NGI FORWARD

REPORT:
DIGITAL TRUSTMARKS

January 2020

NEXT GENERATION INTERNET
INTERNET OF HUMANS

AUTHORS

Hessy Elliott, Researcher, Nesta

ACKNOWLEDGEMENTS

The author would like to thank Peter Bihr at ThingsCon and Allison Gardner and Trish Shaw at Women Leading in AI for their contributions to this report.

ABOUT NGI FORWARD

NGI Forward is the strategy and policy arm of the Next Generation Internet (NGI), a flagship initiative by the European Commission, which seeks to build a more democratic, resilient and inclusive future internet. The project is tasked with setting out an ambitious vision for what we want the future internet to look like, and identifying the concrete building blocks - from new technologies to policy interventions - that might help bring us closer towards that vision.

NGI Forward is made up of an international consortium of seven partners: **Nesta** in the United Kingdom, which leads the project, **DELab** at the University of Warsaw in Poland, **Edgeryders** in Estonia, the **City of Amsterdam** in the Netherlands, **Nesta Italia** in Italy, **Aarhus University** in Denmark and **Resonance Design** in Belgium. The NGI Forward project commenced in January 2019 and will run for three years. To learn more or get involved, visit **http://research.ngi.eu**.

EXECUTIVE SUMMARY

Trustmarks are a well-established mechanism that can help consumers recognise trusted providers and make more informed decisions about the goods and services they buy. This report explores the value and challenges of using a 'trustmark' in the internet space, to consider whether a *Next Generation Internet* trustmark could be created to support the development and use of responsible technology and software.

UNDERSTANDING THE POTENTIAL VALUE OF AN NGI TRUSTMARK

Developing an NGI trustmark would be a valuable initiative in helping to build a future human-centric internet.

- There is considerable public demand for a solution addressing internet safety and user protection.
- Introducing a digital trustmark could build further consumer engagement and positively shape company behaviour, supporting the creation of a stronger market for responsible and ethical technologies, products and services on the internet.
- Little currently exists to fill this gap and if a trusted institution operating for the public good doesn't introduce a trustmark like initiative the vacuum could be filled by more commercial and less accountable certification initiatives.

There are a number of existing and emerging trustmark initiatives in different areas of the digital space which aim to address the specific problems of these different tools.

- The main areas of focus are: cyber security; the Internet of Things; artificial intelligence and algorithms; and 'fake news' and disinformation. No-one has yet sought to develop something more comprehensive that might cover many different issues at once. Very little has so far been done on digital sustainability or environmental impact.

Despite trustmarks being a promising tool for addressing key issues facing internet users, there are several key challenges facing the development of a digital trustmark.

- Creating a meaningful and accessible user experience, given the complexity and dynamic nature of digital tools and technologies is particularly tricky. The need to balance complexity and requirement for regular updates has to be balanced with user simplicity and understandability.
- Establishing trust, recognition and legitimacy of the trustmark among users across Europe will require significant investment.
- The governance structure of the trustmark. Establishing a successful trustmark would require a large organisation with sufficient capacity, resources and legitimacy.
- Evaluation and assessment of digital products or services that may be constantly changing will be difficult.

DESIGNING AN NGI TRUSTMARK

Our research explored examples of trustmarks from digital and non-digital sectors, and identified several key points and potential models for the development of an NGI or digital trustmark:

- Firstly, our research suggests that a **single, comprehensive trustmark would be more successful** than multiple, potentially competing or overlapping initiatives, which would likely lead to consumer confusion. A single point of reference is more likely to become well-known and understood across Europe and beyond. This could be achieved via an **'umbrella' structure** that would balance the consumer's need for a comprehensive trustmark with the organisational and technical need for different metrics for different issues or types of internet tools and products. This umbrella NGI trustmark could act as the overarching brand that consumers recognise as a sign of trustworthiness across all internet tools and technologies. This would have the benefit of giving consumers the same experience across the internet, making the trustmark simple, easy to understand, and widely-recognised.
- A trusted, well resourced and cross European organisation, for example the European Commission, would need to take responsibility for such a trustmark as its success will depend

on adequate investment for development and publicity.

- This trustmark could cover a wider variety of areas but our research suggests that criteria should include developed around **cyber security, privacy and data practices, transparency, bias and inclusive representation, accountability, and sustainability**. As the information related to these areas could become complex or unwieldy, mechanisms such as a traffic light system and route to finding out more granular details (e.g. each website or tool could have a QR code linking to updatable information covering all the relevant areas) could be used. Any criteria used should be supported by existing or future legislation to ensure the trustmark can signal best practice rather than a minimum standard.
- Careful consideration will need to be given to how trustmark criteria might be assessed and audited, its governance framework and how it will be paid for. To do this well a wide varity of stakeholders should be consulted, including companies, citizens and those already developing digital and non-digital trustmarks.
- Governance models usually fall into one of two categories: voluntary and fee-paying, with compliance assessed by the governing institution; and mandatory (supported by regulation/legally-binding agreements) and free, with compliance self-assessed by the participating organisation.

Based on our findings we recommend that the European Commission invests and takes a lead in the development of a trustmark for digital technologies, products and services. The NGI Forward project, funded by the Commission through the Next Generation Internet Initiative, will convene relevant stakeholders again to further co-develop and co-design elements of a potential NGI trustmark.

INTRODUCTION

BACKGROUND

The European Commission has previously considered digital trustmarks, particularly in the context of promoting eCommerce[1], and in 2015 implemented the eIDAS trustmark for online transactions.[2] However, looking beyond these specific use cases, many more of the EU's recent accomplishments and several policy priorities for the incoming Commissioners-designate could be augmented by a strategic and harmonised approach to digital trustmarks. These opportunities range from the immediate – like promoting the new cybersecurity certification framework for ICT products and services or giving Europe a first-mover advantage in the promotion of strong standards for trustworthy AI – to the more long-term, such as President-elect Ursula von der Leyen's vision for a climate-neutral and more circular economy.

A well-designed and industry-supported digital trustmark framework could also have an important role to play in improving the delivery of the Digital Single Market and avoiding further fragmentation through national or commercially-led initiatives in this space. As the incoming Commissioner-designate for the Internal Market, Thierry Breton, recently highlighted, these objectives will require the provision of "broader access to information and advice for citizens and businesses" and "effective and efficient rules [that] enhance consumers' trust and help firms selling their products and services."[3] Given the investment and interest being placed in programmes such as the Commission's Next Generation Internet initiative (NGI)[4], which seeks to develop and define Europe's vision and role in the future of the internet, it is worth re-examining trustmarks as policy tool to meet the Commission's goals in this space. A trustmark is a badge, image or logo indicating a product, service or company conforms to a set of specific criteria, such as the fair treatment of workers or the use of relevant standards, thereby giving consumers trust in the quality of provenance of the goods or services they are buying. This report aims to explore whether and how a trustmark approach, given its consumer-empowering and standard-promoting nature, could deliver on these objectives. This report is based on desk research, a workshop and interviews.

