

CHALLENGES FOR CHANGE

How can Consumers International create positive change for consumers in the digital world?



CONTENTS

PART ONE: CHALLENGES FOR CONSUMERS

ACCESS, INCLUSION AND FREEDOM	7
Sonia Jorge, Executive Director, Alliance for Affordable Internet	7
Gbenga Sesan, Executive Director, Paradigm Initiative	10
PRIVACY, SECURITY AND UBIQUITOUS TECHNOLOGY	13
Robin Wilton, Technical Outreach, Internet Society	13
Gilad Rosner, Founder, IoT Privacy Forum	20
DATA: THE NEW BUSINESS FRONTIER / A NEW FRONTIER FOR BRANDS	24
Colin Strong, Global Head of Behavioural Science, Global IPSOS Mori	24

PART TWO: CREATING CHANGE

A NEW DATA INFRASTRUCTURE	31
Sarah Gold, Founder and CEO, IF by Design	31
MAXIMISING THE IMPACT OF CONSUMER LEGISLATION	35
Christine Riefa, Reader, Brunel University	35
WIDER ENGAGEMENT: CIVIL SOCIETY, INTERNET GOVERNANCE AND BUSINESS SECTOR	41
Andrew Pudephatt, Executive Chair and Charles Bradley, Executive Director, Global Partners Digital	41

AMANDA LONG

DIRECTOR GENERAL, CONSUMERS INTERNATIONAL



**THROUGH
CHALLENGING OUR
OWN THINKING, WE WILL
SPARK THE CONNECTIONS AND
CO-LEARNING THAT WILL LEAD
TO THE EMPOWERMENT OF
CONSUMERS AROUND
THE WORLD**

As part of a strategy review, we wanted to seek out fresh and challenging perspectives. We invited a small number of international experts and opinion formers to produce a challenge piece on how Consumers International, and the global consumer movement, can best respond to the challenges and opportunities facing us in the digital world.

We spoke to individuals from leading digital NGOs, global market and opinion specialists, digital designers and academics and asked them how Consumers International could work with members and partners around the world to create positive change for consumers in the digital world.

We also asked them to constructively challenge us to be more effective, and to think as creatively as they could. These external perspectives have stimulated much debate and have helped to inform future strategy and priorities for action.

We are now publishing the whole set of contributions as a valuable resource for anyone working for positive outcomes in the digital economy and society.

Through challenging our own thinking and that of others, we will continue to spark the connections and co-learning that will lead to the empowerment of consumers around the world.

KEY THEMES

THE CHALLENGE IN CONTEXT

Much of the contributors' responses were shaped by a recognition of the increasing reach of technology into all aspects of our lives as we move towards a world in which technology has a ubiquitous presence in our lives. Rather than interacting with web-based services where we can choose the terms of when and how we engage, we are entering a phase where our entire experience of the world we live in is shaped by digital devices and services.

As more and more devices become internet enabled and can communicate with each other and external data holders, the internet will become a ubiquitous physical environment that is continually collecting, analysing and using personal data to predict our behaviours and shape our lives, in ways we may be oblivious to and are too complex to fully engage with.

But these are not yet challenges for everyone. Despite the world reaching 50% global internet penetration in 2017, almost half the world's population remain offline. As digital technology continues to develop at an incredible pace, digital inequality is expected to widen and those without adequate internet access are at risk of being left behind.

INFLUENCING THE DIGITAL ECONOMY AND SOCIETY

Many contributors commented on how the fast pace of digital innovation forces policymakers to play catch up - reacting to gaps in policy as they are exposed, rather than pre-empting problems before they happen. This is added to by a lack of technological literacy in most policy making circles – including advocates. As digital processes cross borders, the discrepancy in levels of protection against various digital issues has become a major problem.

Between them, the authors also picked up on other issues created by this lack of speed and co-ordination. For example, appropriate responses to more systemic issues like digital privacy are even harder to craft, as multiple stakeholders are motivated by different incentives, and will respond to different interventions. This means cross border approaches to protection and security are required. Others thought the lack of an effective and joined up policy response has meant that large technology companies have become hugely influential in setting trends and common practices that small operators tend to follow.

**CONSUMERS
INTERNATIONAL CAN
USE ITS POSITION TO LEAD
THE WAY IN BUILDING AND
CONNECTING THE PIECES OF
A NEW DIGITAL
INFRASTRUCTURE**



CHALLENGES TO CONSUMER ORGANISATIONS

There were calls for a much broader concept of 'consumer' than consumer organisations might currently work with, moving beyond traditional consumer issues such as 'does this product or service work as expected?' and towards a wider consideration of the role consumers play in the business models of tech companies and the value their data generates.

And technical knowledge must be improved. In an interconnected and highly digitalised world, issues such as cybersecurity, data protection, and data ethics are beginning to dominate the global policy agenda. Consumer organisations will need to develop a more informed understanding of these trends and establish new partnerships to continue to influence and shape policy.

But as well as thinking about future work, there was a challenge from some not to forget the fundamentals which are still not adequately covered, for example doing more to educate and raise awareness on the privacy implications of targeted advertising. Most thought it was still essential to continue to lobby for strong consumer protection, mobilise consumers to demand high levels of protection, and to use things like the ambitious European General Data Protection Regulation as a way to raise the base level of consumers rights across the world.

As well as working with legislators and international processes, the importance of an open dialogue with businesses was stressed by many.

MAKING THE MOST OF OUR GLOBAL REACH

Everyone thought collaboration with other stakeholders was key to developing a more in-depth and nuanced understanding of technology and finding the best solutions to the problems consumers face in the digital world.

A diverse selection of stakeholders was mentioned, with some recommending being open to engaging in new conversations and more constructive debates with businesses on things like data privacy – showing that services can champion privacy without compromising user experience. Others suggested working with developers to use the power of technology to solve consumer problems, for example developing digital applications that can detect unfair practice or using online platforms to build closer relationships with consumers.

Others focused more on making the most of our global reach, balanced out by a clear understanding of local approaches and actions, and supporting local, country-based coalitions with stakeholders from private industry, the public sector, and civil society. And, for consumers in countries that need more access, the new trend witnessed in many authoritarian states of shutdowns or network disruption must be urgently addressed as a both a consumer and a citizen issue.

A digital design specialist felt we could use our position at the heart of the consumer advocacy community, to lead the way in building and connecting the pieces of a new digital infrastructure.

**COLLABORATION
WITH OTHER
STAKEHOLDERS WILL BE KEY
TO FINDING THE BEST
SOLUTIONS TO THE PROBLEMS
CONSUMERS FACE IN THE
DIGITAL WORLD**

PART ONE: **CHALLENGES** **FOR CONSUMERS**

**WE ARE ENTERING A
PHASE WHERE OUR
ENTIRE EXPERIENCE OF THE
WORLD WE LIVE IN IS SHAPED
BY DIGITAL DEVICES AND
SERVICES**



ACCESS, INCLUSION AND FREEDOM

**EXECUTIVE DIRECTOR, ALLIANCE FOR AFFORDABLE INTERNET
HEAD OF DIGITAL INCLUSION PROGRAMMES, WEB FOUNDATION
SONIA JORGE**

The Alliance for Affordable Internet (A4AI) is a broad coalition working to enable everyone, everywhere to access the life-changing power of the Internet

Web Foundation is an independent, international organisation fighting for digital equality – a world where everyone can access the web and use it to improve their lives



Sonia N. Jorge is an expert in the confluence of development and communications policy. She has over 25 years of diverse international experience in a career spanning both the private and not-for-profit sectors.

Her work has included ICT policy and regulatory advice and analysis, strategic industry planning, national ICT/ broadband policy development, and the creation of new legal and regulatory frameworks to address issues around competition, cost-based pricing, spectrum management, and infrastructure development and sharing. Sonia is an avid advocate of gender equality in development, and has worked extensively to promote gender analysis and awareness in the ICT planning process, as well as an

understanding of the importance of universal access and digital inclusion for development.

She serves as a member and expert in a number of Committees, including the DFID's Digital Access Panel for Africa, the ITU-UN Women EQUALS Initiative, The World Economic Forum's Future of the Internet Initiative, the Broadband Commission Working Group on the Gender Digital Divide, and the Advisory Committee on International Communications and Information Policy (ACICIP) Subcommittee of the US State Department on ICT4D.

Having been a partner of Consumers International for some time now, the Alliance for Affordable Internet (A4AI) and the Web foundation see our growing partnership as critical in the journey to ensure that **Digital Equality - a world where everyone has the same rights and opportunities online** - becomes a reality. We also believe that by putting people, and consumers in general, at the center of policy making processes, we are a step ahead in ensuring that policy focuses on securing consumer rights and opportunities in a digital ecosystem designed by and for the people.

Yet, as the digital revolution marches forward, billions are being left behind. This digital divide falls along gender and income lines – women and the poor comprise the majority of those offline today. These populations are often already marginalised offline and, as a result, arguably stand the most to benefit from the opportunities associated with online access; instead, they are now seeing these offline inequalities replicated online. While internet access has the power to upend this balance of power, today's digital exclusion is instead reinforcing existing patterns of privilege... and discrimination.

Consumers International's motto of 'Coming together for Change' speaks directly to A4AI and the Web Foundation's belief in the strength of multi-stakeholder coalition processes as the foundation for policy change. Collectively, we have a responsibility to advance the digital rights of citizens while remaining focused on policy change that advances affordable and equal access to all, specially to those traditionally marginalized, unconnected and unprotected as consumers.

I would like to suggest that we focus on women, since they particularly feel the impact of this digital divide. Over half of today's offline population are women – this means that more than 2 billion women globally are not connected, unable to access health, educational, and other resources and information available online.



Web Foundation research has found that women in poor, urban areas are up to 50% less likely to be online than men in the same communities and once online, women are 30-50% less likely than men to use the Internet to increase their income or participate in public life.

**AS THE DIGITAL
REVOLUTION MARCHES
FORWARD, BILLIONS ARE
BEING LEFT BEHIND. THIS
DIGITAL DIVIDE FALLS
ALONG GENDER AND
INCOME LINES.**

So, I challenge Consumers International to mobilize, engage and support its members to come together for change by focusing on marginalized and unprotected consumers, with a special focus on women and the poor. Without efforts to enable opportunities for access and use that focus specifically on women and other offline populations, we risk entrenching current inequalities and contributing to a more unbalanced and unequal world.

At A4AI and the Web Foundation, we believe in the power of developing local solutions to local problems. For this reason, we aim to empower our local, country-based coalitions – which are composed of national stakeholders from private industry, the public sector, and civil society – to develop and advocate for the best solutions for overcoming these issues. Consumers International and its members must be part of these processes, and must support new ones to advocate for and advance consumer's rights in the digital age.

The fight for digital rights must continue – and perhaps becomes even more critical – once people are online. As more and more of our daily lives move online, we each leave a massive data trail in our wake. Most of us do not know what digital trails we are creating, who has collected them or what they will be used for. Companies rely on this data to personalise services and target ads that will be most relevant to users, but this collection of data can also lead to unintended consequences when we are profiled in ways that are detrimental to our interests, or when governments around the world take advantage of our digital trails to extend the state surveillance apparatus to unprecedented levels.

We the people, consumers of digital technology, have a right to know what is collected about us and what it will be

used for. And we have a right to transparent explanations of how our personal data is processed, sold, and used to make decisions for and about us. All of us — government and public sector policymakers, tech companies and service providers, activists and civil society — must come together to develop policy and regulatory frameworks that protect us online, and which put a fair level of control back into the hands of the people.

It is up to us to ensure that the digital revolution becomes a movement that empowers all. Failure to act means leaving billions behind; it means eroding consumer trust — a core foundation upon which the digital economy is built.

For us collectively, this means working not only to expand affordable access to everyone, everywhere, but also to ensure that the web remains truly open so that once people come online, they have the opportunity to access and use the information and tools needed to participate fully in civic life. Consumers International's leadership, engagement and partnership is critical to achieve these goals and I urge you to grow and strengthen your networks to reclaim consumer trust in the digital economy. We look forward to continuing to work with you and your members throughout the world to achieve Digital Equality!

**IT IS UP TO US
TO ENSURE THAT THE
DIGITAL REVOLUTION
BECOMES A MOVEMENT
THAT EMPOWERS ALL.
FAILURE TO ACT MEANS
LEAVING BILLIONS
BEHIND.**



EXECUTIVE DIRECTOR, PARADIGM INITIATIVE 'GBENGA SESAN



Paradigm Initiative is a social enterprise that builds an ICT-enabled support system and advocates digital rights in order to improve livelihoods for under-served youth

'**Gbenga Sesan** is the Executive Director of Paradigm Initiative. Originally trained as an Electronic & Electrical Engineer at Obafemi Awolowo University, 'Gbenga completed Executive Education programs at Lagos Business School, New York Group for Technology Transfer, Oxford University, Harvard University, Stanford University, Santa Clara University and University of the Pacific. His consulting experience includes assignments completed for Microsoft, Harvard University and United Nations agencies, among others, in over 30 countries.

