Ctrl SHIFT Understanding Consumer Empowerment

Consumer Focus
Campaigning for a fair deal

Defining and defending consumer interests in the digital age

Ctrl-Shift: Claire Hopkins, Alan Mitchell and Paul Smith

Contents

Executive summary

Consumer Focus, the statutory consumer champion for England, Wales and Scotland, has asked Ctrl-Shift to add to its body of research. The internet and new technologies have made powerful new approaches to consumer empowerment possible: most observers would probably say that, on balance, these new technologies have brought significant benefits to consumers. However, these benefits are not unqualified. There are real and potential downsides too – and that is what this particular project focuses on. The aim of this research is to build an inventory and a publicly accessible database of all the potential consumer risks and downsides or 'digital detriments' of the emerging digital age. Armed with a broad perspective and understanding of what these detriments are, consumers and consumer bodies like Consumer Focus will have greater ability to proactively work to head off or avoid these detriments before they do too much damage or become too entrenched in the system.

The research methodology involved crowd-sourcing by reaching out to Ctrl-Shift's network to build the 'long list' of potential detriments. Activities included blog posts, issuing a newsletter to a community of 600 people interested in consumer empowerment, reaching out to groups such as Consumers International, requesting feedback from the international 'Project VRM' community (focused on empowering consumers via 'vendor relationship management') and engaging with a number of experts to gather their feedback.

Qualitative analysis enabled the 'long list' of approximately 50 detriments to be categorised under eight overarching themes. These are:

1 privacy in a surveillance society;
2 digital identity;
3 information access and trustworthiness;
4 the workings of e-commerce;
5 rights and responsibilities;
6 living virtually;
7 exercise of power; and
8 changing technologies.

Any relevant references in the media and peer reviewed research that throws a light on the issues raised have been added to ensure the document is as up-to-date as possible.

To assess the impact of detriments a framework was created. Each detriment has been assessed according to its: severity/impact; scale or number of people it could potentially affect; and whether it is happening now, or in the near future. The framework shows two things. First, there are a significant number of detriments and many of these detriments are real and important – a strong counter to naive enthusiasm ('if it's digital it must be good'). Second, it is a genuine scatter diagram: no single 'meta-issue' or detriment dominates. It's not possible to say that one theme – such as privacy, or the workings of e-commerce – deserves to be prioritised ahead of others.

Ctrl-Shift's conclusions are that some of the detriments, such as the role and exploitation of personal data in modern commerce, are still new. People are struggling to understand their implications; they involve conflicting interests, values and agendas which can only be resolved by society-wide debate. We need effective instigators, leaders and orchestrators of such debate. Others, such as sharp practice in e-commerce, are simply old tricks reinvented for new times and contexts, a by-product of a still immature market. Nevertheless, they still need addressing. Yet others, such as 'internet addiction' have been raised in some quarters as detriments. Whether they are or not remains a moot point – a subject of controversy. We have included them on the precautionary principle: if some people are concerned about a potential detriment it needs to be kept under review until there is widespread agreement that the threat is not real or has not materialised.

We present five different approaches, mostly needed in some form of combination, for reducing the impact of the detriments: consumer education; further research; creating more choice; technology and regulation.

The following recommendations have been made. The need for:

- a review of the terms and conditions consumers are presented with and agree to when visiting web pages and doing business online; and
- reframing and clarifying the privacy debate.

We need much more informed debate, for society to make real choices as to where it wants to go, and (perhaps) for regulators to act with regards:

- the way new e-commerce practices affect what prices consumers are charged and how these prices are presented to consumers (the detriment 'an end to standard prices');
- ubiquitous face recognition both online and offline;
- the emergence of new web monopolies and (so far) unaccountable concentrations of power; and
- the downsides of personalisation (widely thought of as unmitigated 'good').

The list of detriments is a 'starter for ten'. Its purpose is to generate awareness, stimulate debate, and to help create an action agenda – to identify issues that need addressing. It is not meant to be exhaustive. For example, it arguably underplays issues relating to the digital divide and digital exclusion. That reflects the terms of reference of this particular research project. Adding these considerations to the list/map is one of its potential uses. The real value of this initial mapping exercise will be demonstrated over the coming years as the list is revised and extended and as we gain deeper understanding of the issues raised: it needs to be a 'living document'. We strongly recommend that Consumer Focus uses it as a means of instigating and informing ongoing debate.

Introduction

This document sets out a horizon scanning report and inventory of real and potential consumer detriments, risks and downsides of the emerging digital age.

Definition of the problem

Digital technology is now pervasive in peoples' lives. The range of products and services online is expanding. Opportunities to interact in different ways with companies, service providers, communities, friends, colleagues and other individuals are growing online. New devices and platforms such as smart phones are changing when, how and where consumers interact, use services and access information.

Whilst many of the benefits and opportunities of these developments for consumers have been documented, there has been less focus on the potential risks, challenges and 'detriments' of engaging in this new world.

