design things for their lifetime
10. In the end, we are human beings

Projects by IF's Data Licenses is a prototype licensing tool (Project by IF 2016a) for user-generated data. Maybe best understood as an artistic provocation, it lets users choose if and how to share user-generated data types including location, household, and biometric, and trade them on a data market place. This is the closest we have seen so far to a Creative Commons style license picker for IoT-related data.

In their **Proclamation of User Rights** Crowdsupply (2017) offers a list of user rights producers of consumer products commit to. This aims to vet producers and products "not only for originality, usefulness, and feasibility, but also for their commitment to user rights. Below are the rights our users can expect and our creators agree to uphold."

In food labeling, every time the content changes, the packaging (and hence the label) changes. In IoT products, that's not necessarily correct. We recommend considering creative approaches to tackle this challenge, for example through a **"best before" date** that makes transparent for how long an IoT device might be "stable" in its current incarnation.

POTENTIAL COLLABORATORS

Summary:
We identified a number of promising emerging proposals and initiatives, as well as potential collaborators and allies, that we highlight: The #iotmark initiative, Doteveryone, Projects by IF (all UK), Just Things (Netherlands), Consumers International,The Digital Standard, and ThingsCon (all global) are some organizations and initiatives we recommend working with.

Recommendations:

- *We recommend a highly collaborative approach for the IoT trustmark and beyond. Concretely, we recommend reaching out to potential collaborators and discuss how to mutually support each other. Depending on the partner, this could mean joint projects, amplifying ongoing work, or supporting existing initiatives financially or through promotion, commissioning work, or other creative uses of existing resources.*
- *We recommend working with the #iotmark initiative to align the IoT trustmark and the #iotmark initiative's certifications, both of which take slightly different approaches but appear compatible in a layered approach.*
- *We recommend exploring a commission for the "Lint for good data practices" suggested by David Ascher and scaling it under Mozilla's roof to a global open source tool.*
- *Insurances as well as city & national governments could be powerful partners for adopting and leveraging the IoT trustmark.*

#iotmark London

#iotmark (#iotmark 2017) is a community-driven IoT certification initiative initiated at a London event in June 2017 by Alexandra Deschamps-Sonsino and Usman Haque. This initiative builds on the success of the 2012 Open IoT Declaration (initiated by the same group, see Sterling 2012). at the time of finishing this report (early Sept 2017), the group still had some foundational decisions to make, but multiple working groups are actively figuring out proposals on how to tackle the numerous challenges in this space.

Judging by its early days, #iotmark initiative appears promising and worth exploring as a collaborator. The energy and commitment apparent in this broadly interdisciplinary group shows wide-ranging interest and expertise that might well lead to solid results. As outlined before, we expect that their certification approach will be fully compatible as another trust layer that complements the IoT trustmark.

(Full disclosure: The author was part of the foundational group and has been involved in the governance working group since.)

Doteveryone

Founded by Martha Fox-Lane, the UK's digital literacy charity Doteveryone has been doing tremendous research around responsible and trustworthy tech and shared some of their early thinking around what it means for digital technology to be responsible. Since their launch a few years ago, they have been consistently ramping up efforts to campaign both for consumers and leadership circles on digital literacy. Their work focuses on the Internet and digital technology more generally, but has plenty of touchpoints with IoT.

ThingsCon

ThingsCon is a global non-profit community of IoT practitioners with the mission to foster the creation of a responsible and human-centric IoT. They have been working on related topics with their network as well as allies for years, both in advocacy and through reports like the recent *The State of Responsible Internet of Things* (ThingsCon 2017) and *View Source: Shenzhen* (Bihr 2017b). Their extended community would make for strong collaborators.

(Full disclosure: The author co-founded ThingsCon in 2014 and is the chair of the board of ThingsCon e.V.)

Just Things

The Dutch Just Things foundation aims to increase the awareness about ethical dilemmas in the development of internet connected products and services. In 2015, the group launched the IoT Design Manifesto which outlines 10 strategies for creating responsible IoT products, and which gathered a lot of attention across the industry. Now they build on these principles aiming to transform them into actionable standards for a broader audience to work with.