A Schwab Foundation Social Entrepreneur of the Year (2014) and former member of the United Nations Committee of eLeaders on Youth and ICT, he is a Fellow at several high-profile institutions. 'Gbenga was listed by CNN as one of the Top 10 African Tech Voices on Twitter and by Ventures Africa as one of 40 African Legends Under 40.

If anyone got a dollar each time someone said, “*technology has changed everything*” or “*the future is digital*,” they would be billionaires by now. For producers and consumers, improvements are reported – and experienced – daily. There is also an opportunity for exposure to options, thanks to connected mobile devices that are now available to 66% of the world’s population¹. Beyond their place in statistics, are consumers better today, in the digital age, given the many opportunities for improvement though? Beyond being the target of advertising, how can consumers and organisations that support their interest, get a better deal in the digital world? In 2018 alone, Statista² projects that \$269.85B will be spent wooing consumers; will they – we – get commensurate benefits?

Let me start with this: we must kill assumptions. In the years preceding the arrival of mobile phones in Nigeria, a policymaker was quoted as saying that “*telephones are not for the poor*” and though he has since accused the media of misquoting his original “*poor people don’t own phones*” statement, it is still as bad. One of the things that we must change in the digital world is this premise that has defined many consumer experiences. When we assume that the “*poor*” either cannot pay, or that they need a different type of experience that relives the “*half a loaf is better than none*” mantra, we limit the opportunity for that now-connected consumer to decide what is useful and then prioritise towards the adoption of products or services.

Less than two decades later, Nigeria now has more than 142 million mobile phones³, and even if multiple device ownership is considered, the final adoption numbers defeat the assumption that “*poor people don’t own phones*”. Almost 95 million of these mobile phones are connected to the internet and these consumers, in Nigeria and beyond, are increasingly connected to exposure opportunities that have led to acquired sophistication – and introduced new opportunities for engagement between consumers, producers and anyone else in the product ecosystem. For example, social media rants are the new consumer feedback, and this provides a unique opportunity for feedback monitoring even before the consumer goes through the perceived (or real) stress of contacting support.

Given these opportunities, we must go ahead to remove the silent “*but*” after the popular phrase, “*consumer – or customer – is king*.” The but may be replaced by because, giving reasons why consumer experience must become better in a digital world. For example, a consumer that trusts a service because the provider will not violate their digital rights is likely to add more value to the company’s bottom-line than another customer who only remains an advert target. The famous story of the lone passenger of

a Japanese train station is a great example of consumer consciousness by a service provider: a defunct train station was kept open so a teenage girl could commute to school daily⁴. Even though she has now graduated and the station is finally closed, the station remains an example that many consumers will use as benchmark for services they subscribe to.

The equivalent of the Japanese train station in the digital world would be a company that insists on protecting the rights of its consumers even when it does not appear to make sense at first. On the surface, the defunct train station had no business being in business but the goodwill generated from what is now seen as an act of kindness will help the parent company. When next a government requests that a service provider should either deny a contractual service – as has been the case in countries that have experienced digital rights violations such as internet shutdowns – the companies should not take the easy road. Scenarios vary from complex to very complex but service providers should not easily give up on consumers; they must look for what could be complex solutions that serve as many interests, with as little negative impact, as possible.



**BEYOND BEING
THE TARGET OF
ADVERTISING, HOW CAN
CONSUMERS AND
ORGANISATIONS THAT SUPPORT
THEIR INTEREST, GET A
BETTER DEAL IN THE
DIGITAL WORLD?**

Consumers International’s work, with members and partners around the world, can help create positive change for consumers in the digital world. One of such positive changes is around digital rights. Given the role played by telecommunications companies in countries where citizens are denied access to the internet, and building on its work to “*ensure consumers are treated safely, fairly and honestly*,” Consumers International could

1 ‘Digital in 2017: Global Overview’, Simon Kemp, We are Social, 24/01/17

2 Statista, Digital Advertising Spending Worldwide from 2015 to 2020, <https://wearesocial.com/special-reports/digital-in-2017-global-overview>

3 Nigeria Communications Commission, Monthly Subscriber Data, <https://ncc.gov.ng/stakeholder/statistics-reports/subscriber-data>

4 ‘A Bittersweet Ending for a Japanese Train Station and Its Lone Passenger’, Linda Poon, CityLab, March 28/03/16

work with the mobile sector to build the case for the respect of digital rights and how it is great for the bottom-line. Unfortunately, the countries experiencing the worst digital rights violations are also those on the disadvantaged end of the digital divide – a gulf that is actually deepening. The 2017 edition of the State of Broadband report features ITU estimates showing that “internet penetration in the developing world is projected to reach 41.3% by the end of 2017, while internet user penetration is projected to reach only 17.5% in Least Developed Countries in 2017.”¹

In the 2017 edition of the Digital Rights in Africa report featuring 21 African nations, Paradigm Initiative discussed the trend of network disruptions – including outright internet shutdowns – and recommends that, given the likelihood of the repeat of 2016 and 2017 violations because of elections being held in various countries in 2018, “a viable route to at least reduce the incidents of internet shutdowns in Africa, and stemming digital rights abuses, may be through partnership with internet businesses. Telcos, ISPs, social networking platforms, content producers and all other internet businesses must take on a greater and more visible role if governments in Africa are to take digital rights seriously.”²

For consumers in countries that need more access, this new trend of consumer rights violations poses a threat that must be urgently addressed by stakeholders – businesses, government, private sector and international organisations.

THE COUNTRIES EXPERIENCING THE WORST DIGITAL RIGHTS VIOLATIONS ARE THOSE ON THE DISADVANTAGED END OF THE DIGITAL DIVIDE – A GULF THAT IS ACTUALLY DEEPENING



1 Broadband Commission, 'The State of Broadband 2017: Broadband Catalyzing Sustainable Development', 2017
2 Paradigm Initiative, 'Digital Rights in Africa Report 2017: 'Good for Business: Why Private Sector Must Work With Citizens, Civil Society for Digital Rights', 2017.

PRIVACY, SECURITY AND UBIQUITOUS TECHNOLOGY

TECHNICAL OUTREACH (IDENTITY & PRIVACY), INTERNET SOCIETY ROBIN WILTON



The Internet Society advances the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society.

Since 2001, **Robin Wilton** has specialised in digital identity, privacy and public policy, building a reputation as a thought-leader, communicator and translator between different stakeholder groups.

Before joining the Internet Society, Robin spent two years as a research analyst in Gartner's Identity and Privacy Strategies team, where in addition to his privacy work he specialised in public key infrastructure, electronic signature, single sign-on and federated identity.

Robin's experience includes: 12 years with IBM in systems engineering, technical support and consulting roles, at the UK and EMEA level; three years as Principal Consultant at JCP Trustbase Ltd, a start-up specialising in Java cryptography and PKI-enabling middleware; eight years with Sun Microsystems in technical pre-sales and the CTO team; 18 months establishing Future Identity Ltd. as an independent consultancy on privacy and digital identity. During his time at Future Identity he was also Director of Privacy and Public Policy for the Kantara Initiative.

To create positive change for consumers we need to look at two things; ethics and habits, as well as how we think about digital privacy.

WHAT'S THE DIGITAL PRIVACY PROBLEM?

A few weeks ago, preparing for a conference panel, I was asking people what they thought the problem was with digital privacy, from the consumer perspective. One person, after a little thought, replied that their experience of the privacy problem had gone through four phases:

- "I wasn't aware there's a problem."
- "OK, I see there's a problem, but why should I care?"
- "I care, but I don't know what I can do about it."
- "I tried to do something about my privacy, and now my browser/email/app doesn't work."

There is a model for this kind of experience: how people come to make decisions, and how those decisions turn into habits (or not). It is rather grandly called the 'transtheoretical model of behaviour change' – but it's a useful thing, despite the name, and we'll come back to it later.

The fourth phase is the point at which our attempts to improve privacy outcomes frequently break down. At that point, as a technologist, I'm often asked why there isn't some technical widget – an app, a browser plug-in, a black box – that can take care of a user's privacy on their behalf. The question is usually tinged with a degree of frustration.

I can sympathise with both the question and the frustration. After all, we can look back on some 30 years of data protection law, much of it based on the OECD's Guidelines governing the protection of privacy and transborder flows of personal data, which were adopted in September 1980. Those Guidelines, like the Council of Europe's Convention 108 of 1981, and the EU's Data Protection Directive of 1995, are long-standing enough to have matured and gone through at least one cycle of substantial review and renewal.

And yet, when we look at individuals' general experience of privacy and data protection, the outcomes don't appear to reflect either that maturity, or the effectiveness of the revised and updated guidance. Here are some of the common symptoms:

- Unexpected or excessive collection of personal data
- Insufficient care taken with its storage/use, leading to data breaches and inappropriate access
- Unexpected or unwelcome use
- Unexpected sharing

Individuals' expectations concerning their personal data are at odds with what actually happens - but why is there this misalignment? One answer I've been given is that "technology changes too fast; people just can't keep up, so their expectations lag behind reality". I'm not sure I buy that. After all, people seem to be adjusting fairly readily to the use of new technology; for instance, I've seen toddlers perfectly at ease with the user experience presented to them by a tablet computer, as is my 90-year-old mother.

Is the answer, perhaps, that the user experience gets a lot more design attention than the privacy experience? Possibly – and that's certainly the thinking behind the concept of 'privacy-by-design': to try and ensure that the privacy-related aspects of a product or service get as much attention as the rest of its design, and from as early as possible in the development process. But if that's the case, why is privacy is so slow to gain traction as a competitive differentiator? Technology products that make privacy a unique selling point such as Silent Circle's "Blackphone" handsets or Purism's laptops still seem to find favour with only a niche segment of the market, and that segment is often derided by other consumers as the 'tin-foil hat brigade'.¹² I know. I'm a card-carrying member of it, and even some of my colleagues can't understand why I get so concerned about potential privacy risks. So, the problem may be one of product design, but privacy-enhancing technologies still need to find the key to making usable privacy a 'must have' feature, rather than a 'why bother?'.

Privacy-by-design has to address a further design challenge, too. As an example here, think of a browser plug-in that alerts you every time a website tries to set a cookie. It probably wouldn't take long for most users to get bored and frustrated by constant warnings, and either ignore them, or disable the warning mechanism. Expose the function to the user in the wrong way, and no

**THE DIGITAL PRIVACY
PROBLEM IS HARD, NOT
BECAUSE IT IS COMPLICATED,
BUT BECAUSE IT IS
SYSTEMIC**

1 Silent Circle's "Blackphone" handsets website, <https://www.silentcircle.com/>

2 Purism's laptops website, <https://puri.sm/>

matter how worthy it is, they may reject it. However, at the other end of the scale, there's also a risk in shielding users too effectively from the complexities of what is being done on their behalf. Hide the function from the user completely, and they lose all awareness of what is happening – we don't want that outcome, either.

The ideal approach is to present these user-supportive functions in ways that increase comprehension and encourage adoption, rather than the reverse. This, too, relates to the behavioural model I referred to earlier, and to which I will return later.

And then there's the question of what happens to users' personal data when it is in the hands of third parties. So much of what happens on the Internet is driven by a powerful economic engine fuelled, in turn, by the monetisation of personal data. I have often heard monetization described as "the reason you can have free stuff, and cool innovation". The questions this raises for me are:

- Is that the only economic model available, or just the one with the greatest momentum?
- Is my privacy a fair price to pay for cool apps and free content?
- If I am paying for an app or service, or paying not to receive advertisements, does that guarantee that my data isn't being monetised?

In short, am I getting an honest bargain, and if not, how can I, as an individual, redress the balance between me and a multi-billion dollar corporation?

To recap, briefly: the problem of digital privacy involves elements of user awareness and choice; regulation and its effectiveness; technology design and adoption; data monetisation as an economic force... and that persistent mismatch between users' expectations and their experience.

ARE WE LOOKING AT THE PROBLEM IN THE RIGHT WAY?

As I noted above, individuals' reaction to the privacy problem is often accompanied by some frustration – and frankly, as a privacy advocate, so is mine. It often feels as though promising privacy-protecting efforts come to nothing, fizzle out without achieving critical mass, or fail to shift the behaviour of the market.

My theory is that this is not because the digital privacy problem is particularly complicated - or even particularly new, in some respects. After all, intermediaries have been collecting and monetising data about me since before the Internet. Rather, I think the digital privacy problem is hard because it's systemic. Multiple stakeholders are involved, many with differing motivations and sometimes conflicting interests; the influences that would change one stakeholder's behaviour won't work on some of the others, and the influences that work at one point in time may fail



at another. The best way to change how we think about solving the problem is to change how we think about the problem. I packed a lot into this paragraph, so let's look at some specific examples, to make it less abstract.