Value of a digital trustmark for a human-centric internet

Our research shows that many relevant stakeholders consider trustmarks as a viable and valuable approach to helping build a more human-centric internet, which embodies European values of openness, transparency, resilience, privacy and protection of data. Stakeholders agreed that it would be worth pursuing the development of a digital trustmark despite the challenges this would pose, since it could offer an effective solution to key issues facing internet users. Peter Bihr, founder of The Waving Cat[5] and ThingsCon[6], emphasised the importance of a digital trustmark in addressing the current lack of transparency, accountability and consumer protection in the internet space, suggesting that a trustmark could be hugely valuable in helping to balance the "asymmetry of information and power that currently exists between companies and consumers".[7] Trish Shaw from Women Leading in AI stressed the need for a digital trustmark in order to protect, inform and empower users with regard to algorithmic decision-making, and to create a culture of understanding around AI and internet safety.[8]

Consumer demand

There is debate over how extensive consumer demand for a digital trustmark might be. Laura James, from the University of Cambridge and the UK NGO Doteveryone, has expressed doubts: "We're not yet at the tipping point where consumer concern around tech trustworthiness and ethics translates to action. Purchasing pressure is a very limited lever for change at present".[9] However, a survey conducted by the Finnish innovation agency Sitra found that these issues are considered important by the general public, leading Laura Halenius from Sitra to conclude that a trustmark of this kind would be valuable.[10] Sitra found that 66% of 8,002 respondents across four countries agreed that a label indicating fair data use would be fairly to very important, and 42% of respondents said a lack of trust in service providers prevents them from using digital services.[11] Others have also argued that there is undoubtedly consumer appetite for responsible technology- there may not necessarily be demand for a trustmark specifically, but there is certainly growing public demand for some kind of action to promote internet safety and protection and offer consumers a better way to verify that they can trust a product.[12]

Building consumer engagement

Even if consumer-driven demand for a digital trustmark is not particularly strong right now, introducing a trustmark could be effective in helping to build consumer engagement. By actively engaging consumers in an informative way, a digital trustmark could raise awareness and help the general public to better understand processes such as algorithmic decision-making and use of data. Introducing a trustmark could create a virtuous cycle:

1 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1815
2 https://ec.europa.eu/digital-single-market/en/eu-trust-mark
3 https://www.europarl.europa.eu/resources/library/media/20191113RES66410/20191113RES66410.pdf
4 https://ec.europa.eu/digital-single-market/en/next-generation-internet-initiative
5 https://thewavingcat.com/
6 https://thingscon.org/
7 Peter Bihr (2019), pers. comm.
8 Trish Shaw (2019), pers. comm.
9 Laura James (2019), Why we haven't made a trustmark for technology, https://doteveryone.org.uk/2019/09/digital-products-and-services-arent-bananas/
10 Laura Halenius (2019), pers. comm.
11 Sitra (2019), The use of digital services, p.23/56, https://media.sitra.fi/2019/01/16142451/citizen-survey-digital-services-all-countries.pdf
12 Peter Bihr (2019), pers. comm.

it would help build consumer engagement and shape consumer behaviour, which could consequently shape the field, as consumers making smarter choices might put pressure on more developers and companies to follow suit.[13]

A vacuum waiting to be filled

There is a strong feeling among many working/active in this area that a trustmark-like mechanism would fill an important vacuum. Stakeholders feared that if a trusted institution operating for the public good, like an NGO or the European Commission, does not develop a digital trustmark covering the areas explored in this report soon, a proliferation of industry-led certification initiatives will likely emerge to fill this gap. As a result of recent controversies and existing business models, many believe that industry actors could not be trusted to create a meaningful trustmark tool as there will likely be commercial - and perhaps cynical - interests underlying these initiatives. Consequently it is important that any digital trustmark initiatives are led by respected and trusted public authorities or non-profit bodies. The trustmark itself could prove to be a valuable tool in creating a European market for responsible and ethical technologies.

Structure of this report

To explore the value of trustmarks, we have gathered examples of similar initiatives which already exist in the digital space, as well as salient examples of successful trustmarks from non-digital sectors. This is not a comprehensive survey of all existing initiatives, but the examples cited highlight different possible models for trustmarks, and provide important insights on the kinds of challenges we face in attempting to create a trustmark for the internet. The report is structured as follows:

- An overview of some existing trustmark initiatives in different areas of the digital space, and the issues which these are trying to address;
- An examination of the challenges and obstacles trustmark for the internet;
- An exploration of each of these challenges, with relevant examples of trustmarks from digital and non-digital sectors which involve specific practical elements that may offer possible solutions to these challenges.

13 *Peter Bihr (2019), A trustmark for IoT, p.6 https://www.mozillapulse.org/entry/436*

DIGITAL TRUSTMARKS

We found numerous examples of interesting and valuable initiatives in the digital space that are attempting to address issues around user protection through the use of a trustmark. Each of these initiatives focuses on a specific area or concern surrounding digital technology. The main focus areas identified are:

- Cybersecurity
- Internet of Things
- AI & algorithms
- 'Fake news' and disinformation.

CYBERSECURITY

Trustmarks in the field of cybersecurity are a widespread and an established tool for consumer protection. Cybersecurity trustmarks are most frequently governed by security software companies. For example, ***McAfee Secure*** certification indicates to consumers that a site has been tested and certified to be free of malware, viruses, phishing attacks, and other harmful elements.[1] Often, the function of cybersecurity trustmarks is to offer consumers reassurance when making online purchase.

INTERNET OF THINGS

Trustmarks for the 'Internet of Things' (IoT) and connected/smart devices are of growing interest. A literature review commissioned by the UK Government found that certification mechanisms for IoT products and services are being widely discussed at ***EU level*** and within internet governance and technical organisations such as the ***ITU*** and ***IEEE*** as a potentially advantageous mechanism to enhance user trust.[2] A ***ThingsCon report*** commissioned by Mozilla's Open IoT Studio argues that a trustmark for IoT would be valuable to help consumers see whether the specific challenges and risks facing IoT products have been addressed by the company. These challenges include: security breaches, the selling and sharing of user data, surveillance, remote software updates changing devices in unexpected ways, risk to physical safety, lifecycle and maintenance.[3] ThingsCon have developed and launched a trustmark for connected products, the ***Trustable Technology Mark***, which signals to the user that the company has a commitment to high standards in trustable technology, user rights and responsible data practices.[4] An issue highlighted by advocates of a trustmark for IoT is that due to the interconnectivity of smart devices, a trustmark for IoT products would need to be approached holistically: there must be consideration of how systems function in relation to the cloud and regarding data passed onto other parties, rather than focusing only on individual products.