Consumers International: Policy actions

Consumers International—with support of Projects By IF—published a list of "policy actions that support consumer protection and empowerment in the digital age". It touches upon a wide range of areas including data protection, security and more

(Consumers International 2016).

As part of this set of proposed policy actions they specifically include certification for "products that meet certain requirements of transparency, privacy and security are awarded a certification mark so that people know they can trust the product."

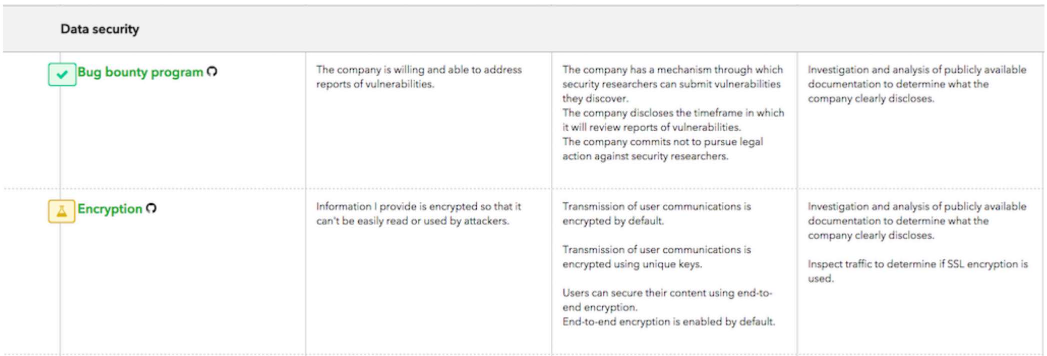
The Digital Standard

The Digital Standard is a collective effort by several consumer rights and digital rights groups, led by Consumer Reports, Disconnect, Ranking Digital Rights, and The Cyber Independent Testing Lab, with assistance from Aspiration Tech.

The group describes the Digital Standard as "an ambitious, open, and collaborative effort to create a digital privacy and security standard to help guide the future design of consumer software, digital platforms and services, and Internet-connected products." (The Digital Standard 2017)

The project description also highlights one of the core challenges of connected services: It is both strength and weakness of IoT products that they can be software updated—and potentially a software update can add, change, or take away a feature. This makes it inherently hard for consumer organizations to test and evaluate connected products.

The core of the Digital Standard consists of a series of tests, criteria, indicators, and procedures to tackle these challenges.



Data security			
✓ Bug bounty program	The company is willing and able to address reports of vulnerabilities.	The company has a mechanism through which security researchers can submit vulnerabilities they discover. The company discloses the timeframe in which it will review reports of vulnerabilities. The company commits not to pursue legal action against security researchers.	Investigation and analysis of publicly available documentation to determine what the company clearly discloses.
⚠ Encryption	Information I provide is encrypted so that it can't be easily read or used by attackers.	Transmission of user communications is encrypted by default. Transmission of user communications is encrypted using unique keys. Users can secure their content using end-to-end encryption. End-to-end encryption is enabled by default.	Investigation and analysis of publicly available documentation to determine what the company clearly discloses. Inspect traffic to determine if SSL encryption is used.

The Digital Standard identifies a range of characteristics for IoT products and how to test them. (Image: Screenshot of thedigitalstandard.org/the-standard)

The Digital Standard is a collaborative and open project. The criteria and tests are on Github for the public to view and comment.

This open approach might be key to solving the challenges of a complex, fast moving field like IoT: It allows for emergence, and input by many different and diverse stakeholders.

Transparency Mark & QR codes

In an early stage exploration, UK design and research studio Projects By IF proposed a transparency mark (Bourke 2016): "a digital proof a bit like a certificate of transparency or SSL. It's a symbol that can be applied to packaging in shops or on websites through which consumers can find out more about a product. The mark is a gateway for finding out the hidden information behind a product. Consumers can scan the symbol and see information about the software that runs on a device, including the terms and conditions and information about how data is used on it."