First, what might motivate, say, the vendor of a connected object such as a smart light bulb? Probably, selling at a compelling price, achieving mass adoption, and maximising profit. Those motivations might lead to the following actions:

- **Do as much as possible to minimise design/ manufacturing cost**
 - If the cost of adding security or privacy functions doubles the price of your smart light bulb, relative to the competition, it might not sell.
- **Sell on user functionality, not on vendor functionality**
 - The user benefit is, say, the ability to control the lighting from your phone. The vendor functionality might include collection of data about usage patterns – but that isn't necessarily a compelling incentive for user adoption, so don't mention it.
- **Increase your margins by monetising the data you collect about usage patterns, and the inferences you can draw from that data.**

I may be caricaturing slightly, here, but I think these are elements we can all see, to some extent, in the products and services offered to us in our connected lives. For a detailed examination of these issues, backed up by numerous case studies, I can recommend 'Networks of Control', by Wolfie Christl and Sarah Spiekermann of the Vienna University of Economics and Business.³

There are also elements, in my hypothetical example, of what economists call 'negative externalities'. That is: the vendor gets the benefits of data monetisation, while the

3 Cracked Labs Website, <http://crackedlabs.org/en/networksofcontrol>

costs and risks associated with it fall on someone else (the consumer). For example, if the vendor suffers a data breach, and the personal data it has collected is abused, the resulting cost and harm fall on the consumer. Troy Hunt, a trainer and data breach consultant, has blogged recently about several worrying instances involving products aimed specifically at children.¹

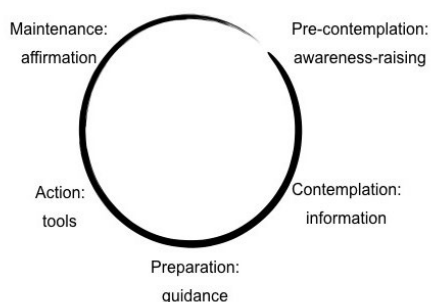
In an ideal world, some cost might return to the vendor in the form of legal penalties. However, the risk of that happening does not, currently, seem to influence vendor behaviour significantly in many jurisdictions - and particularly, when the hacking/abuse happens in a different jurisdiction from the vendor.

The topic of data breaches is one which the Internet Society examined in detail in its Global Internet Report for 2016, looking particularly at the economic factors and making five recommendations to build online trust.² In summary, those are:

1. Put users at the centre of solutions; include externalities in the cost/benefit analysis.
2. Increase transparency through data breach notifications and disclosure.
3. Make data security must be a priority.
4. Make organisations should be accountable for their breaches.
5. Stimulate the market for independent security accreditation services.

Second, I want to return to the 'transtheoretical model' I mentioned earlier. According to this model, people go through a number of stages in the course of making decisions. Good, clear explanations of the model can be found online, but this diagram gives a high-level summary:³

Nudge by nudge...



USER ACTION ALONE IS UNLIKELY TO SUFFICE, BECAUSE OF THE POWERFUL NATURE OF THE ECONOMIC INFLUENCES THAT DRIVE SO MUCH INTERNET-RELATED COMMERCIAL ACTIVITY

According to the model, repeated iterations through this cycle can result in the formation of habits (whether good or bad); so, if we want to encourage consumers to form 'better' privacy habits, it should be useful to understand the formative process. What the model made clear to me was that, at each stage, the kind of intervention likely to succeed is different.

Think back to the first answer I got in the conversation I relayed at the beginning of this paper: "I wasn't aware there's a problem". That's the 'pre-contemplative' phase... I'm not even thinking about the problem, because I'm not aware of it. At that point, something has to make the individual aware of the problem.

Once they are aware of it, their next concern may be to find out if it's relevant to them: "OK, I see there's a problem, but why should I care?". At that point, they really want a binary answer: should I worry about this, yes or no?

At the next stage, though, a simple yes or no isn't enough: "I care, but I don't know what I can do about it." Better outcomes depend on more information.

1 'Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages', Troy Hunt's blog, 28/02/2017
 2 'Internet Society's Global Internet Report for 2016', The Internet Society, 2016
 3 Study.com website; Transtheoretical model, <http://study.com/academy/lesson/transtheoretical-model-definition-stages-of-change.html>

So, even for these three 'informational' stages, we can see that different kinds of intervention are needed, if we are to respond to the individual's needs:

1. A compelling event that raises awareness of the problem
2. A quick, simple indication of its relevance to the individual and the need for action
3. Easy access to more information about what to do

The fourth answer I got was the point at which it all went wrong for the individual I was talking to. The model describes this as the 'Action' phase. The individual tried to fix the problem, only to find that the 'fix' broke their technology. This is the stage at which we are often inclined to expect some kind of technical widget to fix the problem, with greater or lesser success. We can also surmise that, if there is a working technical fix, but users aren't aware of the problem, or don't think it affects them, or don't know what to do about it, the technology is unlikely to see adoption. In other words, the 'action' phase can fail in numerous ways.

The final stage of the model is the 'Maintenance' phase. Here, the user's experience so far will influence whether or not they make the same choices next time they encounter the problem. Over time, whatever reinforcement they experience here (positive or negative) can lead to the formation of habit. So, for instance, if I make unhealthy eating choices but experience gratification in the 'maintenance' phase, and don't immediately keel over with a heart attack, I may well develop long-term bad eating habits, though in due course I may end up with furred arteries. Similarly, if I make poor privacy choices, experience gratification, and appear to suffer no ill consequences, I may continue with privacy-eroding habits until it's too late to repair the damage.

Part of the issue here is about the deferred consequences of poor privacy habits. The negative results of privacy-eroding behaviour are often remote, in time and place, from the action that caused them, so we tend not to 'learn the lesson'. By contrast, if I put my hand over a candle, I get negative feedback which I immediately associate with putting my hand in the flame, and I quickly form a habit of not doing so.

To recap: Habits develop as a result of an iterative decision-making cycle. To influence the formation of habits, we need to be able to intervene successfully in different ways, depending on the phase the individual has reached. Intervention at one phase may fail because it is poorly conceived (a technical 'fix' that breaks the user experience), or it may fail because previous phases have not been successfully addressed.



RECOMMENDATIONS FOR A NEW APPROACH

The digital privacy problem is hard, not because it is complicated, but because it is systemic. Different stakeholders have different incentives and will respond to different interventions. In the case of user motivations, there is a plausible model for how behavioural change takes place, and that model suggests that we should expect to intervene in different ways at different stages, if users are to develop awareness, motivation, capability, and privacy-enhancing habits.

However, user action alone is unlikely to suffice, because of the powerful nature of the economic influences that drive so much Internet-related commercial activity. Where market forces can be influenced, we should design the interventions that are likely to increase service providers' incentive to enhance privacy. Where market forces will predictably fail, there is a case to be made for regulatory intervention.

As noted earlier, this is a systemic problem - so the over-all approach should be prepared to apply different interventions to different stakeholders at different points in the process.

CHANGING STAKEHOLDERS' BEHAVIOUR

A key element of the Internet Society's proposed approach is to try to align the interests of consumers and service providers. We suggest that one way to do this is through the creation of a 'trust mark' that represents an organisation's commitment to ethical data-handling principles. Those principles, in turn, would reflect a set of policies and procedures that govern the organisation's collection and use of personal data. The organisation's entitlement to display the trust mark would be confirmed by an accreditation step and could then be monitored through external audit.

We believe this would give some service providers an incentive to distinguish themselves from the rest of the market, in much the same way as Fairtrade vendors do in the retail market. By analogy, the measure of success for a trust mark would not necessarily be 100% adoption by every vendor, but rather, the general shift in the market that results from consumers being aware of more ethical alternatives to existing products and services.

We would expect trust-marked services to perceive a competitive advantage based on improved user trust - a concept which is explored in a set of over 50 case studies, assembled in 2016 by Gary Hasselbalch and Pernille Tranberg.¹ Depending on the regulatory environment, organisations able to show compliance with the trust-mark criteria might also perceive some form of regulatory benefit (a "safe harbor", in US terms).

In terms of user behaviour, the trust-mark approach fits well with the transtheoretical model. The trust mark itself serves as the simple, binary signal (or perhaps a three-

value 'traffic light' model) that gives the consumer an instant indication of a service provider's privacy stance. The underlying principles would give further information in support of the consumer's decision, and ultimately, an organisation's accreditation and audit status could be open to inspection. Over all, it is conceivable that the increased transparency associated with trust-marked products would increase pressure on competitors to be more explicit about their own business models, or risk losing trust because of the implied inferiority of their offering.

Designers and vendors would have an incentive to respond to any general shift in the market, generated by adoption of trust-marked alternatives, by improving the privacy design of their offerings. A similar trust mark model could, we believe, also be applied to apps (a privacy score, linked to more information about the permissions the app requests, the data it collects, and any back-end processing), and to connected objects (a score linked to more information about what data the object collects/generates, where it sends it, and what processing is done in the 'cloud'). The Internet Society's Global Internet Report (GIR) for 2016 discusses the role played by trust marks and similar 'credible signals' in establishing and reinforcing service providers' credibility. The GIR does this in the context of the economics of online security, but we believe there are direct parallels with the trust and privacy case.⁵

However, this does still leave at least one gap in the picture, concerning the transtheoretical model: what interventions are possible for the 'maintenance' phase of the cycle? What positive reinforcement can we achieve for users who are on track to develop positive privacy habits? Could it be turned into a game, for example, much as the "Cheevos" plug-in does for privacy features in Mozilla's Firefox browser?²

There is an alternative form of reinforcement, based on principles I heard about from the Design Thinking labs at Stanford University. In their experience, based particularly on projects to do with food labelling and healthy eating, was that the most effective approach is to influence the values that users apply to the decisions they make. Let's take donuts as an example. If you present the choice simply as 'have a donut or don't have a donut', the chooser has an 'instant gratification' incentive to take a donut, and (as remarked earlier) probably no instant heart attack to persuade them otherwise. However, if you present the choice as 'have a donut, or have an apple and live a longer and healthier life', you change the values the chooser applies to the decision.

**ONE REASON IT
CAN BE HARD TO
SENSITIZE PEOPLE TO
PRIVACY RISK IS THAT
PRIVACY-ERODING BEHAVIOUR
OFTEN APPEARS TO HAVE
LITTLE OR NO ADVERSE
EFFECT AT THE TIME**

1 G Hasselbalch and P Tranberg, Data Ethics – The New Competitive Advantage 24/09/2016

2 "Cheevos" Firefox add-on website, <https://addons.mozilla.org/en-US/firefox/addon/cheevos/>

The Stanford labs found that this approach is more likely to result in sustained behavioural change. Fortunately, this too can be fitted into the transtheoretical model, at the informational phases of the decision-making cycle. One reason it can be hard to sensitize people to privacy risk is that privacy-eroding behaviour often appears to have little or no adverse effect at the time, and this can result in a dangerously low assessment of the risk of continuing. By analogy, it's not the first donut that fatally clogs the arteries, so we might persist with this potentially damaging behaviour until it produces serious physical symptoms, at which point much of the damage may already have been done.

In practical terms, this means that when we make those 'informational' interventions in the decision-making cycle, we need to do so in ways that are directed more towards influencing the values the individual applies to the decision, and less towards the possible consequences of that single act. So, for instance, we might frame the decision in terms of its long-term effect on the individual's credit rating, or the intimacy of the profile the service provider can build. It may be important to find ways of showing the disparity between, say, the trivial nature of the service and the intimate nature of the behavioural profile it creates. Making such disparities visible to the user may help them make their decisions less in terms of immediate convenience, and more in terms of their personal, long-term values.

WHERE MARKET FORCES WILL PREDICTABLY FAIL, THERE IS A CASE TO BE MADE FOR REGULATORY INTERVENTION.



FOUNDER, INTERNET OF THINGS PRIVACY FORUM

DR GILAD ROSNER



Internet of Things Privacy Forum is a nonprofit think/do tank promoting privacy values and responsible innovation in the Internet of Things

Dr. Gilad Rosner is a privacy and information policy researcher and the founder of the non-profit Internet of Things Privacy Forum, a crossroads for industry, regulators, academics, government and privacy advocates to discuss the privacy challenges of the Internet of Things. Dr. Rosner's broader work focuses on the IoT, identity management, US & EU privacy and data protection regimes, and online trust. His research has been used by the UK House of Commons Science and Technology Committee report on the Responsible Use of Data and he is a featured expert on O'Reilly and the BBC.