AI AND ALGORITHMS

There have been several calls from leading experts in AI to implement a trustmark type mechanism for algorithms. The ***German Data Ethics Commission*** has made explicit mention of the value of standards and the need to provide manufacturers with adequate incentives to implement features it has identified as critical, such as ensuring privacy-friendly design. The Data Ethics Commission also recommends the introduction of a labelling scheme for algorithmic systems, which would oblige operators to make it clear when and how algorithmic systems are being used.[5] Australia's Chief Scientist **Alan Finkel** has called for the development of a trustmark for AI, the ***Turing Certificate,*** so that consumers can identify and make informed decisions about which products and vendors are worthy of trust, and to build a culture of improved standards within companies.[6] ***Women Leading in AI (WLAI)*** are proposing an infomark for AI[7] that would flag to users when they have been subjected to an automated process, notifying them when a machine-learning decision is influencing their interaction or processing their data. They propose that the infomark should be an active tool, which clearly explains to users what the algorithm is and does, who is accountable for it, and where the user can go if they wish to make a complaint.[8] ***O'Neil Risk Consulting & Algorithmic Auditing (ORCAA)*** have created a process for assessing potential bias in algorithms and artificial-intelligence programs and a trustmark labelling scheme for companies that meet their standards. ORCAA offers an algorithmic auditing service for specific algorithms and use cases, and awards the ORCAA's Seal of Approval when the algorithm is judged to be relatively robust according to their standards. This Seal of Approval functions as a trustmark, signalling to users that the company is trustworthy and that the algorithms used meet agreed standards.[9]

'FAKE NEWS' AND DISINFORMATION

There have been concerted efforts to tackle the spread of disinformation through unreliable sources on social media. ***'Disputed' tags*** - which attach warnings to news stories that have been disputed by third-party fact-checkers, often after being flagged by users - have been widely employed by platforms like Instagram and Facebook.[10] Disputed tags are essentially the inverse of a trustmark, as they highlight that users should be wary of trusting a source. However, there are concerns about the capacity and effectiveness of disputed tags. A study found that there is an 'implied truth effect' whereby false stories that fail to get tagged are considered validated, and thus are seen as more accurate - the mechanism would need to be all-encompassing to be effective, yet fact-checking every story would be nearly impossible.[11]

1 *https://www.mcafeesecure.com/for-consumers*
2 *Petras (2018), Summary literature review of industry recommendations and international developments on IoT security, p.7, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775854/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf*
3 *Peter Bihr (2019), A trustmark for IoT, https://www.mozillapulse.org/entry/436*
4 *https://trustabletech.org/*
5 *German Data Ethics Commission (2019), Opinion of the Data Ethics Commission, p.21, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=1*
6 *https://www.weforum.org/agenda/2018/05/alan-finkel-turing-certificate-ai-trust-robot/*
7 *WLAI have moved away from using the term 'trustmark' and prefer the term 'infomark'.*
8 *Allison Gardner & Trish Shaw (2019), pers. comm.*
9 *http://www.oneilrisk.com/*
10 *https://www.bbc.co.uk/newsround/49370683; https://www.bbc.co.uk/news/blogs-trending-49449005*
11 *Gordon Pennycook et al (2019), The Implied Truth Effect: Attaching warnings to a subset of fake news stories increases perceived accuracy of stories without warnings, Management Science, https://ssrn.com/abstract=3035384*

A US-based initiative has introduced a tool which functions more like a traditional trustmark: the ***Trust Project*** has developed a common set of standards for media transparency that it calls 'trust indicators'. The Trust Project has partnered with social media sites and search engines including Facebook, Twitter and Google, which have started using the indicators in their feeds to give users a measure of the trustworthiness of articles.[12] Similarly, ***NewsGuard*** is an internet trust tool launched by journalists in 2018 to help tackle the problem of disinformation online. NewsGuard rates and reviews news and information websites using nine standards of credibility and transparency, allocating a 'nutrition label' review which provides information on the site's ownership, financing, content, credibility, transparency and history. NewsGuard is installed by users as a browser extension, and displays these 'nutrition labels' next to headlines in social media feeds, search results and on news sites, warning users when they view content from what it considers to be fake news websites. The initiative has attracted support from some major tech companies - for instance, NewsGuard is now offered by Microsoft as an optional setting in the desktop and mobile versions of its Edge mobile browser.[13]

Each of the trustmark initiatives outlined above focus on one specific technology or product. There is a sense among stakeholders that, although it might be highly beneficial for users, developing a comprehensive trustmark that applies to trustworthy tools, technologies and products across the whole internet would be incredibly challenging and ambitious. One of the main perceived obstacles is the cost and organisational capacity that would be required to govern such an all-encompassing trustmark.[14]

SUSTAINABILITY

We did not identify many digital trustmarks that included criteria related to sustainability or environmental impact - with the exception of the recommendations of the German Data Ethics Commission and in the field of IoT, where issues of device maintenance and life-cycle are being addressed. Environmental sustainability is of growing concern to both consumers[15] and the European Commission with a key focus on the concept of a Green New Deal. As such any future NGI trustmark initiative would need to include some provision for sustainability and environmental impact. Critical issues include: energy use, supply chain impact and resilience, natural resource use (including use of rare earth metals), device life-cycle and reparability, and systems design (e.g. discouraging excessive consumer use).

12 *https://niemanreports.org/articles/can-extreme-transparency-fight-fake-news-and-create-more-trust-with-readers/; https://thetrustproject.org/*
13 *UK Government Online Harms White Paper (2019), p.91 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf; https://www.newsguardtech.com/*
14 *https://doteveryone.org.uk/2019/09/digital-products-and-services-arent-bananas/*
15 *https://www.nielsen.com/eu/en/insights/article/2018/global-consumers-seek-companies-that-care-about-environmental-issues/; https://www.cgsinc.com/en/news-events/CGS-Survey-Reveals-Sustainability-Is-Driving-Demand-and-Customer-Loyalty*

THE CHALLENGES OF CREATING A DIGITAL TRUSTMARK

Despite trustmarks being a promising tool for addressing issues facing internet users, we have identified several key challenges facing the development of a digital trustmark:

- **How to balance making the trustmark both meaningful and accessible for the user?** Digital tools and technologies are highly complex and evolve rapidly. This means it might be difficult for a digital trustmark to convey meaningful and up-to-date information in a way that is useful and simple enough for the consumer to understand. Too much information may confuse consumers or complicate the meaning of the trustmark.
- **How to establish trust, recognition and legitimacy of the trustmark among users?** This is essential in order for the trustmark to be successful.
- **How to develop a comprehensive trustmark which is still fit-for-purpose?** A pervasive trustmark intended to cover all internet linked devices or services would arguably be more meaningful and effective for users. However, this is not straightforward due to the huge diversity of internet tools. It would be nearly impossible to develop specific metrics that could meaningfully apply to all these types of products, for example requirements and issues related to the use of AI may be very different to issues posed by some IoT devices.
- **How to govern a digital trustmark?** It is costly and difficult to evaluate and monitor compliance. There are difficult decisions to be made regarding the process of accreditation. Should the trustmark be voluntary or mandatory? Should the governing body actively audit tools to monitor compliance, or should the criteria be self-assessed by the participating companies? Should participating companies pay fees for certification or should the trustmark be free or charge?
- **How to encourage companies to participate?** There is a concern that companies might be resistant to the idea of a trustmark, as they might not perceive any benefit to themselves. If there is not enough buy-in for the initiative among companies, its effectiveness will remain limited.