Research objective

The goal of this research is to build a publicly accessible database of the potential 'digital detriments' to consumers in the medium term future (from now until approximately 2016, a five-year period), anticipating what form the detriment is taking or could take.

What is a 'digital detriment'?

By 'detriment' we mean a situation where an individual or individuals face a risk, suffer a loss (e.g. theft), incur an emotional cost (e.g. anxiety), a material loss (e.g. time and/or money), or suffer a lost opportunity (e.g. forgo a potential benefit). This definition is important because some of the biggest detriments may take the form of 'dogs that don't bark': benefits that individuals could experience but which they miss out on partly because they are not aware that the opportunities exist in the first place.

Research methodology

Building the 'long list'

To build the 'long list' of potential detriments Ctrl-Shift has 'crowd-sourced' by reaching out to our network. We have:

- issued a newsletter to approximately 600 people within our community interested in consumer empowerment;
- taken the debate to a broader international audience via the VRM community;
- reached out to groups such as Consumers International and Consumer Focus's own network;
- posted an update on our blog asking for response;
- asked for feedback from our Explorers' Club members;
- reviewed our data bank of 800 examples of consumer empowerment in action; and
- requested expert input from a panel of academic experts Ctrl-Shift has long-standing relationships with.

As the long list has been developed we have collated any references in the media and peer reviewed research that throws a light on the issues raised. We have listed and evaluated the detriments as objectively as possible.

Creating a 'short list'

Qualitative analysis of the emerging 'long list' of detriments involved reducing the list to a series of meta-issues and repeated testing of these. Eight overarching issues have emerged. These are:

1. privacy in a surveillance society;
2. digital identity;
3. information access and trustworthiness;
4. the workings of e-commerce;
5. rights and responsibilities;
6. living virtually;
7. exercise of power; and
8. changing technologies.

Assessing the impact of detriments

An impact assessment framework was created (see Figure 1). Each detriment has been assessed against four criteria:

- its severity/impact – this is an indication of the potential harm which an individual could suffer;
- its scale – the number of people the detriment could potentially affect; and
- whether it is happening now, or could happen in the near future.