Dr. Rosner has a 20-year career in IT, having worked with identity management technology, digital media, automation and telecommunications. Dr. Rosner is a member of the UK Cabinet Office Privacy and Consumer Advisory Group, which provides independent analysis and guidance on Government digital initiatives, and also sits on the British Computer Society Identity Assurance Working Group, focused on internet identity governance.

The new motto of Consumers International, 'Coming together for change', is for me most valuable in the sense of forming a bloc with other like-minded organisations and individuals. I am in favour of an adversarial approach to the forces that place consumer welfare in a subordinate position to ideas like 'innovation' and 'progress.' There is a pernicious orthodoxy that strong support of privacy, data protection, and regulation generally are in opposition to innovation. This sound bite-sized idea ultimately serves entrenched economic interest at the expense of citizen welfare and economic justice. So, I encourage you to unite with your fellow advocacy organisations to press for change in the following areas pertinent to the digital economy:

WORK TOWARDS EUROPEANISATION

With regard to data protection, the most important development in the world is the rollout of the General Data Protection Regulation (GDPR), Europe's update of the 1995 Data Protection Directive. While not radical, its improvements on the prior European data protection regime are significant. The GDPR seeks not only to improve the state of consent in digital interactions, but also force companies to take a much closer look at the nature of their operations that impact personal data.

Further, the GDPR intends to reach beyond Europe and affect companies outside the EU who process the personal data of Europeans, threatening those who mishandle such data with significant monetary penalties. Importantly, the GDPR creates private and class rights of action – meaning the ability for individuals and classes to sue companies for mishandling of personal data. The combination of rights to sue and significant fines makes the GDPR the most ambitious data protection regime in the world, and therefore one of the more important developments with regard to consumer rights and protections online.

Another major European initiative that directly affects the rights of consumers online is the Digital Single Market (DSM), which seeks to harmonize and streamline a wide variety of online regimes, markets and activities. Key goals are:

- harmonized and improved e-commerce
- affordable, high quality cross-border parcel delivery
- dismantling of geo-blocking of content and purchasing
- harmonized copyright regime
- reducing cross-border VAT compliance costs
- a general bias towards a free flow of data except for privacy and data protection needs

Elements of the strategy can already be seen in the abolition of mobile phone roaming charges within EU member states and forthcoming removal of content blocking based on location.¹

The DSM and the GDPR are the yin and yang of consumer improvement and protection efforts in Europe. They exemplify the power, direction and intent of a European Union, and therefore imply that the broad concept of Europeanisation is beneficial to the citizens and residents of the EU. Consumers International should work with agencies, directorates, and organizations that support and enhance the DSM and GDPR, and generally support stronger unification of Europe and its institutions. While Brexit complicates this, Consumers International's partners and members in EU member states are in a position to contribute to Europe's 'ever closer union'.

ENCOURAGE DATA BREACH NOTIFICATION; PARTNER WITH ONLINE RIGHTS GROUPS

One regulatory strategy that can have a broad effect on digital markets is data breach notification. Simply put, these are requirements for companies to notify regulators and the public when they've had a breach of personal data due to hacking, cybercrime or accident. This is a naming and shaming strategy, and it both causes regulators to question victim companies about their security practices, and makes them vulnerable to market punishments by potentially causing customers to 'vote with their wallets' and take their business elsewhere.

Data breach notification requirement is a straightforward, institutionally-derived market shaping strategy that has general application to all businesses that deal in personal data. It is one small piece of a rising tide that can raise all ships – the goal being general improvement of the cybersecurity landscape, which ultimately benefits consumers by reducing the risk of their personal data being stolen. Fortunately, the GDPR strengthens data

**WITH REGARD
TO DATA PROTECTION,
THE MOST IMPORTANT
DEVELOPMENT IN THE WORLD
IS THE ROLLOUT OF THE
GENERAL DATA PROTECTION
REGULATION (GDPR)**

1 European Commission, [European Commission Digital Single Market factsheet](#), , 2016

breach notification in Europe. But, such requirements are weaker elsewhere in the world, such as the United States, Asia, South America and Africa.² Consumers International should partner with organisations and academics that champion data breach notification in non-European nations as a part of a general online advocacy strategy.

HIGHLIGHT PRICE DISCRIMINATION; BUILD DISCOURSE, CONTRIBUTE TO DETECTION EFFORTS

Within the privacy and consumer protection community, there is a growing awareness of the potential harms of online price personalisation. While shaping the price of goods and services based on a variety of conditions is a well-established element of commerce, there is a danger for pricing to become discriminatory. For example, there is evidence of [Mac users being shown higher prices for goods and hotels than PC users](#).³

Due to the opacity of this ‘price steering,’ it is very hard to determine if, for example, women, older adults or minorities are inappropriately shown different prices based on those factors. A central issue is the difficulty of detecting such price discrimination – there is a limited amount of research on this, as well as only a small amount of popular discussion. Consumers International should discuss this topic with its partners and members and support any existing efforts they may have undertaken.

Consumers International should track price discrimination in the news and in privacy and consumer protection circles to stay abreast of new detection and research. Possible partners include the Information Commissioner’s Office (ICO), the Norwegian Consumer Council (Forbrukerrådet), The European Consumer Organisation (BEUC), and the data protection authority for the German state of Schleswig-Holstein (the ULD). At this stage, it’s important to build popular and professional discourse around this topic so as to support further research and regulatory efforts.

INVESTIGATE AND CHAMPION CHILDREN’S ONLINE PRIVACY AND SAFETY

There is a growing concern about children’s online privacy and safety. Certainly, safety from predators online has been a key issue around children’s use of the internet for some time, but the ever-evolving set of networked technologies makes children’s safety a moving target. Children’s privacy is both less studied and the recipient of less advocacy than safety. In part, this is caused by privacy’s broader and hazier boundaries.



However, increases in the availability of networked toys and intelligent devices aimed at children is bringing privacy issues to the fore. In December 2016, multiple complaints were raised with regulators over the sale of a wildly insecure [networked toy called My Friend Cayla](#).⁴ This doll’s security was so bad, a user half a world away could hack into it and speak through it. Further, Cayla was programmed with advertisements for Disney movies and products, though this was not disclosed in the doll’s privacy policy.

More research and discourse is needed regarding the privacy and safety of what is sometimes called the ‘internet of toys’ – toys that have networking and sensing capabilities. Consumers International should begin discussions with other advocacy groups already working in this area: the Center for Digital Democracy, the Campaign for a Commercial Free Childhood, and Common Sense Media. Also, the Oxford Internet Institute has recently launched a research project into children’s online safety, and so there may be an opportunity to contribute to that research as a voice from the advocacy community.

CHAMPION PRIVACY FOR CONSUMERS OF ADULT CONTENT

For decades now there has been a gulf between restriction of adult content in the physical world and in the online world. In the physical world, adult content is restricted to over 18s by requiring shop owners to demand to see official IDs to prove age in order to purchase adult content, products and services.

2 World Law Group, [Global Guide to Data Breach Notifications](#), 2016

3 [‘Mac and Android users charged more on shopping sites than iPhone and Windows users’](#), International Business Times, 12/10/2014

4 [‘What to get for children this Christmas... Surveillance!’](#), LinkedIn Website, 06/12/2016

Until very recently, the online equivalent of age verification was not feasible – many adult sites merely required users to affirm they were of legal age. Many factors hampered online age verification: lack of technology, lack of business interest in providing age verification services outside of gambling markets, lack of access to official sources of identity and age by the private sector, and general sensitivities around the use of identity information in adult services. Now, the UK has made it a political priority to enforce long-standing [prohibitions on child access to adult content](#) in the online environment.¹ However, there is an essential privacy concern with any initiative to verify age online. Building age verification systems that can prove age but not reveal identity is costly and uncommon, but far from impossible.

Adults who wish to consume adult content should be able to do so with a maximum degree of privacy, but the higher cost and complexity of pseudonymous, privacy-protecting age verification systems may cause policymakers and the adult content market to elect to build systems that reveal people's identities and consumption habits to content companies, credit card companies, and others within the supply chain. Stockpiling the names of adult content consumers along with their preferences is privacy-invasive and possibly dangerous, as revealing such private preferences and habits could cause stigmatisation, job loss, relationship damage, blackmail, and violence. Consumers International should participate in UK age verification policy deliberations to ensure that a voice is heard for strong privacy to be maintained. Consumers International should engage with the [Digital Policy Alliance](#), a key stakeholder for such deliberations, to help ensure that the age verification regime for legal and private use of adult content does not force consumers into unwanted and unwarranted exposure.²

OFFER TO BE A PLACE FOR INTERNS; OBTAIN FUNDING FOR YOUNG FELLOWS

In policymaking, there is a widely acknowledged lack of technologists. Unsurprisingly, this results in poor understanding of technology by those who legislate it. This same problem exists in advocacy circles, resulting in a lack of depth and nuance in advocacy efforts that revolve around particular technology problems. In both the policymaking and advocacy domains, there is great benefit to be derived from engaging computer scientists, engineers, data scientists, network engineers and others whose primary educational and career focus has been technology. Consumers International should seek funding for Fellows to work alongside its staff and to investigate technology-specific consumer protection issues. In particular, Consumers International should target undergraduate and Master's-level students who are motivated by consumer fairness and justice issues, and who are close to the technologies of the day.



1 [‘Pornography sites face UK block under enhanced age controls’](#), *The Guardian*, 19/10/2106
2 Digital Policy Alliance website, <https://www.dpalliance.org.uk/groups/age-verification/>

DATA: THE NEW BUSINESS FRONTIER / A NEW FRONTIER FOR BRANDS

GLOBAL HEAD OF BEHAVIOURAL SCIENCE IPSOS MORI COLIN STRONG



Ipsos MORI is a market research organisation. Its Social Research Institute looks at public attitudes to key public services, and informs social policy.

Colin Strong is Head of Behavioural Science at Ipsos. In his role he works with a wide range of brands and public sector organisations to combine market research with behavioural science, creating new and innovative solutions to long-standing strategy and policy challenges. His career has been spent largely in market research, with much of it at GfK (Society for Consumer Research) where he was Managing Director of the UK Technology division.

As such, he has a focus on consulting on the way in which technology disrupts markets, creating new challenges and opportunities but also how customer data can be used to develop new techniques for consumer insights. Colin is the author of *Humanizing Big Data* which sets out a new agenda for the way in which more value can be leveraged from the rapidly emerging data economy. Colin is a regular speaker and writer on the philosophy and practice of consumer insight.

To understand the answer to this question, Consumers International can start by asking itself; will brands ever be good data citizens?

Brands have ever more personal data at their disposal, driven by technology fundamentally disrupting the nature of their relationship with consumers. We are starting to see the way that data offers brands unprecedented insights not only into consumer behaviour but also their minds. Whilst the temptation to leverage this for short term gain is understandable, there is a compelling case for brands to remember that trust is what sustains their relationship. And as such, being a good data citizen will become a core part of a successful brand strategy.



THE CHANGING CONSUMER ENVIRONMENT

We are now in an environment where the valuation of companies is increasingly based on intangible (non-physical) assets. Much of this is because of the way technology has transformed the modern company, which led Erik Brynjolfsson, Director of the Massachusetts Institute of Technology Initiative on the Digital Economy to point out that "more and more important assets in the economy are composed of bits instead of atoms". Indeed, it is now estimated that some 70% of the value of a modern company is now derived from intangible assets.

The fact that technology is influencing company valuations reflects how technology is increasingly a platform for consumer interaction. Of course we know this – an increasing amount of our lives are played out via technology, whether this is through social media, engaging with a company's customer service team, buying goods and services and so on.

This is a break from the past, where we would rely on brands as shortcuts to guide us through the complexity of our everyday choices. Many of our purchases are pretty functional and, frankly, we either don't have the time to evaluate the pros and cons of different toilet cleaners or we don't have the necessary access to information to really gauge whether the claims made by one are really better than the competition.

Brand therefore became a shortcut for us, signalling a promise of quality and consistency. We did not have to do the leg-work, we could simply rely on the brand. From the marketer's perspective, the idea was to create an emotional connection so that consumers built a lasting affinity with the brand. Many is the time that I have heard companies saying they want to be the 'best loved' brand in their category.

However, technology has now fundamentally changed the landscape. Consumers no longer need to rely on brand signalling to act as a shortcut for quality. Instead, there are huge swathes of information available online to support us when making decisions. This will not necessarily apply to very low cost / low involvement goods, but in many categories this is fundamentally changing the way we shop.

When we book a holiday, buy clothes or higher value foods, for example, we don't plunder the depths of our memories for past positive experiences or indeed rely on brand associations to determine where to go. Instead we turn to Google to access other users' experiences and expert reviews. That's not to say that all consumers do this but when my mum is keenly using Google to establish which brand of electric heater she should buy rather than relying on John Lewis, I know things have changed.