The following sections will explore each of these challenges, providing relevant examples of trustmarks from digital and non-digital sectors which involve specific practical elements that may offer possible solutions to these challenges.

CHALLENGE 1: HOW TO BALANCE MAKING THE TRUSTMARK BOTH MEANINGFUL AND ACCESSIBLE FOR THE USER?

When considering the design and functioning of a trustmark for internet technologies, a tension emerges between the needs of the consumer and the requirements of digital tools and products. For consumers, a trustmark needs to be simple and easily comprehensible. Traditional trustmark logos - like ***Fairtrade***, the ***Vegan Trademark,*** and ***Woolmark*** - act as a stamp of approval: no further information is required because the public recognises what the symbol signifies. But as Laura James highlights, developing a trustmark for the internet is more complicated, because digital tools and technologies "aren't like bananas": they are highly complex, and are dynamic, evolving rapidly with new updates, new technology and new data.[1] Is it possible to design a trustmark which deals with this complexity and dynamism, while remaining simple enough for users to understand?

Dealing with complexity

Striking the right balance on this issue is considered key to a successful digital trustmark: it should alert consumers in a simple, accessible way, yet also be informative enough to be useful. ***Nutrition labels*** are commonly cited as a useful example to follow for the internet space, for achieving a balance between being accessible and informative. The consumer understands the nutritional rating from a quick glance at the traffic light system (e.g red might equate to high levels of salt) on the front of product, then can inspect the more detailed information on the back of the product for a breakdown of the different components. This model of a rating system accompanied by a detailed list of information is felt to be more appropriate for complex internet products than a simple stamp like Fairtrade.[2]

In the digital space, it has been suggested that a trustmark could be presented as an interactive button or a QR code linking to an online information repository. This way it could still function as an easily-comprehensible 'sticker on the box' for non-expert users, but would also be an active tool, allowing users to engage and find out more information about the product. We found examples of this model in our research. ***Ecommerce Europe*** is a Europe-wide trustmark initiative to stimulate cross-border ecommerce, which balances simplicity with transparency and information. Participating businesses display the trustmark logo on their website, and the consumer can click it to see the Code of Conduct and a clear explanation of their rights and the merchant's

1 *Laura James (2019), Why we haven't made a trustmark for technology https://doteveryone.org.uk/2019/09/digital-products-and-services-arent-bananas/*
2 *Peter Bihr (2019), A trustmark for IoT, p.8, https://www.mozillapulse.org/entry/436; Allison Gardner & Trish Shaw (2019), pers. comm.*

commitments.[3] ***SmartLabel*** offers consumers access to a wealth of further information about products via a number of methods: consumers can scan a QR code, visit a website, call a phone number or use an app to access in-depth information about hundreds of attributes which could never fit on a package label, including the ingredient sourcing, manufacturing process, animal welfare, and environmental impact associated with the product.[4]

Another useful trustmark model incorporates different levels of comprehensibility and functionality. The ***Creative Commons*** label-picker function is praised for its accessibility and utility: the lawyer-readable layer is the legal text of the licence; the user-readable layer explains this licence's permissions for a non-expert; and the machine-readable layer wraps the licence in code so developers can use it, for example in search tools or to build APIs.[5] A similar idea is used in the ***Trust Project*** initiative for transparent media. Their 'trust indicators' have a machine-readable 'tag' embedded in HTML code which can be used by the Trust Project's tech partners in their algorithms, to filter searches or to more easily surface, display or label trustworthy news to users.[6]

Keeping pace with new developments

A trustmark which links to further information via a QR code or interactive button could also be a potential way to cope with the continuous updates and developments of digital tools because it facilitates a dynamic element. Stakeholders noted that this could be a useful model, as the trustmark could link to an online repository of live information, which can be updated as the product changes, for example with software updates. This means that developments can be accommodated and evidence for the product's trustworthiness remains up to date.[7]

Another simple mechanism for keeping up with developments is to make certification time-limited, so that the trustmark is only valid for a certain period of time. This method is commonly used in the non-digital sector. For example, companies wishing to display the ***Vegan Trademark*** on their products have to renew their licence every 12 or 24 months.[8] There was a suggestion from stakeholders that a similar time-limited method could be used for a digital trustmark, indicating the date of certification, and the time period for which certification is valid (depending on agreed standards for the product). This may need to be paired with updates to different systems- though evaluation costs must be considered.

CHALLENGE 2: HOW TO ESTABLISH TRUST, RECOGNITION AND LEGITIMACY AMONG USERS?

In order for trustmarks to be effective and meaningful, it is essential that they are well-known and perceived as legitimate and trustworthy. A market research survey about consumer responses to trustmarks on ecommerce websites found that 76% of respondents had decided not to purchase something in the absence of a recognised logo, indicating that the effectiveness of trustmarks depends on customer recognition of the logo: trustmarks are not useful if they are not well-known.[9] Accreditations from well-known, trusted organisations are more valuable as they are perceived as legitimate by users and therefore build consumer confidence. A proliferation of different trustmarks adds to the problem of a lack of recognition and legitimacy: the existence of too many different, little-known trustmarks leads to confusion and a lack of trust among consumers, rendering the trustmarks meaningless. There is a sense that a single, pervasive, recognisable mark would be more effective at gaining consumer trust. Recognition of the mark could be boosted via an information or marketing campaign.[10]

The most successful trustmarks are easily recognisable, well-known, and pervasive in their respective fields. ***Fairtrade*** "has become synonymous with a fairer way of consumption", despite criticisms in recent years.[11] The Vegan Society coined the word 'vegan' in 1944 and their ***Vegan Trademark*** has been a well-established and respected symbol for consumer confidence since 1990.[12] ***Woolmark*** is recognised worldwide as the definitive textile fibre trustmark, established over 50 years ago and marking over 5 billion products.[13]

Another tool which can build users' perception that a trustmark is legitimate and meaningful, and therefore trustworthy, is a recourse or complaints mechanism. ***Ecommerce Europe*** has a dedicated complaints handling service to protect consumers - their Trustmark Service Centre provides mediation between the consumer and the business, to try and help consumers reach an out-of-court solution.[14] The UK-based certifier of domestic trades professionals, ***TrustMark***, provides information for consumers on how to resolve disputes, listing procedures to follow and advice on contacting the trustmark's affiliated professional scheme providers.[15] ***WLAI*** advocate for this model, underscoring the importance that an infomark for AI should not only indicate to users when they have been subjected to an automated process, but also offer recourse for users and information on how to make a complaint or challenge if they wish.[16]

3 *https://ecommercenews.eu/ecommerce-europe-trustmark-rolls-out-in-11-countries/*
4 *https://www.pkgbranding.com/blog/what-cpg-brands-need-to-know-about-the-smartlabel; https://www.gmaonline.org/file-manager/SmartLabel_White_Paper_June_2018.pdf*
5 *https://creativecommons.org/faq/*
6 *https://thetrustproject.org/faq/#how_tech_use*
7 *Laura James (2019), Why we haven't made a trustmark for technology https://doteveryone.org.uk/2019/09/digital-products-and-services-arent-bananas/; Peter Bihr (2019), pers. comm.*
8 *https://www.vegansociety.com/your-business/frequently-asked-questions*
9 *Econsultancy (2011) https://econsultancy.com/which-e-commerce-trustmarks-are-most-effective/*
10 *Philippa Ryan (2019), Trust & Distrust in Digital Economies, Taylor & Francis; Allison Gardner (2019), pers. comm.*
11 *Peter Bihr (2019), A trustmark for IoT, p.49, https://www.mozillapulse.org/entry/436*
12 *https://www.vegansociety.com/your-business/about-vegan-trademark*
13 *https://www.woolmark.com/our-story/about-us/*
14 *https://www.ecommercetrustmark.eu*
15 *https://www.trustmark.org.uk/consumers/if-things-go-wrong*
16 *Allison Gardner (2019), pers. comm.*

CHALLENGE 3: HOW TO DEVELOP A COMPREHENSIVE TRUSTMARK WHICH IS STILL FIT-FOR-PURPOSE?