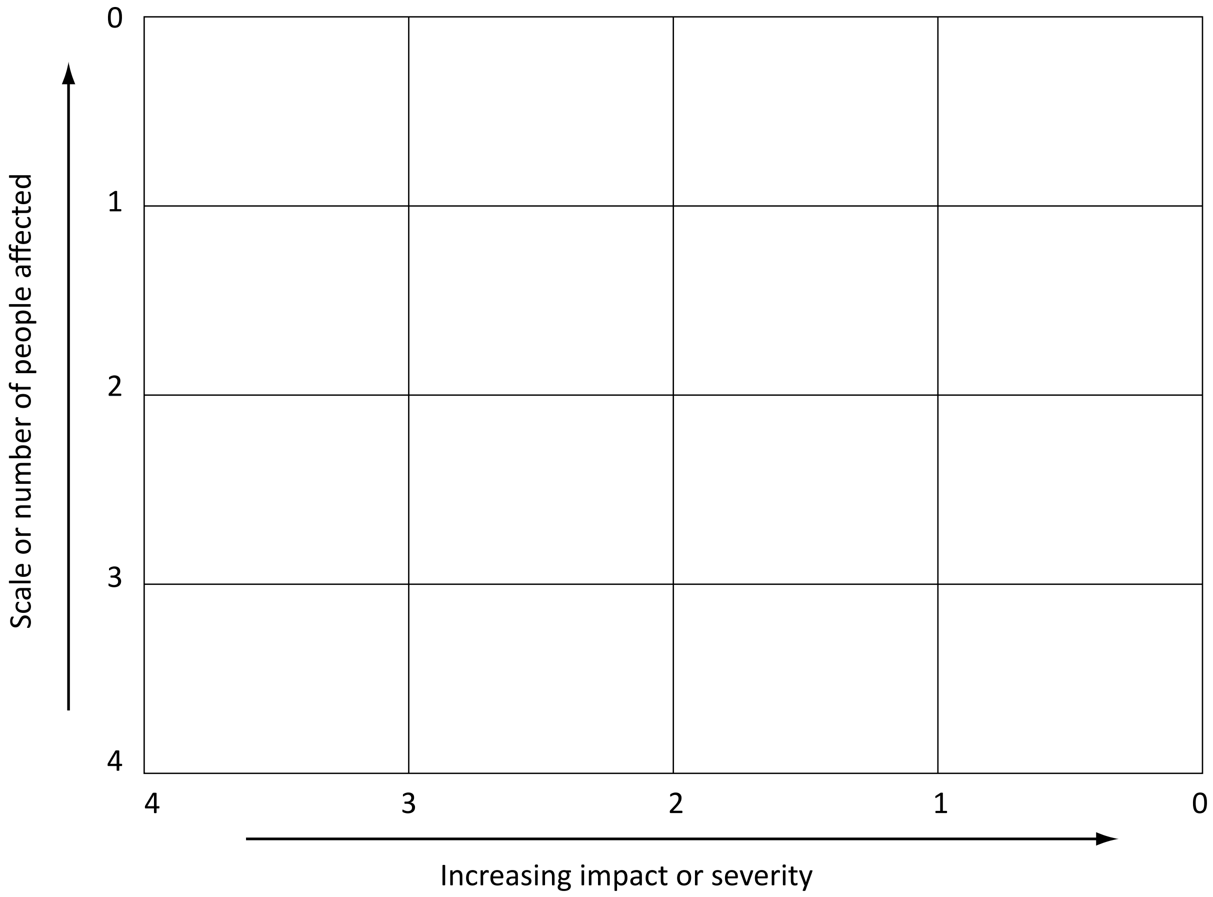

0
1
2
3
4
Scale or number of people affected
4
3
2
1
0
Increasing impact or severity

Figure 1 Impact Assessment Framework

Severity/impact

1 Could lead to severe damage – health, financial, reputation or to society.
2 Significant long-term impairment involving ongoing loss of time, money, opportunity or privacy, damage to reputation or society in general.
3 Significant one-off impairment involving loss of time, money, opportunity or privacy, damage to reputation or society in general.
4 Low level one-off impairment or irritant.

Scale

1 Affects everyone.
2 Potential to affect millions of people.
3 Affects significant but specific sections or groups of the population.
4 Affects a relatively small number.

Each of these elements – the long list, short list and impact assessment – are intended as ‘starters for ten’ designed to initiate and inform debate. They are not intended as definitive statements.

Horizon scanning

Outlined below is a list of around 50 detriments, organised into primary and secondary detriments, each falling within one of the eight meta-issues.

Privacy in a surveillance society

Not long ago 'the consumer' was a faceless entity. Mass audiences consumed TV and other forms of media. While these audiences were heavily researched using statistical techniques, there was no way of identifying individuals within these audiences, or what each individual was watching. When shopping, they paid with cash – a payment medium that kept them anonymous. Today, virtually every step of every part of daily activity generates some new digital data – data that is usually personally identifiable and captured, stored, analysed and shared. In this surveillance society privacy is a real challenge. For a recent overview of the key issues see Internet and Surveillance: The Challenges of Web 2.0 and Social Media.

Primary detriment

Whose data is it?

Nowadays, consumers leave a trail whenever they log on to the web, use their mobile phones and even when they use public transport. This information has huge and growing commercial value and the incentives to extract more and more personal information from consumers is growing. One big debate going forward is how big a share of this value should individuals receive (if any).

For this reason, none of the secondary detriments listed below should be considered solely in isolation – but in the general context of the question 'whose data is this? Who should benefit from its use? Individuals are often not aware that the data is being collected, exactly what data is being collected, by who, who has access to it, or how the data is being used. They have little or no control over these decisions even though they may also result in a loss of privacy. There is increasing tension between some consumers who are starting to recognise the value of their data and assert their rights over it, and vendors for whom information has value when hoarded.

References and resources

See How much should people worry about the loss of online privacy?

See a report from the BBC Do You Have The Right to be Forgotten Online?.

Personal data services are developing to help people manage their personal data. See Start-Up's Aim to Help Users Put a Price on Their Personal Data.

Secondary detriment

Privacy/new payment systems.

Mobile and contactless payment systems are becoming more common and resulting in the collection of large volumes of new types of personal data. As they are new and untested there are dangers of new invasions of privacy, of fraud and of identity theft, of inequitable monetisation of consumer data. Usage can show a person's location at a given time. For example, Oyster cards give a good picture of a person's movements over the London transport network. This could be used to identify travel patterns, or to intrude on someone's personal life.

References and resources

Since 2009 there has been a 90% increase in the number of contactless cards distributed across the UK, and during 2010, over 1.7 million contactless transactions were processed.

The Data Protection Act does apply to contactless payment systems, but some in the IT industry suspect that organisations which break the law aren't being dealt with severely enough.

Privacy/geo-location data.

Geo-location data is another new opportunity for data gathering, which could result in a range of valued new consumer services. However, there remain big question marks such as: whose data is this? who should have access to it? and what are the legitimate uses of this data?

Mobile phone companies are seeing location data as a new revenue stream, but how much value will consumers see of this monetisation of their data? In effect mobile phone companies are becoming consumer data companies collecting information about: who is talking to who, when; where people go, when; what services they use on the internet via their phones; what they buy using their phone; what media they use on their phone etc. Each one of these data streams is exploding. As yet, there is very little scrutiny or regulation of these new data streams, and very little understanding of the unintended consequences of their collection, analysis or use by corporations.

Geo-location data is already the subject of underhand data gathering techniques – for example 'free' mobile 'wallpaper' services whose prime purpose is to gather data on the user's location data for third party marketing purposes.

Location-based marketing is a fast-growing specialist area. Best practice says all location-based promotions and offers should work on an opt-in basis. But location-based spam is on the rise.

Services like FourSquare that encourage a person to advertise their whereabouts may also tell people the individual doesn't want informed where they are. They also advertise where the individual is not – they could be a good way of telling potential thieves when an individual is not at home, for example.