Especially the idea of using a scannable QR code rather than "hard", unchangeable printed or embossed icons is certainly worth exploring given the inherent characteristics of IoT products, which could change with the next software update.

In many regions—including North America and Europe—QR codes are not widely used by consumers. However, this isn't true globally. In many Asian countries, especially China, QR codes are used ubiquitously. It's not unthinkable that user behavior in the West might also change over time given the right tools and incentives.

Data Permissions

UK design and research studio Projects By IF launched a catalog of design patterns for personal data sharing (Projects by IF 2016), maintained as a living document on Github. These design patterns (ranging from controlling access to data licensing to giving consent and voice verification) can provide inspiration and guidance for consumer-relevant data practices and potential labels to convey these practices.

Tracking provenance

With a focus on supply chain transparency and traceability, UK startup Provenance (website) offers manufacturers the tools to show consumers how they manufacture: Provenance helps them open up their products' supply chain and origin stories to potential buyers. This creates a bridge between supply chain management and branding. As they describe their service on their website: "With our technology, you can easily gather and verify stories, keep them connected to physical things and embed them anywhere online."

This focus on origin and process rather than outcome and use scenarios is slightly different than what we would describe as IoT trust labels, but it plays to the same larger notion: Transparency and "good" processes will lead to better outcomes, empower consumers to make better decisions, and allow responsible manufacturers to differentiate themselves through quality rather than price.

Lint for good data practices

Lint (Wikipedia) is a software tool for programmers which flags suspicious code. Having been around since 1979, Lint (or Lint-like tools) for example highlights unused variables (which indicate discrepancies between the developers intentions and actual code), or style inconsistencies in the code. This supports developers in making better informed decisions in their day-to-day work.

We were introduced to the notion of "Lint for good data practices" by David Ascher (website). The software developer, former Vice President of the Mozilla Foundation, and O'Reilly author proposed building a Lint-like tool that would highlight not code inconsistencies but potentially problematic security practices.

For example, it might flag code that stores passwords in clear text, reminding the developer that this is a bad data practice, and instead propose a better solution.

For non-developers like product managers, designers, or entrepreneurs check lists could potentially play a similar role. Rather than highlighting faulty code, a checklist might probe if a connected product would share data with third parties, if cameras could be physically blocked, or if selling user data was part of the business model.

We would include the list of 37 principles outlined in the Online Trust Alliance's "IoT Trust Framework" (OTA 2017) in the category of checklist as well.

Restart Project: Software lifecycles

Recognizing that in IoT, product lifecycles are increasingly not limited by hardware but by software, The Restart Project has announced working on an initiative increase transparency about software lifecycles and, hopefully, increasingly the lifecycles as well.

Insurances

As Mozilla Tech Policy Fellow and Director of NYU's Technology Law & Policy Clinic points out in personal communication, collaborating with insurance companies around cybersecurity insurance might offer significant leverage. An insurance would need to use the trustmark as a criterion in the context of financial incentives.

City & national governments

City and national governments are also great potential adopters of the IoT trustmark and similar labels. Especially in their procurement these governments can make a big difference by agreeing to only purchase IoT devices that carry the IoT trustmark.

REFERENCES

Adryan, B 2015, "Connected product labelling", blog post, 30 September 2015. Available from http://iot.ghost.io/connected-product-labelling/ [7 July 2017]

Adryan, B 2017, 'Strong commitment to openness at Bosch. "Some people hate me for missed business opportunities", says @Stefferber at #iotmark', Twitter post, 16 June 2017. Available from https://twitter.com/BorisAdryan/status/875638841956114432 [7 July 2017]

AvantGadget 2017, "Iot Identity Brand Guide". Available from http://avantgadget.io/iot/ [7 July 2017]

Beyond.io, 2016, "Washing instructions for the IoT", commissioned by Just Things Foundation.