As the above section on recognition and trust outlined, a single pervasive trustmark across the whole internet would arguably be more effective and beneficial for users, compared to a set of separate trustmarks designed for specific issues or technologies. Multiple trustmarks for similar issues may lead to confusion and a lack of recognition and trust among users. However, separate trustmarks for different tools would make more sense from a technical and legibility perspective, due to the vast range of internet issues that a digital trustmark might encompass. The majority of the initiatives we have identified each focus on one specific tool or technology: for instance, on IoT devices, or on AI algorithms. It is very difficult to imagine a specific list of standards/metrics that could meaningfully apply across the enormous variety of internet products, services and systems.[17]

One potential solution could be to create a standardized, comprehensive trustmark which could apply across all different technologies and products by simply indicating a minimum quality assurance on features which were common to all these tools - for example, sustainability of the supply chain and cyber security. However, this trustmark would not be particularly meaningful or contribute to building a human-centric internet, as it would merely be a baseline certification scheme with very low minimum standards.

Potential solution: an 'umbrella' trustmark model

A promising potential solution which would both enable the trustmark to be comprehensive, yet would also allow for meaningful engagement with the different standards required across the diverse range of internet tools and technologies, would be to employ an 'umbrella' trustmark model. In this model, there is a single, overarching, recognisable trustmark, but under the surface there is an ecosystem of different standards/metrics for different products and services. This model avoids the problems associated with having multiple trustmarks (a lack of recognition and confusion among users), and the problems associated with having a standardized comprehensive trustmark (the difficulty of making it fit-for-purpose and meaningful across different tools and technologies).

Our research found examples of this umbrella model in non-digital sectors. The UK-based certifier of domestic trades professionals, ***TrustMark***, has an interesting and potentially transferable governance structure. TrustMark is a government-endorsed, not-for-profit social enterprise, established in conjunction with government, industry bodies and consumer protection groups. TrustMark acts as an umbrella for different industry bodies, providing consumers with a single, comprehensive, well-known trustmark across a broad range of trades professions, while beneath the surface each different profession (builder, plumber, electrician, etc.) is governed by an associated profession-specific Scheme Provider. Businesses register with the relevant Scheme Provider, who ensures that these participating businesses maintain the required standards of technical competence, customer service and trading practices.[18]

The umbrella model is seen as a promising approach for the development of a digital trustmark. For example, NGI could act as an umbrella trustmark, providing an overarching brand that consumers recognise as a sign of trustworthiness across all internet tools and technologies. This would have the benefit of giving consumers the same experience across various elements of the internet, making the trustmark simple, easy to understand, and widely-recognisable. To make the trustmark actionable, there would be an organisational ecosystem behind the scenes whereby different standards and metrics were defined and evaluated for different tools, and the governing body would connect these different streams.

Deciding specific standards and metrics

Our research found substantial work is already being carried out by industry experts, civil society groups and policymakers to define trustmark-related standards for different aspects of digital tools and technologies. Any future NGI trustmark initiative should connect with and build on the work that has already been done in each field (IoT, data, AI, etc.) Such initiatives include[19]:

In the field of AI:

- The ***German Data Ethics Commission*** recommend that the following principles should be observed to ensure the responsible use of algorithmic systems: human-centred design, compatibility with core societal values, sustainability, quality and performance, robustness and security, minimisation of bias and discrimination, transparent and comprehensible systems, clear accountability structures.[20]
- ***Women Leading in AI (WLAI)*** have made significant progress in their work towards developing an infomark for AI. WLAI have been working alongside the ***Information Commissioner's Office (ICO)***, whose remit as the UK's data protection authority covers important work on AI regulation and considerations around algorithmic auditing. WLAI have created a proposition paper and are hosting a roundtable in the UK Parliament in conjunction with the ***All-Party Parliamentary Group on Artificial Intelligence.*** They are still in the process of developing their recommended requirements for AI, but their standards would likely include an evaluation of whether an algorithmic impact assessment has been done, whether the data is ethically sourced, and what the representative target

17 *Laura James (2019), Why we haven't made a trustmark for technology https://doteveryone.org.uk/2019/09/digital-products-and-services-arent-bananas/*
18 *https://www.trustmark.org.uk/aboutus/what-is-trustmark*
19 *Note: this is an illustrative rather than comprehensive list.*
20 *German Data Ethics Commission (2019), Opinion of the Data Ethics Commission, p.17-18, https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=1*

audience is. WLAI also stressed that a trustmark for AI should foreground the notion of accountability: any organisation implementing an algorithm should be held accountable for it (much like GDPR for personal data), and the trustmark should also offer recourse to challenge decisions.[21]

- The ***UK House of Lords Select Committee on Communications*** also recommended that the ICO should take a leading role in this field, suggesting the ICO should publish a code of best practice informed by the work of the ***Centre for Data Ethics and Innovation*** around the use of algorithms, and that this code could "form the basis of a gold-standard industry 'kitemark'". The Select Committee also recommended that the ICO should be empowered to conduct impact-based audits on the use of algorithms.[22]
- The ***O'Neil Risk Consulting & Algorithmic Auditing (ORCAA)*** model is a system developed by mathematician Cathy O'Neil to assess potential bias in algorithms and artificial-intelligence programs. Algorithmic auditing is undertaken using ORCAA's Ethical Matrix framework, which assesses accuracy, bias, consistency, transparency, fairness and legal compliance.[23]

Promoting transparent media and combating 'fake news':

- The ***Trust Project*** has developed 8 core 'trust indicators': best practices (regarding funding/mission/ethics); author/reporter expertise; type of work (news/comment/sponsored); citations and references; methods; whether the reporting has local origin or expertise; diversity of voices; and whether there is a possibility of actionable feedback and public participation.[24]
- ***NewsGuard*** has developed 9 criteria used to assess websites, including 5 indicators of credibility, and 4 indicators for transparency. Each criterion is scored out of 100, with scores >60 receiving a green rating, and scores <60 receiving a red rating.[25]

In the field of IoT:

- The ***PETRAS IoT Hub*** conducted a literature review of the security recommendations and standards for IoT being developed by leading industry bodies and international fora, including: the European Commission, EU Article 29 Working Party, European Union Agency for Network and Information Security (ENISA), Alliance for the Internet of Things Innovation (AIOTI), Organisation for Economic Co-Operation and Development (OECD), World Economic Forum (WEF), Association of Southeast Asian Nations (ASEAN), International Organization for Standardization (ISO), International Telecommunication Union (ITU), GSM Association (GSMA), and Institute of Electrical and Electronics Engineers (IEEE).[26]
- The UK's ***Department for Digital, Culture, Media and Sport (DCMS)*** has undertaken considerable work in this area, putting forward a set of recommendations for IoT standards and considering the development of a labelling or kitemark scheme for IoT products. Recommended standards include: password length and complexity; frequency of software updates; vulnerability disclosure policy; secure data storage; protection of and ability to delete personal data; secure communication; minimising exposed attack surfaces; system resilience to outages; and device installation and maintenance.[27] On the basis of these standards, DCMS is actively considering a Secure by Design labelling scheme for consumer IoT products to aid consumer purchasing decisions and facilitate consumer trust in companies. DCMS is currently furthering the development of a potential labelling scheme in collaboration with academic research partners and in consultation with public and industry stakeholders.[28]
- ThingsCon's ***Trustable Technology Mark*** evaluates five dimensions to establish the trustworthiness of connected devices: privacy and data practices; transparency about data use; security; stability and device life-cycle; and openness.[29]

Regarding the use of data:

- The ***IEEE Standards Association*** has launched a Global Initiative to Standardize Fairness in the Trade of Data, aiming to engage a global multi-stakeholder group of practitioners, academics, and thought leaders from the private and public sectors in a multi-year work plan where the final work product is a proposed fair trade data standards framework."[30]
- ***Sitra*** and the ***Lisbon Council*** have published a Roadmap for a Fair Data Economy, which includes the policy recommendation to develop and market a 'fair data label' to inform consumers about services' compliance with basic principles and standards of data protection and reuse.[31]

As discussed earlier, we did not find substantive engagement with sustainability and environmental issues within the digital trustmark space. Again, given the growing importance of sustainability to consumers and the European Commission - not to mention the global need to embed sustainable practices everywhere to combat the environmental impacts of human activities - it should be a core part of any future digital trustmark.

Based on existing standards and criteria currently being developed as part of digital trustmark initiatives, as well as core issues highlighted by key stakeholders, there are at least 6 areas a future NGI digital trustmark would need to cover to be comprehensive:

21 *Allison Gardner & Trish Shaw (2019), pers. comm.*
22 *https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf*
23 *http://www.oneilrisk.com/*
24 *https://thetrustproject.org/faq/#indicator*
25 *https://www.newsguardtech.com/ratings/rating-process-criteria/*
26 *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775854/PETRAS_Literature_Review_of_Industry_Recommendations_and_International_Developments_on_IoT_Security.pdf*
27 *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf*
28 *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf*
29 *https://trustabletech.org/*
30 *https://standards.ieee.org/industry-connections/gisftd.html*
31 *https://www.sitra.fi/en/publications/roadmap-fair-data-economy/*

- Cyber security
- Privacy and data practices
- Transparency
- Bias and inclusive representation
- Accountability
- Sustainability

Metrics which complement existing standards frameworks

Where new standards/metrics might be developed it is key, where possible, that they are in line with existing standards frameworks and guidelines. DCMS states that its Code of Practice for IoT is "designed to be complementary to and supportive of [other standards-setting] efforts and relevant published cyber security standards. It has been created directly with industry with the hope that future assurance and trustmark schemes related to consumer IoT will align with it".[32] The ThingsCon report on a trustmark for IoT underscores that "compatibility is key" and that a digital trustmark's standards should align with existing high-level policy and guidelines, such as GDPR. Creative Commons is praised for complementing rather than replacing existing legal frameworks.[33]

CHALLENGE 4: HOW TO GOVERN A DIGITAL TRUSTMARK?

The next major challenge is deciding on the governance structure of a trustmark. Monitoring compliance is difficult and costly, and there are various different accreditation models. Any governance model would need to consider the potential scale of auditing a vast array of different products and services on the internet.

There are several interlinked issues to consider:

- **Should compliance with the trustmark's criteria be assessed by the governing body, or should the criteria be self-assessed by the participating companies?** Actively auditing internet tools to monitor compliance would be difficult: due to the IP-intensive, technical and diverse nature of companies operating in the digital economy, products and processes can often constitute 'black boxes' that are difficult to interrogate. This creates significant hurdles for third-parties wishing to access, audit or verify them. However, allowing companies to self-assess would mean trusting a company's claims about, for example, data handling, which could mean a trustmark ends up championing tools that do not in fact meet its standards.
- A top-down approach in which the governing body carries out assessments may be more trustworthy, but would be much more time-consuming and costly. The governing body would need significant organisational capacity. If running the trustmark is very resource-intensive, then another question arises: **should participating companies pay fees for certification or should the trustmark be free?** Charging fees would help fund the trustmark, but may impose a barrier to entry, particularly for start-ups and SMEs, limiting uptake of the trustmark.[34]
- A third question to consider is **whether the trustmark should be voluntary or mandatory?** Trustmarks are traditionally voluntary schemes, but if the decision is made to pursue a self-assessed model, then it would be possible to include some mandatory requirements for companies developing digital products if this was deemed valuable.

Governance models

The governance structure of trustmarks and certification can roughly be divided into two main categories:

1. Traditional trustmarks tend to be **assessed by a governing body,** either through audits or by evaluating evidence submitted by the participating organisation that demonstrates how they meet the trustmark criteria (or through a combination of the two). These types of trustmarks are usually **fee-paying,** to cover the costs of this heavyweight, top-down approach. These schemes are **voluntary.**

For example, the ***British Council*** runs an accreditation scheme for language schools in the UK. Schools submit evidence to the governing body, then undergo an inspection which rigorously assesses the accreditation criteria. Inspections are repeated every 4 years, there may be interim inspections at random. Schools pay for inspections and an annual fee for accreditation.[35]

Similarly, companies wishing to display the ***Woolmark*** trustmark pay an application fee and submit their product for inspection. The product undergoes stringent testing (of, for example, durability and fibre composition) at an independent laboratory authorised by the governing institution. Companies pay an annual licence fee for certified products. Labelled products are subject to spot checks at any time.[36]

There is a concern that a fee-paying trustmark in the digital sector may impose a barrier to entry for start-up and SME tech companies. However, several trustmark schemes in the non-digital sector, like ***Woolmark*** and the ***Vegan Trademark***, link the fee level charged to the company size and turnover.[37] This approach could be a potential model to ensure the trustmark remains accessible to start-ups and SMEs.

2. Another model of certification is **self-assessed**: the participating organisations themselves evaluate how they measure up to a set of standards. Such schemes tend to permit self-assessment because they are either **mandatory** (and the standards are legal requirements) or because they are accompanied by some form of **accountability** and penalty for providing misleading information.