References and resources

Geo-location data is regarded as one of the main drivers of the trend towards 'big data'. See McKinsey report.

See Mobile phone geolocation, why would people want to know where you are at any exact moment, and the dangers and downsides of geo-location.

See Technology once protected our privacy, now it erodes it.

The website pleaserobme.com also highlights some of the privacy issues raised here.

Privacy/face recognition.

Ubiquitous face recognition technologies have the potential to change the sociology of society. People have grown used to the idea that in big cities they are effectively anonymous. This gives people certain freedoms – to meet people, go places without others knowing about their activities.

Ubiquitous face recognition has far-reaching implications for civil liberties and privacy.

Now, the same issues are moving online as internet companies like Facebook deploy face recognition technologies to identify the names of individuals posting pictures of themselves and their friends on the internet.

Facebook introduced face recognition by default earlier this year. All uploaded photos are run through this software, which users (640 million of them) have to opt out of, rather than opt in to. The nudge towards opting in could also cause social pressures. Opting out could create the suggestion or question: 'what or why are you hiding?'.

Google caused controversy with Google Maps and showing pictures of people and their houses without their permission.

References and resources

Courts in Germany have threatened legal action, quoting concerns over privacy and security.

See 'facial monitoring' in the Economist.

Whose shopping data is it?

Some shopping sites collect personal data and sell it to other organisations for their advertising and other use.

Their terms and conditions stipulate that this may happen but often consumers have no idea that they are 'agreeing' to these practices which are invariably buried in the small print. Consumers have little or no ability or power to control their data, opt-out or negotiate different terms and conditions.

References and resource

A study released in October by the McCann Worldgroup suggests close to six in 10 (57%) of US respondents say it is important to know exactly how their data is going to be used, selecting this as one of the most important criteria when deciding to trust a brand.

See How Companies Learn Your Secrets

Whose media usage data is it?

Under its terms and conditions Sky, for example, can collect data about what consumers watch and sell this data to other organisations. As above, consumers are not always aware of this contractual agreement, and have little or no ability or power to negotiate different terms and conditions.

Online surveillance and stalking.

Cookies are small files placed on a person's computer by sites they visit, which capture information about their movements online. Some cookies are strictly necessary for online operations to work, such as completing online shopping. Others are not 'necessary' for a specific function: their main purpose being information gathering. Some cookies are 'for the session only' while others are permanent. Sometimes cookies are placed by third parties. Many cookies are used for the purposes of behavioural targeting, which lets organisations track an individual's movements across the internet, gathering a record of which websites they visit and which items they click on. This is often referred to as profiling.

Most consumers are unaware that cookies are being placed on their computers. They do not understand what different cookies are being used for, and have no say or control over these practices.

This creates three detriments: potential invasions of privacy; new intrusive and irritating forms of advertising; and inequitable monetisation of individuals' data. This latter point means that vendors are unfairly trading with a consumer's data. There may be complex arrangements set up between commercial partners trading this data, making it almost impossible to work out who has what and how they are using it. In a bid to get round Data Protection legislation some organisations export data and transactions across borders (e.g. in gambling and pharmaceutical industries).

Current UK law requires users' consent before a cookie is placed on the individual's computer but there is uncertainty as to how this law will be implemented.

References and resource

A recent study by Stanford University has found that individual pieces of data being deposited by a person's web browser are gathered and reassembled by dozens of companies and sold.

Making money out of behavioural targeting is now big business. For example, the world's largest advertising agency WPP recently launched XAXIS which claims "to allow advertisers to target consumers with what they want, in real time."

It appears that legislation to enforce 'do not track' is still some way off, although pressure from consumers and privacy groups may force the issue.

Advertisers say there are no privacy problems with behavioural targeting because it uses no personally identifiable information: individuals are identified via a proxy – the IP address of their computers. But this is only one small step away from identifying the individual; many organisations can link a name and address to an IP address, and there are widespread concerns that 'pseudonymous' information of this sort does little or nothing to protect privacy.

Regulation of data processing by third countries is covered in the revised EU Data Protection legislation. Data can be transferred to a third country only if certain criteria are met to ensure the level of protection of individuals for the protection of personal data.

See Google's iPhone Tracking.

Privacy/smart meters.

Smart meters recording consumption of energy use will soon be in all UK homes (the Government is committed to a deadline of 2020 for this). The devices will contain a raft of personal information such as when occupants go to sleep and when they are out, raising security concerns.

References and resource

See Why smart people are suspicious of smart meters.

Lack of complete awareness.

Often the consumer lacks visibility at the actual data level of what is being shared or stored. Although the consumer may give consent to the outward manifestation of a transaction, it's what happens to the data at the back end that determines whether or not there are more serious causes for concern, for example iris scanning at airports.

Primary detriment

Unfair terms of data sharing.