Bihr, P, Thorne, M 2016, *Understanding the Connected Home*. Available from https://theconnectedhome.org/ [30 March 2017]

Bihr, P 2017, "Connected doll Cayla, connected TVs & the legal status of IoT in Germany", *The Waving Cat blog*, blog post, 9 March. Available from http://www.thewavingcat.com/2017/03/09/connected-doll-cayla-connected-tvs-the-legal-status-of-iot-in-germany/ [3 April 2017]

Bihr, P 2017b, "View Source: Shenzhen", a ThingsCon report. Available from http://www.thewavingcat.com/viewsource-shenzhen/ [5 September 2017]

Bourke, G 2016, "Knowing more about the things we buy", Projects by IF blog, blog post, 19. August. Available from https://projectsbyif.com/ideas/knowing-more-about-the-things-we-buy [11 April 2017]

BSI 2017, *Internet of Things (IoT) Secured BSI Kitemark*. Available from https://www.bsigroup.com/en-GB/kitemark/services/-Internet-of-Things-IoT-Secured-BSI-Kitemark/ [11 August 2017]

Consumers International 2016, "Building a digital world consumers can trust". Available from http://digitalpolicies.consumersinternational.org/ [30 March 2017]

Creative Commons 2017, website, available from https://creativecommons.org [3 July 2017]

Crowdsupply 2017, 'Proclamation of User Rights'. Available from https://www.crowdsupply.com/about [7 July 2017]

CUPS 2010, *Privacy Nutrition Labels*, CyLab Usable Privacy and Security Laboratory, Carnegie Mellon University. Available from https://cups.cs.cmu.edu/privacyLabel/ [13 April 2017]

Deschamps-Sonsino, A 2015, "What does it do? A proposal for connected product labelling", Designswarm blog, blog post September 2015. Available from http://designswarm.com/blog/2015/09/what-does-it-do-a-proposal-for-connected-product-labelling/ [29 March 2017]

Deschamps-Sonsino, A 2017, personal communication, interview on 30 June 2017.

Deutscher Bundestag 2017, *Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, Beschlussempfehlung* und Bericht des Innenausschusses (4. Ausschuss), Drucksache 18/11908, 30. March. Preview available from http://dip21.bundestag.de/dip21/btd/18/118/1811808.pdf [6 April 2017]

European Commission 2016, "The 'Blue Guide' on the implementation of EU product rules 2016". Available from http://ec.europa.eu/DocsRoom/documents/18027/ [29 March 2017]

European Commission 2017, "CE marking". Available from http://ec.europa.eu/growth/single-market/ce-marking_de [29 March 2017]

European Commission 2017b, "Internet of Things Privacy & Security Workshop". Available from https://ec.europa.eu/digital-single-market/en/news/internet-things-privacy-security-workshop [10 August 2017]

European Union 2017, "CE marking", Your Europe. Available from http://europa.eu/youreurope/business/product/ce-mark/index_en.htm [29 March 2017]

Fairphone 2015, "Comparing Fairphone's approach to a sustainability label", blog post, 23 July 2015, available from https://www.fairphone.com/en/2015/07/23/comparing-fairphones-approach-to-a-sustainability-label/ [12 July 2017]

Fairphone 2016, "Fairphone 2 is first smartphone to receive Blue Angel certification", blog post, 24 October 2016. Available from https://www.fairphone.com/en/2016/10/24/fairphone-2-first-smartphone-receive-blue-angel-certification/ [12 July 2017]

Fairtrade International 2012, "For Producers, With Producers", Annual Report 2011-12. Available from https://www.fairtrade.net/fileadmin/user_upload/content/2009/resources/2011-12_AnnualReport_web_version_small_FairtradeInternational.pdf [12 June 2017]

Federal Communications Commission (FCC) 2016, Consumer Labels for Broadband Services. Available from https://www.fcc.gov/consumers/guides/consumer-labels-broadband-services [13 April 2017]

Fimin, A 2016, "A Trusted IoT label", AOTIO, workshop on security and privacy in the hyper-connected world. Available from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16507 [29 March 2017]

FTC 2017, "What Vizio was doing behind the TV screen", FTC news published 6 February 2017. Available from https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen [14 August 2017]