32 *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf, p.3*
33 *ibid., p.44*
34 *https://www.mozillapulse.org/entry/436, p.60*
35 *https://www.britishcouncil.org/education/accreditation/how-we-regulate/compliance*
36 *https://www.woolmark.com/certification/become-a-licensee/*
37 *https://www.woolmark.com/certification/become-a-licensee/; https://www.vegansociety.com/your-business/about-vegan-trademark*

This type of scheme is usually **free-of-charge** for the participating organisation.

For example, ***nutrition labelling*** is self-assessed, with producers responsible for calculating nutritional values and providing information. However, it is a legal requirement to declare this information on pre-packaged food, with specific authorities established in each country to enforce regulations.[38] Non-compliance with regulations is considered an offence and can be subject to harsh penalties.[39] Similarly, ***CE marking*** indicates that the manufacturer has carried out an assessment of their own product and deemed it to meet EU safety, health and environmental protection requirements. CE marking is mandatory for many products before they can be sold in the EU. Manufacturers carrying out conformity assessments themselves do not have to pay any fees.[40] Enforcement is carried out by authorities in each country, and failure to comply can lead to product recalls, prohibition notices, fines or imprisonment.[41]

Some small-scale digital trustmark initiatives provide an alternative model within this category. For the ***Open Source Hardware Certificate***, participating organisations may self-certify when they meet the certification requirements, by signing a Certification Mark Licence Agreement. This agreement binds the organisation to follow the guidelines, but it is a comparatively soft approach. Non-compliant parties may simply remove the mark from their product in good faith, or incur penalties for persistent violations, which increase in severity for repeat offenders.[42]

Similarly, the ***Trustable Technology Mark*** for IoT operates via self-assessments by participating companies which are then reviewed by a panel of experts from the ThingsCon network. The panel relies on the companies to be transparent and act in good faith, although they do make binding agreement statements on the record, so theoretically could be taken to court as an enforcement mechanism. Peter Bihr from ThingsCon said that a more heavyweight approach to governance would be preferable, but would require a great deal of funding.[43]

Using regulation to set minimum requirements and a trustmark to define higher standards

It is a well-established mechanism to have underlying legislation for minimum standard requirements, combined with a trustmark for companies who demonstrate they are employing best practices and going beyond minimum standards. For example, in the UK there is a statutory minimum wage, as well as an independently-calculated 'living wage': employers who pay staff this higher rate of pay can gain trustmark accreditation from the ***Living Wage*** Foundation which demonstrates their commitment to these higher standards. Similarly, there is EU regulation on textile labelling which specifies minimum fibre standards for use of the term 'wool' in labelling, while the term 'pure new wool' is an indication of higher fibre standards and is associated with the trustmark ***Woolmark***.[44]

The same set up has been proposed for a digital trustmark initiative. Regulations will be designed to set minimum requirements and necessary protections around issues such as data collection or accountability, and a trustmark would indicate when companies meet higher standards. Reporting or auditing of relevant systems for both regulatory and trustmark purposes could be aligned, with the trustmark governing body carrying out spot-check audits to verify whether companies or products displaying the trustmark were adhering to agreed standards. Particular concerns have been raised around the ability to verify a 'black box' system, particularly those that rely on complex neural nets. Here a much stronger legal requirement for companies to make their code accessible and auditable by a regulator or trustmark governing body would be hugely valuable. While arguments around IP can, and have, been made against these kinds of proposals, it would not be possible to assess these systems properly without access. However there is a question around how open the code should be made and the role of other non-regulatory bodies in assessing or interrogating how systems are built and used. It is important that the overall governing body would need to be a large and trusted public authority with sufficient capacity and legitimacy, but aspects of auditing could be fulfilled by different actors across member States.

CHALLENGE 5: HOW TO ENCOURAGE COMPANIES TO PARTICIPATE?

Companies might be hesitant to adopt a trustmark if they fail to perceive any commercial benefit or consumer interest. Sitra highlighted that a lack of industry interest and participation could constitute a bottleneck for the introduction of a trustmark scheme: in a survey conducted among 1600 companies across 4 countries, only a third of respondents thought that a 'fair data label' would be beneficial.[45] If there is not enough buy-in for the initiative among companies, its effectiveness will remain limited.

Benefits for participating companies

However, the widespread adoption of successful trustmarks in non-digital sectors suggests that trustmarks can offer companies benefits. If a trustmark is well-known and trusted by consumers, this builds consumer engagement and demand for products to carry the trustmark, meaning it becomes in the interest of companies to participate. Because of the wide recognition of the ***Vegan Trademark***, the Vegan Society highlight that companies displaying the mark on their products enjoy a wider appeal and

38 *https://www.gov.uk/guidance/food-standards-labelling-durability-and-composition#general*
39 *http://www.legislation.gov.uk/uksi/2014/1855/regulation/11/made*
40 *https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm#shortcut-4*
41 *https://www.cemarkingassociation.co.uk/how-is-the-ce-mark-enforced/*
42 *https://www.mozillapulse.org/entry/436, p.44*
43 *Peter Bihr (2019), pers. comm.*
44 *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/513963/BIS-16-193-textile-labelling-regulations-guidance.pdf, p.7-8*
45 *Laura Halenius (2019), pers. comm.; https://media.sitra.fi/2019/09/18135001/future-of-european-companies-in-data-economy.pdf*

increased sales.[46] A number of established trustmarks offer a reciprocal relationship with their participating organisations, whereby membership of the network has associated benefits. ***British Council*** and the ***Vegan Trademark*** offer promotional opportunities for accredited products and companies, which both helps to build public awareness of the trustmark itself, and increases company buy-in due to the marketing benefits.[47]

Reputational gains for participating companies

If there is an ecosystem of minimum standards regulations combined with a trustmark indicating adherence to higher standards, there can be reputational benefits for companies who participate in the trustmark scheme rather than just satisfying the legal minimum. In a survey conducted by ***Living Wage,*** certified employers reported that the main benefits to them were reputational gains: becoming accredited had enhanced the employer brand, differentiated the organization from competitors and improved corporate reputation. Certified employers reported improved relations with customers and clients, and agreed that the positive benefits firmly outweighed any challenges associated with becoming accredited.[48]

Tiered rating systems

Another trustmark model, which differentiates between tiered higher standards, could also help incentivise companies to participate and strive for higher standards in order to benefit their reputation. When considering how to design a potential trustmark for technology, ***Doteveryone*** highlighted that a tiered system (e.g. traffic light system, 1-5 stars or bronze/silver/gold) could support organisations in increasing their performance over time, and would also allow consumers to differentiate more clearly between products and services and make more informed decisions.[49] The ***German Data Ethics Committee*** recently released their proposal for rules around AI, arguing that algorithmic systems should be labelled according to a 5-rank system depending on the risks they pose and potential harm: systems ranked in category 3 and 4 would have to fulfill tough transparency obligations; those labelled in 5 would be outright banned.[50] This ties into the notion that there should be a combination of regulations for minimum standards, accompanied by a trustmark orabelling scheme to indicate which products and companies embody higher standards. These proposed systems resemble ***energy efficiency ratings***, an established mechanism which indicates efficiency to consumers. Energy efficiency ratings have been shown to affect consumer choice, with a study commissioned by the European Commission finding that products with more efficent energy ratings were chosen by a greater proportion of respondents.[51]

Positive side-effects of trustmarks

Trustmarks can have positive knock-on effects, not only creating new markets around trusted solutions by targeting end-users, but also helping to change production and development processes further upstream by targeting the developer community and creating a culture of improved standards. The ***CE mark*** is technically a trustmark to inform consumers that a product meets health and safety requirements, but since every product is required to display it, it has become the expected norm; in practice, the more useful function of the scheme is to set the standards for developers upstream in the design and manufacturing process. There was a strong sense among stakeholders that it would be highly valuable to establish another initiative - separate but complementary to the trustmark scheme - which focused upstream on encouraging tech companies to improve their practices and develop more responsible tools and technologies.