It's becoming a saying on the internet: "if it's free, you are the product". In other words, the service makes its money by collecting and selling the data it collects about the person in the course of using the service. However, individuals may have no control over who this information is shared with or what purposes it is put to. Their privacy may be compromised. They may have no idea just how much commercial value they are giving away 'for free'. This can become a highly profitable way of exploiting consumers' ignorance about the value of their personal data.

Currently, the terms under which individuals' data is captured and shared is set by terms and conditions which consumers have to 'agree' to (by ticking a box in an online process) if they want to access the product or service in question. Most consumers do not read these T&Cs, and have no means of influencing their content if they do. Moving forward, a major benefit will be mechanisms that let consumers stipulate data sharing permissions. Consent mechanisms and the technology behind them may be too immature: it's too easy for people to 'click the app' and proceed.

References and resource

A recent review of data sharing in the UK by Richard Thomas and Mark Walport found a "fog of confusion about the circumstances under which personal data can be shared".

According to the Guardian, "Facebook outraged civil liberties campaigners after introducing new privacy settings [in 2009] that could dramatically increase the amount of personal information people expose online". The 2009 changes required that personal profile information be viewable to everyone. Previously, Facebook users could limit the people to which that information was visible.

According to The Wall Street Journal in November 2011 "Facebook Inc. is close to a settlement with the U.S. government over charges that it misled users about its use of their personal information....the settlement would require Facebook to obtain users' consent before making 'material retroactive changes' to its privacy policies. That means that Facebook must get consent to share data in a way that is different from how the user originally agreed the data could be used."

"Facebook Privacy: Site Confirms It Tracks You After You Leave."

See also a recent study by the Direct Marketing Association – social media sites not trusted with personal data.

See also "Down and out in EULA-ville"

"These days, we overwhelmingly ignore every single notice that appears on our computers and phones every time we install, update, or sign up for something, whether it's an End User License Agreement, a list of Terms of Service, or just a plain old Agreement. And we're raising an entire generation to have even less respect for the fine print. But we're also inundated with unexpected fees, nasty online privacy violations, and the sinking sense that none of us knows exactly what our devices can and can't do."

Confusion is compounded by the fact that many services are hosted overseas where different laws apply to those of the UK.

Excessive data gathering.

Under UK law, personal data should only be obtained by a company for specific purposes and should not be used for other purposes. Furthermore, the data collected should not be "excessive in relation to the purpose or purposes for which they are processed". However, in the current environment some companies are tending to collect as much data as they can, and to use it for as many purposes as possible.

In some instances, there can be a mismatch between the level of consent the consumer thinks they have given and the amount of data that is collected; and also between the level of consent requested and the amount of data actually required to carry out a service on a consumer's behalf. There are little or no practical ways for individuals to monitor or control what is going on.

References and resource

See ICO guidance on the Data Protection Act.

Digital identity

Consumers are placing large amounts of information online – credit card details, bank details and addresses when they buy goods or services, their personal likes/dislikes on social networking sites such as Facebook, Twitter, and even their work history on Linkedin. Managing and protecting identity online is, therefore, becoming more complex.

Primary detriment

Identity theft.

Identity theft is becoming easier as individuals place large amounts of data online. Date of birth, address, full name and place of birth will often provide an identity thief with enough information to use a consumer's identity.

References and resource

A report in ComputerWeekly found that criminals need only three pieces of personal information to steal someone's digital identity to commit fraud. The UK Serious Organised Crime Agency (Soca) estimates online fraud is costing UK internet users around £3.5bn a year, and that 11% of the UK's online community has been a victim of fraud in the past year.

Figures from Financial Fraud Action UK (the organisation which the financial services industry co-ordinates its activity on fraud prevention) estimates that online banking fraud losses totalled £16.9 million during January to June 2011.

In October Sweden suffered its worst internet security breach in its history.

According to the Norton Cyber Crime Report for 2011, 431 million adults worldwide were victims of cyber crime in 2010. The total cost of those crimes amounts to $114 billion. The report also found 10% of respondents had experienced cybercrime on a mobile device.

Cybercrime laws do exist, but enacting them is extremely difficult.

See also Callcredit warns online shoppers to keep personal details wrapped for Christmas.

Secondary detriment

Spoofing.

Email impersonation (spoofing) is on the rise. It is email activity in which the sender address and other parts of the header are altered to appear as though the email originated from a different source. Because core SMTP doesn't provide any authentication, it is easy to impersonate and forge emails.

References and resource

The FBI's Internet Fraud Complaint Center (IFCC) has seen a steady increase in complaints that involve some form of unsolicited e-mail directing consumers to a phony "Customer Service" type of web site, contributing to a rise in identity theft, credit card fraud, and other internet frauds.

Phishing.

Phishing is also a rising problem. It is a way of attempting to acquire information such as usernames, passwords and credit card details by masquerading as a trustworthy entity.

Primary detriment

Pretend anonymisation.

Some activities, like making a cash payment, are intrinsically anonymous.

Other activities use data that may be 'anonymised': with the name, address or other identifying information removed, or data may be 'pseudonmyised' with a name replaced by a code number, for example.