So what does this mean for brands? Surely, there are two significant implications. First, the traditional brand funnel is in need of rethinking. Simple awareness is not in itself sufficient because technology means that brands can quickly leapfrog into consideration through the use of digital marketing. Indeed, we are [starting to see](#) that best-selling brands in an online environment are often quite different to the best sellers in bricks and mortar.¹

Brands will therefore increasingly seek to differentiate themselves by building relationships through delivery of engaging digitally experiences that deliver genuine value; smart toothbrushes are a great example. In the past the selection of a toothbrush was a simple process of going to the supermarket shelf and selecting based on the quirks of product features, pricing, brand, pack etc. And the toothbrush manufacturer would not know anything about you.

1 Profitero website, <http://insights.profitero.com/amazon-fastmovers-reports.html>

Smart toothbrushes use a number of sensors in the handle to track in real time how you're brushing your teeth. The device is synced to a mobile phone app. As the teeth are brushed, the user is given guidance about where to brush and tells you if you're brushing too much or too little. Often it's possible to programme in guidance for particular outcomes such as whiter teeth or fresher breath.

Clearly, the manufacturer now knows an awful lot about their customers including what you are hoping for, as well as, then tracking exactly when and how they brush their teeth.

The key point to note is that technology is creating a new mechanism for brands to create relationships with consumers. Which, in turn, is creating huge amounts of data that offer an unprecedented insight into very intimate consumer behaviours on an ongoing basis. The importance of this has clearly not passed by some of the largest FMCG companies as the quotes below illustrate:



“As a business, we need more data, better insight into our customers and their needs and behaviours, to serve them with better products and better messaging.”

Alexandre Ricard, Chief Executive Pernod Ricard

“The next level of competition in the universe of FMCG is the relationships we have with consumers. Relevance, trust and on-going value add to their lives beyond the product itself.”

Shawn O’Neal, VP global data and marketing analytics, Unilever

LEVERAGING DATA FOR INSIGHTS

It is clear that technology is creating fundamentally new business models for brands – and whilst the majority of sales is still via bricks and mortar the direction of travel for pretty much every category is becoming pretty clear.

So, just what are brands doing with all the data they collect? There is clear huge variability in the degree of sophistication that brands are able to bring to the way they use and interpret data. At one end there are digitally native brands such as Graze, which started out as a subscription box service for snacking. Their whole business model was predicated on leveraging customer insights from data, as illustrated here by an interview with the CEO:

“We receive over 15,000 product ratings an hour from our customers and use these to develop a new product in 24 hours. This allows us to enhance our customer experience by taking risks and surprising our customers with a

product selection that they might like but not necessarily choose. This ability to respond quickly and engage with customers is one of the crucial benefits of having an online channel. However, even with technological advances and access to a sea of data, not all FMCG companies are able to develop a product so rapidly. In fact, few FMCG companies are embracing technology to enhance their customer engagement.”

Anthony Fletcher, CEO, Graze

However, there are also many companies that struggle to obtain insights from data despite the huge investment that is made in infrastructure. So, whilst AT Kearney estimate that by 2018 the big data tech market will be USD114 billion, research by The Economist found that 65% of CEOs think their organisation is able to interpret only a small proportion of the information to which they have access.

An important impediment much of the time is the presence of legacy systems on which much personal data is held. It is not always easy for brands to access and manipulate the data they hold – so whilst much is possible, making it happen can be a challenge.

In addition, the skill sets are not always necessarily attuned to leveraging valuable insights about consumers. Many data analysts are computer scientists, mathematicians and statisticians – perhaps necessary but not sufficient for understanding consumers. There is still quite a long way to go before brands start to see the value of including social scientists – psychologists, sociologists, geographers - to generate insights of real value. The lack of consumer insights from data led one frustrated head of analytics to comment:

“I have lost count of the times I have been presented with some amazing fact that data has told us through the use of some incredible new technology, to be left thinking ‘so what?’ or ‘isn’t that obvious?’”

But this is all set to fundamentally change.

WHAT TO EXPECT

There is a huge wave of new activity involving personal data, based around the opportunities presented by deriving psychological insights from data trails. Whilst it is relatively early days, there is a huge amount of interest from brands.

One example of this capability was work undertaken by Cambridge University and the Microsoft Research Centre, which found that Facebook ‘likes’ can be used to predict a variety of personal attributes including religion, politics, race and sexual orientation. Their research involved 58,000 Facebook users in the US who completed a psychometric questionnaire through an app called ‘myPersonality’. Those taking the test were asked to provide the researchers with access to their Facebook data. The team were able to create some highly predictive models using these ‘likes’. For example, they were able to identify male sexuality and sort African-Americans from Caucasian Americans, Christians from Muslims and Republicans from Democrats. There were also some pretty impressive figures for predicting relationship status and substance abuse.



Another example is [a study by researchers at Cornell University](#), who analysed over 1.5 million geotagged tweets from almost 10,000 people in the US. They wanted to understand if the content of the tweets themselves could be used to predict the location of the user, as identified from the geotagging. So they divided the data set in two, using 90% of the tweets to train their algorithm and the remaining 10% to test it against. What they found was that tweets contained an awful lot of information about the likely location of the user.

Some of it was obvious, such as tweets that were generated by the location-based social networking site Foursquare, thus giving exact location. Other tweets contained references to the city they were in. And others made reference to events that were taking place in their location. As a result of all this information, they were able to create an algorithm that correctly predicted people’s home cities 68% of the time, their home state 70% of the time and their time zone 80% of the time.

It is highly likely that these sorts of studies represent merely the tip of the iceberg of activity that is underway in this area. It is usually only academic researchers that place their findings in the public domain and make them available for peer review. And academics often struggle to get access to big data assets. So we can assume that this sort of activity is being widely undertaken by many data-intensive industries including, of course, database marketing organisations.

We are, therefore, on the cusp of psychological based marketing – but importantly, where the insights about consumers are derived from their data trails. Of course, as noted earlier, as brands use technology to create data mediated relationships with consumers then this becomes an activity which has huge potential.

THE TEMPTATION FOR BRANDS

Clearly, a picture is being painted of brands potentially wielding huge amount of power. There are many ways in which this could be used not least personalised pricing. So instead of standard prices and products offered to everyone, companies can instantly set prices specifically for any one individual. In the right circumstances, a company that not only knows how much you need something and how much you can manage to pay but also what your psychological profile indicates in terms of your propensity to pay.

A study by Benjamin Reed Shiller, an economist at Brandeis University examined what happened to Netflix’s profits when collecting varying degrees of data about their customers and charging different prices for the same product. Simply having basic demographic information to

IN 'INTERACTIVE TRUST' WE
MAKE OURSELVES AND OUR
NEEDS KNOWN TO THE BRAND
AND, IN DOING SO, MAKE
OURSELVES VULNERABLE

charge different prices increased profits 0.14%. However, adding data from web browsing history increased profits by 1.4%. Indeed, some customers paid twice as much as others for the exact same product.

So what is to stop a brand wielding this information in a way that is not in the consumer's interest? In a sense the answer is simple – trust.

WHY TRUST IS CRITICAL FOR BRANDS

Trust is a term that is often used but frequently misunderstood. Part of the reason for this is that trust has a number of different meanings which we deal with in turn below.

First, for trust to succeed, we need to be able to rely on others to act in certain ways. So for there to be trust we need to be able to rely on others to do what they say they will do. This is **basic trust**.

Most brands are able to operate reasonably well in terms of 'basic reliance'. We know our shopping will arrive, it will be in line with our expectations and if anything has gone wrong then it will be fixed. Of course, this is far from the case for all brands in all geographies but it is widely understood that doing what you will say you do and fixing it if it goes wrong is the starting point for any brand. Brands such as Amazon, Walmart and MacDonald's have made a virtue of demonstrating this form of trust – you can be sure that the products and service experience is consistently reliable.

Second, is the trust that the brand will treat me well and that it has my well-being in mind in the way it conducts its affairs. This form of trust is called **'active trust'**. This is often associated with consumers being a little more vulnerable. So a retailer may hold a lot of data on consumers via their loyalty card scheme.

We 'actively' rely on the brand to use that data in a way

that will not harm us by, for example selling it to a third party without our consent.

The third level of trust is **'interactive trust'**. In this instance we are making ourselves and our needs known to the brand and, in doing so, making ourselves vulnerable. Essentially, we are asking the brand for something that may not be strictly part of the rules and regulations. But in the process of making the brand aware of our needs, we are giving them some power over ourselves. So we might want to take an item of clothing back but have taken the tags off.








Certain brands have achieved remarkable success by creating a sense of trust between themselves and the customer. Nordstrom, the US retailer, for example has huge reputation for customer service that directly translates into trust. This is exemplified by their 'rulebook' to new employees:

Nordstrom Rules: Rule #1: Use best judgment in all situations. There will be no additional rules.

The challenge that many brands have, of course, is that trust costs money. If the basis of your trusted relationship with your customers is quality of customer service, then that costs money. If it is the quality of your ingredients in the food you make, then the company accountants will always be quick to point out how you can save money by sourcing poorer cheaper cuts.

It can be hard to locate the evidence that this relates to sales but work by Ipsos has found a relationship between 'Attitudinal Equity' (AE) and share of wallet:

Across all sectors brands with an AE of 40 plus give more of their share of wallet to the brand, more in service industries which really benefit from strong brand relationships

	 FMCG	 Alcoholic Beverages	 Retail	 Financial	 Automotive	 Restaurant	 Services
	Share of wallet						
AE 0-20	4	3	4	4	4	4	4
AE 20-40	28	30	31	29	29	29	30
AE 40+	57	58	54	57	53	62	70

*Source: BVC Database 2017

So to return to the issue of personal data, it would seem that brands face a dilemma. There will inevitably be ways in which they can enhance their share price by leveraging the insights about their customers from personal data. And if this is used to facilitate the relationship (for example helping consumers brush their teeth more effectively) then trust grows. But if it is used in ways that transgresses the nature of the trusted relationship, then they are likely to see, in the longer term, a decline.

CONCLUSION

As companies increasingly adopt [data driven decision making](#), it can be ever harder to recognise the importance of the human side of brand relationships which, by their nature, are hard to quantify.¹ We discussed at the outset the way in which intangible assets are accounting for a high proportion of brands' valuations – it makes sense that this is driven by technology. But let's not lose sight of what the technology is facilitating – a relationship. And as everyone knows, if trust is abused in a relationship then it is not long before the relationship falters. Brands need to understand how to use data to develop and enhance their relationship with the consumer – not abuse it.

¹ ['The rise of data-driven decision making is real but uneven'](#), Harvard Business Review, 03/02/2016

PART TWO: **CREATING** **CHANGE**

**THROUGH
CHALLENGING OUR
OWN THINKING, WE WILL
SPARK THE CONNECTIONS AND
CO-LEARNING THAT WILL LEAD
TO THE EMPOWERMENT OF
CONSUMERS AROUND
THE WORLD**



A NEW DATA INFRASTRUCTURE

FOUNDER AND CEO, IF SARAH GOLD



IF works with organisations shaping our digital world. Together we show how they can empower people, be trusted with data and be effectively regulated

Sarah Gold founded [IF](#) in 2015 to develop a more ethical society with organisations shaping people's future. That means ensuring that, as technology develops, people and society are put first. A [NESTA New Radical](#) and [Forbes 30 under 30](#) awardee, Sarah sits on the practitioner panel for the [Research Institute in the Science of Cyber Security](#). She regularly gives talks about privacy, security and ethics.

Digital technology has created new expectations and opportunities in every aspect of life. As [our project for Consumers International showed](#), policy responses to 'digital' range from the mundane to the radical: from investing in broadband to establishing digital personhood.¹ But very few of these policies address something inherent in digital technology: its global nature.

The technologies people use around the world share the same foundations. That means that a vulnerability in a computer chip – like the recently revealed 'Meltdown' and 'Spectre' – can affect millions of people around the globe. But there aren't many services that can support people who are affected by these faults on such a massive scale.

There's an opportunity here for Consumers International to take the lead. They can use their position at the heart of the consumer advocacy community to champion, build and connect the pieces of a new digital infrastructure.

THE RISKS WE CAN'T SEE

An exploit is a piece of software or list of instructions that allow people to take advantage of bugs, weaknesses and flaws in products. [Exploits](#) break the products people use in ways they can't see. These vulnerabilities affect the security of consumer data and privacy, and when someone takes advantage of one it can lead to a direct assault on an individual's rights.

A recent example of an exploit is [CVE-2017-7240](#), which affects an industrial dishwasher made by Miele.² This exploit allowed malicious actors to get information that could help them access other devices on the network the dishwasher is connected to. These dishwashers are marketed to hospitals and schools: if someone were to gain access to the devices on those networks, the consequences could be catastrophic.