Gibbs, S 2016, "Ransomware attack on San Francisco public transit gives everyone a free ride", *The Guardian*, 18 November 2016. Available from https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware [3 April 2017]

Gessinger-Erhardt, B 2016, "Certification Use Case - Challenges of Certified Systems in the Hyper-Connected World", AIOTI workshop on security and privacy in the hyper-connected world. Available from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16510 [29 March 2017]

Gibbs, S 2015, "Samsung smart TVs send unencrypted voice recognition data across internet", The Guardian, 19 February 2015. Available from https://www.theguardian.com/technology/2015/feb/19/samsung-smart-tvs-send-unencrypted-voice-recognition-data-across-internet [14 August 2017]

Greenberg, A 2015, "Hackers remotely kill a Jeep on the highway—with me in it", WIRED. Available from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [3 April 2017]

GSMA 2016, "GSMA IoT Security Guidelines". Available from http://www.gsma.com/connectedliving/gsma-iot-security-guidelines-complete-document-set/ [30 March 2017]

Hackett R 2017, "Why Connected Gadgets Need Security 'Nutrition Labels'", Fortune, 15 February. Available from http://fortune.com/2017/02/15/rsa-symantec-iot-security-labels/ [13 April 2017]

iFixit 2017, 'Device Reparability Scores'. Available from https://www.ifixit.com/Info/Repairability [7 July 2017]

Intellectual Property Office 2014, *Guidance on collective and certification trade marks*, United Kingdom, 29 April 2014. Available from https://www.gov.uk/government/publications/collective-and-certification-trade-marks [11 May 2017]

International Organization for Standardization (ISO) 2014, "ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure". Available from https://www.iso.org/standard/45170.html [3 July 2017]

#iotmark 2017, "An Open Internet of Things Certification Mark project", project website by Alexandra Deschamps-Sonsino and Usman Haque. Available from https://iotmark.wordpress.com/ [13 September 2017]

Ito, J 2009, "Innovation in Open Networks - Creative Commons, the Next Layer of Openness", *Joi Ito's blog*, 30 October 2009. Available from https://joi.ito.com/weblog/2009/10/30/innovation-in-o.html [13 September 2017]

James, L 2017a, "Trustworthy tech — what would it take?", Doteveryone, blog post, 11 July 2017. Available from https://medium.com/doteveryone/trustworthy-tech-what-would-it-take-dc65ab132568 [9 August 2017]

James, L 2017b, "Exploring what "responsible technology" means", Doteveryone, blog post, 24 May 2017. Available from https://medium.com/doteveryone/exploring-what-responsible-technology-means-4f2a69b50a61 [9 August 2017]

James, L 2017c, personal communication, interview on 30 June.

Jenson, S 2017, "The Future IoT: Building Better Legos", *IEEE Computer*, vol. 50, no 2 (Feb 2017), pp. 68-71. Available from http://ieeexplore.ieee.org/document/7842836/ , also available from https://jenson.org/legos/ [29 June 2017]

Just Things 2015, 'IoT Design Manifesto'. Available from https://www.iotmanifesto.com [7 July 2017]

Kelley, PG, Bresee, J, Cranor, LF, Reeder, RW 2009, "A 'Nutrition Label' for Privacy", *Proceedings from the Symposium On Usable Privacy and Security*, Mountain View, CA, July 15-17, 2009. Available* from http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf [13 April 2017]

Kleinhans, J 2016, "IT-Sicherheit im Internet der Dinge", Stiftung Neue Verantwortung, Berlin. Available from https://www.stiftung-nv.de/de/publikation/it-sicherheit-im-internet-der-dinge [29 March 2017]

Larsen, S 2017, personal communication, interview 12 July 2017.

Lewis, A, McKone, D 2016, "To Get More Value from Your Data, Sell It", *Harvard Business Review*, 21 October. Available from https://hbr.org/2016/10/to-get-more-value-from-your-data-sell-it [3 April 2017]

Li, D 2017, personal communication, email 5 August 2017.