Many activities, such as behavioural targeting of online advertising, are justified on the grounds that no personally identifiable information is traded. However, it is often possible to work backwards from a pseudonym (such as a computer's IP address) to the name of an individual. It's also possible to conduct 'inference attacks' which identify an individual by a pattern or collection of data, or to cross-match data.

References and resource

See Inference Attacks by Third-Party Extensions to Social Network Systems for an explanation of how third party Facebook plug-ins can harvest personal information.

In the revised EU Data Protection legislation there is a tightened restriction on 'pseudonymous' data via a new definition of the data subject: "'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."

Data loss by individuals.

For individuals it's bad enough when their computer crashes and they lose precious photos of their holiday or wedding. As more and more of consumers' lives go online, the potential loss and harm of data loss could be far more dramatic – for example, loss of crucial financial or health records, or loss of phone numbers and important messages.

Data loss by corporations.

Centralised customer databases are a natural target for thieves and fraudsters. There have been a number of high profile cases of companies' databases being compromised and records stolen, or data simply mislaid through careless handling.

There are also cases where corporations decide to delete or cease to provide access to cloud-stored data, eg Flickr groups.

References and resource

For example, in April 2011 thieves accessed records, including credit card details, of 77 million users of Sony Playstation; the NHS has lost millions of patient records through careless handling, leading to the Information Commissioner calling for tougher penalties for NHS Trusts and hospitals which lose data.

See Councils breached personal data 1,035 times over three years.

Lack of control using social media sites.

It's not always easy or possible to manage or set the right privacy settings to control when individuals share information and who with. For example there has been much controversy about Facebook's privacy settings and their launch of Open Graph technology.

References and resource

See a recent article in the Guardian – "Facebook's Open Graph technology allows third-party websites to tell Facebook what people are doing. It extends Facebook's Like button to include any action that the site owners think might be interesting to Facebook."

See Facebook is Using You.

Poor control of data histories.

As use of social media becomes the norm people are sharing ideas, actions and photos with each other online, perhaps not realising the difficulty of removing them later in life.

References and resource

A study in June 2011 of 1000 individuals found over half the respondents under 25 years old said they regret posting something online. Over 25% of those who regretted their post said it ruined their marriage or relationship or caused problems at home or work. Even high profile individuals have fallen into this trap – including Church of England bishops.

Abuses of online reputation management.

Online reputation management systems can aid consumer protection, particularly by sorting good suppliers from bad ones. However, they also have some potential drawbacks. It's often easy for a rogue trader to discard a bad reputation and set up under a new name; and it's hard to rehabilitate offenders. An individual or service may earn a bad reputation and work hard to address the faults identified. But there may be no mechanisms for the individual or service to say 'we have changed', and no mechanisms for out-of-date or inaccurate information to be withdrawn.

Reputation systems can be gamed in many different ways. For example, one recent promotion offered consumers the chance to enter a prize draw for free, so long as they 'liked' the brand on Facebook.

References and resource

Online reputation management is now starting to become big business; clients include individuals or businesses who have been wrongly associated with criminal or shady activity; and individuals or companies wanting to portray a positive public image. Online reputation management companies tweak search engine data, but admit it's next to impossible to completely remove negative information.

Digital gossip.

Information posted online about individuals can spread worldwide within minutes. Even if it is true, it can be extremely distressing for

the individual. Sometimes, however, it's not true and the individual is powerless to correct it. They could be pursued for a false crime, or even deported or charged for a tweet. This is not just a problem for pop stars and politicians. It can affect every individual in a social network.

References and resource

Digital gossip and naming and shaming can have unintended and occasionally severe negative consequences – see 'The future of reputation – gossip, rumor and privacy on the internet' by Daniel Solove (Yale University Press).

The need for 'digital wills'.

When individuals die it isn't clear about who has the right to access their a digital information. There may be a requirement for digital wills.

References and resource

Professionals in the legal, funeral, and estate planning professions are starting to come to grips with the problem of what to do with information after death. Companies such as Legacy Locker and Entrustet have sprung up to handle the legal and financial issues of data after death and there have been a series of Digital Death Days intended to educate the industry about the problem.

Poor online identity management.

To do business online individuals need to be able to prove they are who they say they are. Often, companies require individuals to provide information that's far in excess of what's needed to identify them.

In other cases, the identity systems being used are not robust (see credit rating mistakes below).

References and resource

In 2011 The US government published a its National Strategy for Trusted Identities in Cyberspace.

In the UK the Government is spending £10m on the ID Assurance scheme, which will be the means through which citizens electronically provide their personal details to access government services. The programme is suggesting the creation of a new private sector market for online identity providers. It is not clear, yet, what safeguards and protections will be put in place for consumers using these new services.

The UK system will avoid a single identifier approach, where a fixed piece of information is used to identify an individual. Instead it will apply data minimisation (the only data passed across is the data that needs to be passed across) and decentralisation to mitigate the risk of fraud.

The line between collecting too much or too little information about an individual is a fine one to tread – in certain circumstances collecting too little information can have serious consequences, for example enabling identity theft to occur more easily. See 'Privacy and Identity Management'.