Trustmarks can also build a culture of improved standards as certified companies may encourage other associated or partner companies to also become certified. The ***Living Wage*** survey revealed a very positive finding that a substantial number of Living Wage Employers had encouraged contractors in their supply chains to pay the Living Wage and to adopt other good employment practices.[52] This type of outcome would be very beneficial if it were to occur in the internet space, with responsible early-adopters of the digital trustmark encouraging other companies - associated with them through procurement, supply chain or interconnectivity - to also raise their standards and adopt the trustmark.

Finally, the experience of the ***Living Wage*** shows that a trustmark scheme which indicates standards higher than the statutory minimum can end up raising minimum standards in policy and legislation. In April 2016, inspired by the Living Wage campaign, the UK government introduced a higher national minimum wage rate for all staff over 25 years old, calling this the 'national living wage'. The Living Wage Foundation questioned the government's calculations, arguing that this new rate was still insufficient, although they warmly welcomed the development which demonstrated the positive influence of this trustmark scheme and public awareness campaign on the wider policy landscape.[53]

46 *https://www.vegansociety.com/your-business/about-vegan-trademark*
47 *https://www.vegansociety.com/your-business/about-vegan-trademark; https://www.britishcouncil.org/education/accreditation/information-centres/elt-promotion*
48 *https://www.livingwage.org.uk/sites/default/files/Cardiff%20Business%20School%202017%20Report_2.pdf, p.40*
49 *https://medium.com/doteveryone/a-trustworthy-tech-mark-d45681efc019*
50 *Janosch Delcker (2019), AI: Decoded newsletter (23rd October 2019), Politico*
51 *London Economics (2014), Study on the impact of the energy label – and potential changes to it – on consumer understanding and on purchase decisions, p. 49 https://ec.europa.eu/info/sites/info/files/impact_of_energy_labels_on_consumer_behaviour_en.pdf*
52 *https://www.livingwage.org.uk/sites/default/files/Cardiff%20Business%20School%202017%20Report_2.pdf, p.40*
53 *https://www.livingwage.org.uk/what-real-living-wage*

CONCLUSION

Based on our findings, we believe it would be highly beneficial for the European Commission to play a central role in the development of a trustmark for digital technologies. There is considerable public demand for solutions to address concerns around internet safety, accountability and sustainability, and our research indicates that a trustmark mechanism - despite the challenges associated with its coherence, design and governance - could be a valuable tool to help improve levels of trust in the digital economy and build a more human-centric and sustainable internet.

We also believe that the European Commission should undertake this initiative to ensure that it maintains ownership and leadership of this space, both within the Single Market and globally. There was strong agreement among stakeholders that it is crucial for an institution acting in the public interest to introduce a digital trustmark before the vacuum is filled by a proliferation of industry-led certification initiatives, which may be primarily motivated by commercial interests and result in less meaningful or beneficial outcomes for end users.

We found that there are already numerous valuable contributions to the field from non-profit projects and national authorities engaged in the development of digital trustmarks, and we believe it would be desirable for the Commission to help coordinate and draw together initiatives, with the larger goal of supporting the Commission's drive towards building a more human-centric internet. The Commission could play a hugely valuable role in streamlining existing approaches, maintaining cohesion, providing legitimacy and driving the scale and effectiveness of a digital trustmark. While not covered in this report, separate yet complementary initiatives could also be introduced that usefully focus attention upstream (as opposed to the trustmark's focus on the end-user), encouraging tech companies to improve practices and develop more responsible tools and technologies

KEY FINDINGS AND RECOMMENDATIONS

Our initial research has identified several key points and potential models for the development of an NGI or digital trustmark:

- Firstly, our research suggests that **a single, comprehensive trustmark** would be more successful than multiple, potentially competing or overlapping initiatives, which would likely lead to consumer confusion. A single point of reference is more likely to become well-known and understood across Europe and beyond. This could be achieved via an **'umbrella' structure** that would balance the consumer's need for a comprehensive trustmark with the organisational and technical need for different metrics for different issues or types of internet tools and products. This umbrella NGI trustmark could act as the overarching brand that consumers recognise as a sign of trustworthiness across all internet tools and technologies. This would have the benefit of giving consumers the same experience across the internet, making the trustmark simple, easy to understand, and widely-recognised.
- A trusted, well resourced and cross European organisation, for example the European Commission, would need to take responsibility for such a trustmark as its success will depend on adequate investment for developed and publicity.
- This trustmark could cover a wider variety of areas but our research suggests that criteria should include developed around **cyber security, privacy and data practices, transparency, bias and inclusive representation, accountability, and sustainability.** As the information related to these areas could become complex or unwieldy, mechanisms such as a traffic light system and route to finding out more granular details (e.g. each website or tool could have a QR code linking to updatable information covering all the relevant areas) could be used. Any criteria used should be supported by existing or future legislation to ensure the trustmark can signal best practice rather than a minimum standard.
- Careful consideration should be given to how a trustmark's criteria might be assessed and audited, its governance framework and financing model. To do this well, a wide variety of stakeholders should be consulted, including companies, citizens and those already developing digital and non-digital trustmarks.

NEXT STEPS

To take these ideas, and the work that has already been done by many different organisations, forward at a European level, the NGI Forward project, led by Nesta, will seek to bring relevant stakeholders together as part of a flagship NGI policy summit in June 2020. This will be an opportunity to further co-develop content and design related trustmark questions, for example: what areas should an NGI trustmark should cover, what kind of criteria should be set and how would this be assessed? We will bring stakeholders together from within and outside the digital space to share learnings as we have sought to do in this report. The aim of these meetings will be to coordinate action, leverage the expertise of a diverse ecosystem and inform decisions taken at an EU level.

Alongside this we recommend that the European Commission agrees to take a leading role in facilitating and shaping the development of an NGI trustmark, sponsoring and championing its development while helping to coordinate action via more formal means such as a dedicated taskforce. This taskforce would need to take the lead on developing a sustainable approach to governing the trustmark.

This report was created by Nesta for NGI Forward, part of the Next Generation Internet initiative, a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N°825652

Websites

https://www.ngi.eu
https://research.ngi.eu

Twitter

https://twitter.com/ngi4eu
https://twitter.com/ngiforward