Lilliestam, E 2017a, "Open IoT definition—thoughts and suggestions", Medium.com, blog post, 9 June 2017. Available from https://medium.com/@emalstm/open-iot-definition-thoughts-and-suggestions-7103845c03e6 [3 July 2017]

Lilliestam, E 2017b, personal communication, interview on 23 June 2017.

National Institute of Standards and Technology (NIST) 2016, Securing and Growing the Digital Economy, report by the Commission on Enhancing National Cybersecurity, US Department of Commerce, 1 December 2016. Available from https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf [13 April 2017]

Online Trust Alliance (OTA), 2017, "IoT Trust Framework". Available from http://otalliance.actonsoftware.com/acton/attachment/6361/f-008d/1/-/-/-/-/IoT%20Trust%20Framework.pdf [30 March 2017]

Online Trust Alliance (OTA), 2017, "Securing the Internet of Things". Available from http://otalliance.actonsoftware.com/acton/attachment/6361/f-00a1/1/-/-/-/-/IoT%20Shared%20Roles%203-2017.pdf [30 March 2017]

Open Web Application Security Project (OWASP) 2016, "IoT Security Guidance". Available from https://www.owasp.org/index.php/IoT_Security_Guidance [30 March 2017]

Open Web Application Security Project (OWASP) 2015, "Web Application Security Testing Cheat Sheet". Available from https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet [3 July 2017]

Open Source Hardware Association (OSHWA) 2017, "Open Source Hardware Certificate". Available from http://certificate.oshwa.org/ [3 July 2017]

Oxford University Centre for Corporate Reputation 2012, Comment in Reputation Issue 3. Available from http://www.sbs.ox.ac.uk/sites/default/files/CCR/Docs/2012-03-Reputation.pdf [12 June 2017]

Penney J 2016, "Chilling Effects: Online Surveillance and Wikipedia Use". Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117, 2016. Available at https://ssrn.com/abstract=2769645 [9 August 2017]

Project by IF 2016a, "Data Licenses", prototype service. Available from https://datalicences.projectsbyif.com/ [7 July 2017]

Projects by IF 2016b, "IF Data Permissions Catalogue". Available from https://catalogue.projectsbyif.com/ [11 April 2017]

Robbins, H 2017, "The path for transparencies for IoT technologies", The State of Responsible IoT. Available from http://bit.ly/riot-report [27 June 2017]

Robbins, H 2017b, personal communication, interview on 27 June 2017.

Rosner, G 2016, "Trustmarks in the identity ecosystem", Open Identity Exchange, Identity steering group white paper. Available from http://www.openidentityexchange.org/wp-content/uploads/2016/11/Trustmarks-paper-FINAL-v2.pdf [30 March 2017]

Santucci, G 2017, personal communication, interview in June 2017.

Schneier, B 2016a, "We Need to Save the Internet from the Internet of Things", Motherboard. Available from https://www.schneier.com/essays/archives/2016/10/we_need_to_save_the_.html [3 April 2017]

Schneier, B 2016b, "Lessons From the Dyn DDoS Attack". Available from https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html [3 April 2017]

Schneier, B 2016c, "Regulation of the Internet of Things". Available from https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html [3 July 2017]

Smit, I 2017, 'Bosch used the insights of IoT open definition from 5 yrs ago in their iot thinking. Now in brand book. @Stefferber #iotmark', Twitter post, 16 June 2017. Available from https://twitter.com/iskandr/status/875635210615898113 [7 July 2017]

Sterling, B 2012, "The Provisional Declaration of the Open Internet of Things Assembly", WIRED, 21 June 2012. Available from http://iot.london/open-internet-of-things-definition [7 July 2017]

The Digital Standard, 2017. Available from https://www.thedigitalstandard.org/ [30 March 2017]

ThingsCon 2017, "The State of Responsible Internet of Things", report by ThingsCon e.V., published June 2017. Available from http://thingscon.com/responsible-iot-report/ [10 July 2017]

Weber, J 2016, "Certification in the Hyper-connected World", Federal Office for Information Security. Available from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16509 [29 March 2017]