Credit rating mistakes.

Credit ratings can be based on flawed or incorrect personal data held by third parties. Sometimes the individual isn't even aware of the data sources which constitute the rating. Rectifying mistakes is often difficult and time consuming.

References and resource

According to a recent study paid for by the Consumer Data Industry Association (the trade group for the credit bureaus that assemble and sell credit reports), fewer than 1% of credit reports contain inaccuracies. Consumer advocates are skeptical as previous estimates of credit reports with serious errors vary widely, anywhere from 3% to 25%.

See Energy Providers Criticised over Credit Checks.

Information access and trustworthiness

Technology has brought about significant changes in the amount of information that is available online, as well as the way people search and access what they want to know and when. More information is available to people, but is all the information online to be trusted? Issues of transparency and control are exacerbated with online information.

Primary detriment

Naive faith in P2P information.

One of the strengths of the internet is that it can be highly democratic. Consumers can have their say and input their views. This can be extremely valuable – a lone customer's complaint can gain attention and force a large corporation to change its policies, for example. However, one potential downside is it's no longer possible to distinguish between good quality and poor quality information.

There are some situations where the 'wisdom of the crowd' works well. But not always. Sometimes we need experts. But online, there is not a good way of drawing the line between these two types of knowledge.

Traditional quality control methods such as newspaper editorial processes and peer reviews in academic journals can still safeguard against the distribution of poor quality information.

References and resource

See 'The balance between crowd sourced and expert opinion'.

See ABC news, reporting a study in the New England Journal of Medicine which found popular search engines often direct users to sites with misleading or even harmful information on drugs.

See 'You are not a gadget' by Jaron Larnier.

Deliberately misleading online information.

There have been well-publicised examples of organisations misleading consumers through paying bloggers to upload positive comments about their organisations.

References and resource

Wal-Mart was discovered to have paid two US bloggers to post positive comments about Wal-Mart stores as they travelled across the US. When the press discovered this, Wal-Mart and its PR firm took the brunt of a massive backlash and were publicly humiliated. But of course many consumers probably fell for this subterfuge.

Reevoo recently published their trusted reviews manifesto to ensure only genuine reviews are posted. The answer could lie with providing consumers with a mixture of consumer comment, professional reviews provided by commercial entities and trusted comparative information.

Secondary detriment

Abuse of online feedback systems.

Online feedback systems are used by organisations such as eBay or Amazon to build trust and foster co-operation between users but they are open to corruption if consumers post incorrect and deliberately misleading information. This is also the case for sites such as TripAdvisor that is clamping down on false reviews.

References and resource

See 'Some eBay users Abuse Auction Sites Feedback system'.

See Hotelier sues TripAdvisor after accusations she wrote fake positive reviews causes revenue to plummet by 75%.

Abuse of comparison sites.

Comparison sites – increasingly popular for researching and making decisions – can be open to manipulation of results causing misleading information.

Primary detriment

Fact or promotion.

It's not always easy to see the difference between advertising and editorial online. Consumers may be misled into buying purchases through manipulative promotions. This could be a worrying issue for children in particular.

Online scams.

Online, the full buying process isn't visible: individuals have to go from page to page not knowing what the next page has to offer. Unscrupulous businesses lure customers in with 'bargain' headlines and add extra costs at each new step. A classic example is airlines which add extra charges for luggage or paying by credit card.

References and resource

An investiagation in Brooklyn, New York in 2009 found that online retailers have used 'bait and switch' techniques to defraud consumers with non-existent cheap deals. The online retailers agreed to pay to settle complaints brought by the New York State Attorney General's office and to change their business practices.

Faux openness.

Google claims to organise the world's information. It does not and cannot. It can only organise the information that people want made public (i.e. searchable). Google is, therefore, helping to create a two tier information environment: an easily searchable environment which gives the appearance of openness and comprehensiveness, but one which helps to hide a much bigger 'dark' layer of information that has been kept deliberately unsearchable. (This is no different to keeping files secret in an office – but the influence on actual behaviours is different because individuals have become so search dependent.)

References and resource

See '5 myths about the information age' by Professor Robert Darnton, a Harvard University librarian.

Deception.

When searching for information online consumers click on information but it is not what it purports to be. Links take the reader to a different page or initiate another undesired or unintended action.

Deception could also take another guise.

Consumers think they are dealing with one organisation they trust but in fact this is just a front. The back office and operations are managed by another 'masked' organization that the consumer may not have chosen to do business with.

The gaming of search.

Once upon a time there was a clear distinction in search results between paid-for results and editorially independent results. Now, however, the search engine optimisation (SEO) industry means that, increasingly, the first page of search results direct users to commercial interests which are not necessarily germane to the information they are searching for.

References and resource

See how the department store JC Penney gamed Google to ensure their website came top for many home product searches.

Searching vs biasing.