Stories about exploits like these are regular features in the technology press. Companies push themselves to follow a trend and connect devices to the internet without considering the risks to the rights of their customers should something go wrong.

Part of the reason for that, is that it's really hard to track an exploit. That makes it difficult to hold a company to account when something goes wrong.

DATA AS INFRASTRUCTURE

The way exploits are described and documented to date has been for a technical audience. The rather cumbersome name CVE-2017-7240 comes from the [Common Vulnerabilities and Exposures database](#).³ This database gives a reusable identifier to an exploit, accompanied by a brief description of the exploit from the [National Vulnerability Database](#).⁴ More detail is usually published by researchers on their own websites, or on mailing lists like [SecLists](#).⁵

This data isn't legible or usable in a way that would help most consumers find out about problems with the things they own. Sometimes journalists pick up on high profile exploits and make them readable to a general audience, but it's impossible to cover every exploit in every product.

Some websites, like [Have I Been Pwned](#) have started to make exploit information more accessible so people know when their digital rights are being affected.⁶ But it would be better if the databases themselves were human-readable, easy-to-understand, and built in a way that helped developers use that data more effectively. That way they'd be accessible to more people, and more useful for consumers.

GLOBAL DIGITAL INFRASTRUCTURE

Consumer rights organisations all need to do similar things - like [alert people to dangerous products](#), [test digital products](#), agree on technical standards - and do this in the



1 Consumers International website; digital policies, <http://digitalpolicies.consumersinternational.org/>
2 Common Vulnerabilities and Exposures website; CVE-ID, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7240> Common Vulnerabilities and Exposures website; home-page, <http://cve.mitre.org/>
3 National Vulnerability Database website, <https://nvd.nist.gov/>
4 Seclists website, <http://seclists.org/>
5 Have I been pwned website, <https://haveibeenpwned.com/>

context of a global economy.^{7,8} Historically, these organisations have worked together to share best practice and new approaches to challenges. Today, they could continue that work and build a shared, open infrastructure that supports services around the world.

Today, when companies build digital services, they rely on digital infrastructure that's available quite widely. This can be anything from hosting provision to open data. When it comes to consumer advocacy, what would that look like? It probably includes things like:

- an open register of products
- an open register of components
- an open register of software vulnerabilities
- an open register of hardware vulnerabilities
- a versioned database of terms and conditions
- shared software and best practices for testing connected devices
- standards for publishing test results
- shared software and best practices for understanding software supply chains
- an open register of data breaches
- open standards for product recall notices

Some of these do exist in a nascent form, but as independent projects rather than things that governments or consumer rights organisations rely on. Programs from other sectors - like [IATI](#), the open standards for publishing international aid - show that this is both possible and transformative.⁹

If this infrastructure is built in the right way, new services could emerge. Retailers could automatically notify consumers about dangers in products they've bought if issues arise after-purchase. Or home routers might be able to disconnect devices on a network that turn out to have a bug or a security flaw.

Consumer rights organisations, working together, could build this infrastructure. Consumers International is in a fantastic position to convene that conversation. Working with the existing community, it can understand the needs and capabilities of teams around the world, and steer development of infrastructure that would benefit consumers.

GLIMPSES OF THE FUTURE

The recent efforts of Consumer Reports, Disconnect, Ranking Digital Rights, and The Cyber Independent Testing Lab to develop [The Digital Standard](#) shows this kind of collaborative approach is possible.¹⁰



The standard is a community effort to bring together privacy and security best practices for those building digital products and services. Specifically, it aims to help organisations test products - maybe a smart thermostat - and assess how well it respects the owner's rights.

The Digital Standard encourages manufacturers to answer the sort of questions owners currently can't, including:

- Who's the data shared with?
- Will it still work if the company loses interest?
- Can owners update the software after it's out of warranty?
- Does it give hackers an easy way into a network?
- Is there anything on the device that would block a consumer's ability to repair it?

The great thing about the standard is that's [it's being developed in the open](#).¹¹ It's already part of the shared infrastructure needed to build better products and services. It's the kind of thing services like [havebeenpwned.com](#) and the [Restart Project's wiki](#) do too.¹² It involves groups working together, in the open, and making what they've built available to everyone.

That's a critical step towards infrastructure that supports digital rights.

7 European Commission website; consumer safety, http://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm

8 Which? Website; testing and research, <http://www.which.co.uk/about-which/research-methods/lab-testing/>

9 International Aid Transparency Initiative website; <http://www.aidtransparency.net/>

10 The Digital Standard website, <https://www.thedigitalstandard.org/>

11 GitHub Website, <https://github.com/TheDigitalStandard/TheDigitalStandard/>

12 The Restart Wiki website, https://therestartproject.org/wiki/Main_Page

PEOPLE NEED SUPPORT

There's no shared understanding of our rights in the digital world. While the [GDPR](#) starts describing a precedent, what it doesn't do is describe how it will exist in the real world.¹ Digital rights need a digital infrastructure.

The reassuring thing is, we've been here before. The Consumer Bill of Rights was an incredible achievement, and set the precedent for decades of work around the world. Consumer groups around the world have a terrific history of addressing problems around consumer safety, new technology and people's rights.

What's needed now are organisations willing to lead development of a new infrastructure. Consumers International have a pivotal role at the heart of a global network. They can convene, drive and deliver the change needed to support consumers into the future.

**CONSUMERS
INTERNATIONAL HAVE
A PIVOTAL ROLE AT THE
HEART OF A GLOBAL
NETWORK**



1 The information Commissioner's Office website; overview of the GDPR, <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/>

MAXIMISING THE IMPACT OF CONSUMER LEGISLATION

**READER, BRUNEL
UNIVERSITY LONDON
DR CHRISTINE RIEFA**



**Brunel
University London
is a public research
university located in
West London. Founded in
1966, it was named after
the Victorian engineer
Isambard Kingdom
Brunel.**

Dr Christine Riefa is a Reader specialising in consumer and internet law at Brunel University, London. She is widely published on these topics and her monograph *Consumer Protection and Online Auction Platforms - towards a safer legal framework* was published by Ashgate in 2015. She is an elected board member of the [International Association of Consumer Law](#) and one of the editors of the [Journal of European Consumer and Market Law](#) (EuCML), a peer-reviewed Journal, published by Beck and available on [Kluwer Online](#). [More details on Dr Riefa's areas of expertise.](#)

Digital consumers are unequal across the world. Some need access to the internet, others are preoccupied with protecting the masses of data that are collected about their digital footprints or worried about the safety of their credit cards when paying online. Many live in areas of the world where the legal framework is lacking, while others belong to well-developed regional and national legal systems that have now tackled online activity for a few decades, and are becoming more reactive to their needs. The digital world moves a pace everyday, opening up new challenges. It is those challenges that an organisation like Consumers International can help tackle, with a targeted response, as positive change for consumers will not look the same in all regions of the globe.

As my expertise lies in the UK and Europe, I must preface my essay with a warning that my views are largely informed by what I see as positive changes in the European sphere. I have limited expertise in other regions of the globe and would not want to purport to offer a view that would work for all. Having said that, many of the challenges facing European consumers also face consumers around the globe. Big data, payment protection or protection against scams is unfortunately not the only reserve of the developed countries.

European consumers already benefit from a robust legal system of protection, although it is indeed always a work in progress and able to be improved. It forms nevertheless a good base line of protection especially if compared to other regions, even those with high online penetration rates and established legal systems (e.g. USA – note the recent cut-back on data protection by the Trump administration, the absence of a right to withdraw from online transactions, etc.).¹²³ Divergence in levels of protection is one of the key problems consumers face around the globe. It hinders cross-border sales and redress.

A European study conducted in 2015 showed that geo-blocking has negative impact on the single digital market.⁴ Geo blocking is a practice whereby retailers refuse to sell to consumers situated in another state, or service providers prohibit the streaming and download of content from particular regions (tv programme, video download in particular).

The practice is essentially a form of discrimination that is quite rife across Europe, a market where consumer laws are essentially aligned.⁵

Geo blocking is aimed at controlling pricing in so much that it sometimes lead to redirecting consumers to websites in operation to their region of the globe where higher pricing or different condition of sales apply, simply based on their nationality or geographical location. The EU is in the process of adopting legislation to block this practice across the European Union but other regions are lagging behind.⁶

Furthermore, while many countries (including those in the EU) have good legislation in place, my experience is that the way it is applied by judges and enforcement authorities varies widely and the existence of laws on the books does not necessarily translate into adequate protection on the ground.

For example, in Serbia, consumer protection has been transformed over the last 10 years through no less than four versions of the Law on Consumer Protection. The latest incumbent brings Serbian law in line with Directive 2011/83/EU on Consumer Rights and therefore offers protection for online shoppers.

Yet, **“while the new law offers all the hallmark of a fully functioning legal system of protection, Serbian consumer law lacks the teeth needed on the ground to make it a reality. This can be explained by a series of factors including resistance towards the recognition of consumer as an autonomous branch of the law and non-application of consumer law by the Serbian courts, amongst others”**.⁷

Raising the base level and ensuring adequate implementation would therefore be a positive change in itself. Support of the G20 may be invaluable in raising the profile of the protection that is required, work that Consumers International is already tackling.⁸

1 US Federal Communications Commission, [Protecting the privacy of customers of broadband and other telecommunications services](#), 02/11/2016

2 US Federal Communications Commission, [Protecting the privacy of customers of broadband and other telecommunications services](#), 01/04/2016

3 [What really happens when the FCC's online privacy rules are cancelled](#), Fortune, 03/04/2017

4 [Obstacles to the digital single market \(perceived and actual barriers\)](#), European Commission, Market studies, September 2015

5 [‘Geo-blocking of consumers online: findings of a mystery shopping carried out by the European Commission’](#), European Commission; Market studies, May 2016

6 [‘Proposal for a Regulation on addressing geo-blocking’](#), European Commission; Laws, 25/05/2016

7 Riefa, C & Durovic, M, ‘Maastricht Journal’. Serbian Consumer Law, out with the old, in with the new, Vol 22 (6) (862-878), 2015.

8 [‘Consumers International welcomes G20 leaders support for consumer protection in the digital economy’](#), Consumers International. 10/07/2017 recommendations

But such initiative remains limited and does not necessarily provide impetus for less economically stable countries. The work of the OECD and the United Nations is thus equally important to reach out further afield and impress upon all the virtues of protecting consumers.⁹¹⁰¹¹

“Consumers, by definition, include us all. They are the largest economic group in the economy, affecting and affected by almost every public and private economic decision. Two-thirds of all spending in the economy is by consumers. But they are the only important group in the economy who are not effectively organized, whose views are often not heard”.¹²

John F. Kennedy

Many years have passed since President J.F.Kennedy’s speech to Congress in 1962, and yet consumers do not seem to have made that many advances. Giving actual power to consumers by becoming an effective pressure group should be a priority for Consumer international. Lobbying for strong consumer protection is a key action point to be taken on by consumer organisations and Consumer International in particular, for without them, I am unsure such task can be left to businesses and legislators alone.

Tech companies spend an astronomical amount on lobbying activities every year. In 2016, Alphabet, Google’s parent company, spent upwards of USD11 millions in the USA alone and Google’s spend in the EU is known to have increased markedly in the last few years.¹³¹⁴ Consumers International is unlikely to be able to match this expenditure. It can however, reach out to legislators and bring about positive change.

In Europe, BEUC¹⁵ and a number of consumers associations are credited with positive impact on the legislative (and enforcement) process, without the financial might of tech giants.¹⁶ In any event, Consumer International can contribute to the creation and application of good digital practices. Consumers’ education, alongside support to small and medium businesses is an essential stepping-stone to ensure a fair deal for consumers in the digital economy.

The 2015 Consumer Conditions Scoreboard showed that retailers had rather low levels of knowledge of their



legal obligations.¹⁷ In the online world, there is evidence that ‘small copies large’. This is particularly acute when it comes to the use of terms and conditions on websites. A survey into the online auction industry showed that a large amount of cross-fertilisation existed between the legal terms of many sites operating.¹⁸

The reason for such cross-fertilisation is often due to small operators ‘copying’ others without necessarily seeking legal advice. One way to improve this situation may therefore be to educate businesses while also forcing bigger industry players to comply (through enforcement), if they do not already do so. Indeed, big players tend to have a better compliance record than smaller intermediary or retail sites.

This is possibly because they have better access to legal advice, but also because they find themselves more often the target of enforcement authorities, courts and the media; thus forcing better behaviour. In addition, the creation of a terms and conditions blueprint by national enforcers, professional organisations and/or consumer associations for all to use would offer an excellent tool bank for smaller businesses.

9 OECD, *OECD Recommendation of the Council on consumer protection in E-commerce*, 12/05/2016
10 UNCTAD, *United Nations guidelines on consumer protection*, 2016
11 UNCTAD, *Manual on consumer protection*, 2016
12 ‘John F. Kennedy, special message to the Congress on protecting the consumer interest (1962)’, The American Presidency Project, 15/03/1962
13 ‘The 17 tech companies that lobby the government the most’, UK Business Insider, 22/12/2016
14 ‘Google, trying to endear itself to Europe, spreads \$450 million around’, The New York Times, 19/06/2016
15 BEUC website; Latest successes, <http://www.beuc.eu/successes>
16 Consumers International, *Annual Report 2015*, 2015
17 European Commission, *Consumer Conditions Scorecard*, 2015
18 C Riefa, *Consumer Protection and Online Auction Platforms: towards a safer legal framework*. Routledge, 2015

DIVERGENCE IN LEVELS OF PROTECTION IS ONE OF THE KEY PROBLEMS CONSUMERS FACE

Another possible tool may be the use of software to detect potential unfair terms and require their modification.

For issues beyond terms and conditions, collaboration with industry also seems a smart move. Even with the big tech companies, it seems possible to build bridges, understand their technology better and offer practical rather than legal solutions. This solution is unlikely to work in all cases, especially where the trader has rogue predisposition, or where there is not sufficient popular pressure. But it will enable some companies to improve products thanks to the feedback received by consumer associations and other representatives.

Moreover, it is by educating consumers and galvanising them to demand high levels of protection that actions can be most effective. Most online models now rely on consumers' data. It is not feasible for any online business to function without in-depth knowledge of their customers' habits and preferences. The once unbalanced relationship between the trader and the consumer may be about to shift. Data is currency and in many respects, this ought to force online platforms and retail websites to want to engage more fairly with their customers.¹

Their custom, not only fuels direct revenues, buying goods and services, but their data also enables the platforms to a) tailor offering and sell more than they would have otherwise managed and b) use the data to generate revenue streams by renting or selling the data gathered to aggregators. Those can therefore be powerful arguments to engage with tech companies and force a change if consumer demand can be swayed away from suppliers that do not provide consumers a high level of

1 ['Is data the new currency'](#) World Economic Forum, 14/08/2015

2 Christine Riefa and Christiana Markou, Online Marketing: Advertisers know you are a Dog on the Internet!, in Andrej Savin and Jan Trzaskowski (Eds.), Research Handbook on Internet Law, Edward Elgar (2014) 383.

3 European Commission website; Digital privacy, <https://ec.europa.eu/digital-single-market/en/online-privacy>

protection. Yet, we still see a real imbalance mostly due to information asymmetry and the fact that the technology has somewhat runaway from human control. Algorithms can be so complex that even data collectors can be at odds with explaining exactly how the data gathered is being used to build profiles, unless they are IT specialists. Even the simplest of technologies can empower traders to discriminate between consumers.

Through the use of cookies, suppliers are able to collect data on consumers and charge different prices, (price discrimination)making use of their preferences.² This is contrary to the Unfair Commercial Practices Directive, but it is not a phenomenon that is particularly well framed in traditional contract law, or by current distance selling rules in Europe. If the consumer wants to regain control, we must educate them as to the risks the technology poses, and/or legislate to avoid extreme manipulations of data to the disadvantage of consumers. In Europe, privacy laws are in place but still fall short.³ Consumer education can take place in classrooms and I, for one, would welcome consumer rights and digital literacy being included in all schools' curriculum.

But it can also, in the meantime, take the form of short campaigns to warn of the dangers of particular products and/or seek their removal from the marketplace, thanks to the work of enforcers. One recent example is a campaign conducted by the Norwegian Consumer Council: #toyfail. 'My friend Cayla' and the I-Que robot are toys sold in a number of markets, described as interactive. They can be controlled via an app on an iPad or smart phone/ tablet. Children can ask questions and get answers, have conversations, etc.

Yet, the toys are not as innocent as they look. In the case of the doll, it can easily be hacked through a mobile phone enabling the hacker to talk and listen through the toy, without even having access to the physical doll. The child's conversations with the doll are also recorded and transferred to a US based company which reserves the



right to use the voice recording and information gathered from the child, through its terms and conditions of use.

The doll also shares commercially endorsed preferences (for Disney movies for example) and promotes products through targeted advertising based on what information the child shared with the doll.⁴ In Germany, the sale of such toys has been banned, but the toys continue to be sold in various countries.⁵

With increasing appetite to protect one's privacy, inaction does not seem to be an option for tech companies. Indeed, even newer technologies such as block chain may disrupt the current digital market and enable consumers to keep a hold of their data, as well as enable them to transact safely and directly with one another. It has the potential to underpin the next level of the sharing economy, where intermediaries are no longer required to process financial transactions. Block chain technology indeed ensures high levels of security through a decentralised network. It also enables reliable authentication of payment source.⁶

[Openbazaar](#)⁷ is one example of how technology can enable consumer transactions, without the fees that are normally reserved for the intermediary. Yet, the role and liabilities of such platforms is still unclear and requires attention. Unfortunately, to date, consumer rights are largely ignored on these platforms.

This is due to two issues already raised earlier. First, it is because the sellers come from multiple jurisdictions, all with varying levels of protection. Second, it is because the platform template itself does not offer the possibility to document and provide the information normally required in a typical e-commerce transaction (at least under European Law).


This leads us to perhaps one of the most pressing issue to empower consumers worldwide: dispute resolution in the digital sphere. Without enforcement, private or public consumer protection is not worth the paper it is written on. It is therefore essential that consumers can seek and obtain redress where required. Knowledge of the available consumer rights is a first hurdle to clear. A survey conducted in the EU showed that most consumers making digital purchases were unaware of their rights from the outset.⁸

In addition, cross-border dispute resolution, still in its infancy, does not yet allow effective and cheap methods for consumers to return goods and get their money back in a timely fashion and at a cost that is not prohibitive. Unfortunately, when consumers buy cross borders, they will be presented with a host of obstacles. This may include;

- Finding out that their contract is subject to a foreign law.
- Potentially having a foreign court elected the competent court to hear the dispute.
- Their contract being subject to an arbitration clause that prevents them to seek redress in a state sponsored forum.

In Europe, these inconveniences are, in theory, somewhat avoided. This is thanks to Article 15 and 16 of Regulation EC 44/2001, which enables consumers to bring an action, or be sued, where he or she is domiciled, providing that the business pursued or directed its activities to this territory.⁹

In addition, Article 6 of Regulation EC593/2008 also favours the law of the consumer's domicile.¹⁰ Finally, a prohibition on unfair terms that applies to arbitration clauses and jurisdictions clauses limits the potential harmful effects of such terms.¹¹ However, while out-of-court dispute resolution systems are favoured, trust in Alternative Dispute Resolution (ADR) and courts by European consumers remains low.¹²



**THE EXISTENCE
OF LAWS ON THE
BOOKS DOES NOT
NECESSARILY TRANSLATE
INTO ADEQUATE
PROTECTION ON THE
GROUND**

4 ['Connected toys violate European consumer law'](#), Forbrukerradet, 06/12/2016

5 ['Bundesnetzagentur removes children's doll "Cayla" from the market'](#), Bundesnetzagentur press release, 17/02/2017

6 Block Geeks website, <https://blockgeeks.com/guides/what-is-blockchain-technology/>

7 Open Bazaar website, <https://www.openbazaar.org>

8 GfK Belgium, [Identifying the main cross-border obstacles to the Digital Single Market and where they matter most](#), 2016

9 Official Journal of the European Communities, [Council Regulation \(EC\) No 44/2001](#), 22/12/2000

10 Official Journal of the European Communities, [Regulation \(EC\) No 593/2008 of the European Parliament and of the Council](#), 17/06/2008

11 European Economic Community, Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts. 1995

12 C Hodges, I Benohr & N Creutzfeldt, Consumer ADR in Europe. Hart Beck Nomos, 2012

The Consumer Conditions Scoreboard also notes that no clear improvement has been seen since 2010, a fact that is extremely troublesome. Meanwhile the volume of complaints received by European Consumer Centres Network (An EU-wide network that provides free legal assistance and information to consumers) is rising year-on-year and one of the main reasons for not complaining about E-commerce purchases is the assumption that the problem encountered is unlikely to get a satisfactory solution.¹

Access to justice is an international preoccupation. An OECD report from 2006 highlights the importance of cross-border dispute resolution mechanisms.¹ More recently, UNCITRAL started looking into viable ways to resolve disputes and is developing procedural rules on online dispute resolution (ODR).² Its latest output is a draft outcome document, reflecting elements and principles of an ODR process. This instrument is aligned to the European ODR model, although at first glance not as protective, bringing us back to one of our first points: the difficulty in protecting consumers in a world where levels of protection and development of technology are so disparate.³

Many challenges lie ahead for digital consumers and organisations that purport to help them get better protection. Internet of Things, 3D printing, human chip implants, driverless cars are all issues that digital consumers will at some stage be confronted with.⁴ We could not in this essay address them all. While the size of the task ahead is immense, it is with optimism that I conclude.

Consumers International has, over the years, achieved great things and the openness and collaborative nature of its network sets it in good stead to be able to adapt to the realities on the ground and effect positive change for consumers. I wish all involved the best of luck in their campaigns and activism.



**GIVING ACTUAL POWER
TO CONSUMERS BY
BECOMING AN EFFECTIVE
PRESSURE GROUP SHOULD
BE A PRIORITY**

1 OECD, [Consumer dispute resolution and redress in the Global marketplace](#), 2006.

2 United Nations Commission on International Trade Law, [Working Group 3 on Online Dispute Resolution](#), 2016

3 European Commission, [Alternative and Online Dispute Resolution \(ADR/ODR\), or more on these issues](#), 2016

4 [‘Human Microchipping, the benefits and downsides’](#), Richard Van Hooijdonk, 2017

WIDER ENGAGEMENT: CIVIL SOCIETY, INTERNET GOVERNANCE AND BUSINESS SECTOR

GLOBAL PARTNERS DIGITAL

ANDREW PUDDEPHATT

Andrew Puddephatt, is Executive Chair of Global Partners Digital (GPD)'s Advisory Board. As well as being closely involved in GPD's strategy, he also leads the Secretariat for the intergovernmental Freedom Online Coalition. He is an expert consultant to UNESCO, where he developed a methodology for assessing the impact of media on democracy, as well as indicators to measure journalist safety and internet development. He is currently leading a major scoping study of human rights and digital communication trends for the Ford Foundation and assisting GPD's work on cybersecurity.



GLOBAL PARTNERS DIGITAL

CHARLES BRADLEY

Charles Bradley is Executive Director. He oversees the continual development and implementation of GPD's vision, as well as providing strategic support to the organisation.

Before joining GPD, Charles was the Development Manager at Artis Education, a creative education social enterprise that helps children achieve excellence through the arts. Here he led on a number of projects, including the implementation of Artis Impact, one of the most extensive and differentiated professional development programmes in the world, and the management of partner relationships across numerous stakeholder groups. His ongoing involvement with social purpose businesses stems from his keen interest in developing environments that ensure deeper, more sustainable impact within and across communities.



Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

It is commonplace to say that the internet is a rapidly changing environment. The technological changes and developments we are witnessing in the digital environment are rapid, technically complex and only partly foreseeable. Just as the precise nature of the current digital environment could not have been predicted a few years ago, so the future digital environment cannot be predicted today with any degree of certainty. What the trends suggest, however, is that there will be increased digital/physical convergence, increasing amounts of data generated about individuals, an increased use of algorithmic and automated decision-making and an increased use of artificial intelligence and robotics.

In particular, we are likely to see a significant shift from a web-based internet experience where we choose how and when to engage, to something far more ubiquitous, where our entire experience and interaction with the world is shaped and formed by digital devices and services. These developments are already changing the global policy environment, putting issues such as cybersecurity, cybercrime, data protection, and data ethics high up the global policy agenda. They represent a new challenge for consumer organisations and will require an informed understanding of these trends, an ability to develop new partnerships in the field and new capacities to influence and shape policy.

These changes and developments all have significant consumer implications, both positive and negative. While new technologies can create fresh opportunities for consumers to be better protected and promoted, they can also carry considerable risks; either as a result of the technology in and of itself, or its use (and abuse) by state and non-state actors. Furthermore, as the internet becomes a general utility technology, encompassing more and more aspects of our daily lives, it will impact upon more and more areas beyond the current focus of digital communications; including areas such as home security, finance services, retail, education, health and employment.

Despite this, consumer considerations are rarely fully explored or understood during the technological development process. This is partly a result of the rapid pace of innovation, which does not always allow for a fully informed consideration of the consumer implications of innovations as they happen, but also because technical innovation generally follows a 'build now, assess later' approach – in which policymakers are forced to play 'catch up', and be reactive rather than proactive in considering the implications of technological advancements. Consumer organisations must be prepared to fill this gap.

Firstly, it is important to say that use of digital communications depends upon access which remains uneven in many parts of the UK. In fact, the UK lags behind many developed countries in access to high speed internet. A comparison by Ofcom of broadband download speeds in the EU showed the UK only achieving middling status as 12th.¹ While this has been a source of frustration to a range of people, from companies to rural populations,

there has not been a consistently strong consumer voice pressurising government to achieve better results.

Despite these limitations, the internet was used daily by 82% of adults (41.8 million) in Great Britain in 2016, compared with 78% (39.3 million) in 2015 and 35% (16.2 million) in 2006. In 2016, 70% of adults accessed the internet 'on the go' using a mobile phone or smartphone, up from 66% in 2015 and nearly double the 2011 estimate of 36%. In 2016, 77% of adults bought goods or services online, up from 53% in 2008.² All of this emphasises how important the internet is to consumers.

Access will become even more important as digital communications become a ubiquitous technology that is the means through which we access government services, buy and exchange goods, communicate with family and friends etc.

A report from the digital skills committee of the House of Lords recommends that the internet be ranked alongside water, gas and electricity as something that needs to be available for everyone in the UK.

“Digital technology is changing all our lives, work, society and politics. It brings with it huge opportunities for the UK, but also significant risks. This demands an ambitious approach which will secure the UK’s position as a digital leader”.³

House of Lords Select Committee on Digital Skills Report of Session 2014-15

Consumer groups need to have a view as to whether they think framing the internet as a public utility is the correct policy approach.

CONSUMER GROUPS NEED TO HAVE A VIEW AS TO WHETHER THEY THINK FRAMING THE INTERNET AS A PUBLIC UTILITY IS THE CORRECT POLICY APPROACH

1 [‘The top 27 fastest UK and EU countries by broadband ISP speeds’ ISP Review, 06/03/2013](#)

2 Office for National Statistics, [Internet access – households and individuals: 2016](#), 2016

3 House of Lords Select Committee on Digital Skills Report of Session 2014-15, [Make or break: The UK’s digital future](#), 12/02/2015

Online technologies have brought tremendous benefits for people whether as citizens or consumers. Transaction costs online are vastly cheaper than those requiring human intervention. For example, booking a driving test costs £6.62 by post, £4.11 by telephone, but just £0.22 online.⁴ The government has estimated that between £1.7 billion and £1.8 billions of taxpayer's money could be realised as total annual savings to the government and service users.⁵

In the past twenty years, most people access the internet through the world-wide web and it has been a communication service. The business model of the internet is that services – search, social networking, peer-to-peer sharing, are provided without charge in exchange for those services collecting user data and selling it, often through multiple intermediaries who process and analyse the data for sale to advertisers.

The terms of service (ToS) for use of these services, even common ones such as Facebook or Google are detailed, lengthy and hard to understand. Few users bother to look at them and few appreciate quite how much data is being gathered and how much it can reveal about a user. Companies justify the obscurity of the ToS by claiming that users judge an application by the 'user experience' and as targeted advertising is relatively harmless and a mild irritant to most people at best there has been little public concern.

Consumer groups have not flagged up this issue as they might, or talked about the privacy implications enough. At the very least companies should be pressurised into providing simplified summaries of the ToS which make clear the nature of the data gathering and sale that is taking place.

Ever since the first pop-up advert, the business model of the internet has been based on surveillance. The more data a company has about a user, the more targeted its advertisement can be, and the more an advertiser will pay to post their ad. This logic has driven a culture of ever more invasive data extraction and retention; from companies implementing real-name policies, to period tracking apps that store and utilise sensitive information to increase company revenue.

But this asymmetrical model – in which companies have all the power – is coming under increasing scrutiny. For many years, privacy defenders have been highlighting the risks inherent in the advertising model, and have won some important legislative victories in the past few years.⁶ At the same time, regulators are increasingly cracking down on company mismanagement of data, such as through the General Data Protection Regulation (GDPR) in the EU, and the use of ad-blockers is growing fast.⁷



Companies are starting to take notice. At this year's Mobile World Congress, there was a lot of talk about Me2B (me to business), which describes a wholesale transformation in the business/customer relationship – a move, in normative terms, from a model where customers (to quote the business consultancy Ctrl-Shift) are "treated as the passive targets of an organisation's activities", to one which is about "agency, helping individuals achieve their goals".⁸ In practice, this might mean users being able to choose exactly how much data they share, and with which companies, which would be a radical shift indeed.

There are some recent signs which suggest the idea may be gaining momentum – notably among telecommunications companies. Telefonica recently rolled out its AI-powered digital assistant, Aura, which allows users to decide who can access their aggregated data, while its subsidiary O2 has suggested measures that allow customers to control what adverts they see.⁹ The significance of these initiatives should not be underestimated; they would have been inconceivable a decade ago, and show how far the debate has moved along.

Of course, telecommunications companies have different priorities than other parts of the tech sector. After all, their financial model is not based on intrusive advertising, and giving their users more control will not necessarily hurt their bottom line. For media organisations, largely or entirely funded by targeted advertising, Me2B is inevitably going to be a bigger ask.

4 ['Government transaction costs – the story behind the data'](#) UK Government Digital Service, 17/01/2013

5 UK Government Digital Service, [Digital Efficiency Report](#), 06/11/2012

6 ['Ireland challenges Facebook in what could become a landmark data case'](#), *Fortune*, 07/02/2017

7 ['25 percent of smartphone users have ad blockers, according to survey'](#), *Digital Trends*, 07/03/2016

8 ['The rise of Me2b'](#), *Ctrl-shift*, 27,10,2014

9 ['O2 hints at ad-blocking, or at least ad-calming measures'](#), *Gizmodo*, 27/02/2017

So far, rather than trying to understand the reasons some of their readers might be using ad blockers, most have responded by shaming them, begging them to stop, or even blocking them from accessing content. The Guardian's approach – which both asks users with ad-blockers to support them through a membership scheme to, and clearly defines how readers' data is used along with paid 'ad-light' options, like the one offered by Forbes, are examples of more nuanced and thoughtful responses to the issue (although the Guardian continues to make vast losses).¹

At the Mobile World Congress this year, Facebook, another company which depends on advertising revenue, unveiled a new report, "A new paradigm shift for personal data" which attempted to set out some of the principles which would define a "sustainable data sharing environment".² Some of its conclusions – particularly around moving from an implied consent data model, to one based on "choice and control" – are welcome and refreshing, and complement recent improvements in Facebook's data practices.

In the foreword, Facebook's data officer criticises what he describes as "the limiting premise" in the current debate around personal data, which assumes that "the desire to innovate with data is generally incompatible with preserving individuals' rights to privacy and self-determination." In fact, he argues, there doesn't have to be a trade off at all – and it is unhelpful to talk about the amount of data companies are getting.

This is a vital consumer issue and goes to the heart of data management and data governance. The key policy question is whether consumers should accept trading their data for the benefits of 'free' services and the products of data innovation; whether they should insist upon traditional data protections where data can only be used with the conscious assent of the provider; or accept that there will be trade off which, arguably, is how many users already mediate their decisions in the digital environment. Take geolocation data, as just one example, most users know that sharing it with companies carries a certain level of risk, but they do it anyway, because popular apps like Uber and Google Maps require it, and deliver a useful service in return. Others might judge the risk too high for the benefit offered, and decide not to use these services.

Were the consumer movement to embrace a debate about personal data in terms of a contest between competing priorities, it could open the door to a more honest, constructive debate. What are the minimum data requirements for a company to run an effective service? What type – and quantity – of data are users comfortable sharing? Would the implementation of certain policies or safeguards make these red lines negotiable? Consumers have a vital role in framing these debates as well as shaping their outcomes. There is the possibility of developing partnerships with companies to explore how to strike the right balance between services and privacy.

CONSUMER GROUPS MUST PRIORITISE THE PROTECTION OF CONSUMER INTERESTS IN THE RAPIDLY UNFOLDING WORLD OF INTERNET ENABLED DEVICES

These policy questions become even more important with the advent of the so-called Internet of Things (IoT). The potential for people being surrounded by a ubiquitous range of devices is enormous

"For instance, using one of these living services, I might connect my car to my smart garage door opener, which I've connected to my smart lock, which activates my smart thermostat that I've synced to my smart lighting system. I can program them all to simultaneously interact and do their jobs when I turn onto my driveway. My experience of coming home is enhanced, since everything is acting according to my preferences.

We did an open-source analysis of IoT user behaviour, looking at 1,000 IoT technology platforms and services and more than 279,000 early adopter interactions with IoT devices. We found that consumers want an IoT that provides personalized services that can be adapted to different contexts. As with the industrial IoT, the human IoT promises to be transformative."³

Harvard Business Review

1 The Guardian website; Becoming a Guardian member, <https://membership.theguardian.com/>

2 'A new paradigm for personal data: five shifts to drive trust and growth', *Ctrl-shift*, June 2016

3 'How people are actually using the internet of things' *Harvard Business Review*, 28/10/2015

As more and more devices around us are internet enabled and capable of communicating with each other and external data holders, the internet becomes more than a way of accessing information and communication – it becomes a ubiquitous physical environment constantly gathering and analysing data to predict our behaviours and shape our lives. In this world, the question of data ownership and governance looms large. If your fridge communicates with your phone and your cooker and your security device, who owns the data that is being gathered and analysed – what are the appropriate purposes to which this data can be put? What control if any does the user/consumer have over this intimate data? These are fundamental consumer questions.

There are significant security issues that need to be addressed. A report from Samsung says the need to secure every connected device by 2020 is 'critical'.⁴ The firm's Open Economy document says, "there is a very clear danger that technology is running ahead of the game". The firm said more than 7.3 billion devices will need to be made secure by their manufacturers in the next three years. It is particularly worrying that the average spends on providing security for home devices appears to be around \$1. The consequences were seen when a massive shutdown of internet in the USA was caused by the hijacking of internet enabled devices then used to launch DDoS (Distributed Denial of Service) attacks described by one paper as "the internet of things comes back to bite us".⁵

The IoT can sound sinister – but the potential benefits are huge. For example, within the health sector the application of wearables has increasingly been seen as a pre-condition of sustaining a public health service, given the increasing demands of an ageing population with chronic health needs.

“People with conditions such as diabetes, heart failure, liver disease or asthma will wear devices, skin sensors or clothes capable of detecting deterioration and bringing this to the attention of the patient or anyone else they choose, through mobile phones. This monitoring will help keep people safe in their own homes rather than just waiting for serious deterioration necessitating an ambulance or GP call, followed by admission to hospital for several days.”⁶

Prof Sir Bruce Keogh, National Medical Director of the NHS Commissioning Board for NHS England since 2013

But to realise these benefits vital consumer interests must be addressed. For example, IoT devices are built to 'learn' our behaviours and adjust their services to suit our needs. But what is the liability of these algorithmic processes if they go wrong or are hacked? Lax US driven product

liability provisions may not provide the protections consumers need, so what would be the appropriate provisions? Consumer groups must prioritise the protection of consumer interests in the rapidly unfolding world of internet enabled devices.

Finally, there is a massive wave of technological change being unleashed – the increasing use of algorithms to make critical decisions, the development of robotics and artificial intelligence, the application of drones to civilian life, automated driving and piloting applications, all of which will have a profound impact on the way we live our lives. No-one fully understand the implications of these changes or where they will lead us.

Many companies and organisations have established specialist units to think through the implications of future technological change and its implications form their business. Consumers International will need to develop a similar capacity – in house or externally – to make sure it can contribute to public policy debates. Consumers International will also need to identify those policy arenas internationally where significant decisions are likely, such as the International Telecommunications Union which have never had a serious presence from consumer organisations.

Finally, to strengthen its ability to understand the rapidly evolving internet environment and be an effective advocate for consumer interests. It will also be useful to seek out new partnerships within both the technical and internet policy community. Given the growing importance of the IoT and its potential impact upon consumers, Consumers International could become an important junction box to connect different strands of thinking and make a significant impact upon public policy formulation.



4 Samsung, *The open economy report*, 2016

5 'Hacked home devices caused massive internet outage', *USA today*, 21/10/2016

6 'Prof Bruce Keogh: wearable technology plays a crucial part in NHS future', *The Guardian*, 19/01/2015



**CONSUMERS
INTERNATIONAL**

COMING TOGETHER
FOR CHANGE

Consumers International is the membership organisation for consumer groups around the world. Consumers International brings together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly.

Consumers International is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.

consumersinternational.org

[@consumers_int](https://twitter.com/consumers_int)

[f /consumersinternational](https://www.facebook.com/consumersinternational)