In December 2009 Google started tweaking the search results it shows individuals according to the data it holds on them – for example, what they have searched for before. This means that, over time, no individual putting in the same search query will see the same results: what search results show is not 'what's available out there' but 'who Google thinks you are'. What's more, people are unaware of this bias because it's invisible. Search is no longer a window to the world but a mirror. This could, potentially, highly constrain people's practical ability to access the information they want and need. Also if people only see information that reinforces their existing beliefs or prejudices, they are not exposing themselves to a wider body of knowledge, alternative opinions or facts.

References and resource

"With Google personalized for everyone, the query 'stem cells' might produce diametrically opposed results for scientists who support stem cell research and activists who oppose it. 'Proof of climate change' might turn up different results for an environmentalist and an oil company executive. In polls, a huge majority of us assume search engines are unbiased. But that may be just because they're increasingly biased to share our own views. More and more, your computer monitor is a kind of one-way mirror, reflecting your own interests while algorithmic observers watch what you click." (Edited excerpt from Eli Pariser's book The Filter Bubble: What the Internet Is Hiding from You.)

The workings of e-commerce

Faster internet connectivity and new technologies have resulted in the rise of e-commerce. Although there are many opportunities provided by e-commerce, there are downsides too.

Primary detriment

The end of 'fair' prices.

Ever more granular data means organisations have the ability to identify ever more granular costs – and to charge people accordingly. This may mean that some 'more profitable' consumers end up paying more to cover the costs of those that are 'less profitable'. The question is, is this unfair or not?

References and resource

Companies are already beginning to talk about 'sacking' unprofitable customers.

The end of price transparency.

What is the 'real' price of an air ticket? Once, there was a single price consumers could understand. Now there is a headline price and multiple extra charges: for luggage, for changing bookings, for using different channels or payment methods.

This makes the decision-making process more complex, makes the buying process laborious and irritating and creates opportunities for sellers to take advantage of customer confusion to charge higher than necessary tariffs. easyJet and Ryanair have led the way with these practices, prompting a Which? supercomplaint on their card charging policies.

Pricing pot luck.

Airlines have been doing it for years. But now the practice of dynamic pricing is spreading to increasing numbers of online retailers – that are changing prices by the minute, often according to information they have about individual customers and their behaviours. Several questions arise from this. What's a fair price when there isn't 'a standard price' for the product or service any more? How are customers supposed to know what a fair price looks like? How can price comparison services work effectively in such an environment? For people who don't have the time to shop around. these additional complexities are creating an unwelcome trade-off: they either have to invest more time researching best deals or accept that often they may end up paying over the odds.

References and resource

In 2000, Amazon charged different customers different prices for the same DVD, based on the customers' address and purchasing history, in effect looking at a consumer's 'willingness to pay'. Initially a PR disaster for Amazon, dynamic pricing is now commonplace.

The death of the high street.

As online shopping grows the high street is under threat as a place to source the essentials of everyday life. This has a potential social cost including loss of diversity and convenience.

At one level, the decline of high street retailing may be regarded as the simple workings of competition. But it may nevertheless bring unintended social costs, especially for those who remain dependent on the high street for their shopping.

References and resource

Verdict Research quotes UK shoppers spending more than £37bn a year by 2014, with the e-commerce market growing by £14bn, or 61% on 2010 spending, over the next three years.

'Traders will shut shop to focus on selling online and through m-commerce – and this will change the way the high street works', says Verdict.

Exclusion.

Customers sharing information about their suppliers can help them 'police' suppliers' behaviours. But suppliers can use this information to punish customers who criticise them. This potential for exclusion is a downside of the new openness.

The other angle of exclusion is caused by organisations that only adopt a social sign on system such as Facebook or Twitter. If an individual doesn't have access to these they are potentially unable to access or use the service.

References and resource

eHow faced a backlash from users on Facebook only login.

Poor or non-existent customer service.

Providing good customer service is expensive, which is why many companies make it as hard as possible for customers to actually speak to them. Without the ability to speak to someone, customers have one of two options: sort out the problem themselves (whereby the company transfers the cost of customer service to the customer); or not have the problem solved.

References and resource

A YouGov survey in 2010 found more than a third (35 per cent) of UK web shoppers would spend more money online if better customer care or advice was offered. And a Harris survey found 82% of customers had stopped doing business with an organisation due to poor customer service.

‘Always on’ temptation.

Does the ability to purchase online 24/7 encourage people to spend more money and purchase goods and services on a whim? Consumers are disconnected from handing over the actual money.

References and resource

Tactics such as baiting and drip pricing encourage consumers to spend more online.

The Office of Fair Trading found only one in five internet retailers fully complied with consumer laws, and that unfair pricing was a common issue.

Interoperability and data portability.

The Institute of Electrical and Electronics Engineers defines interoperability as “the ability of two or more systems or components to exchange information and to use the information that has been exchanged”. A lack of interoperability can restrict competition as customers get locked in to the offerings of one particular supplier. This can happen ‘by accident’ (because of the technical standards adopted by different suppliers) or deliberately. For example, Apple has adopted a ‘walled garden’ approach to what applications, content and devices can be used on its platforms. The same effect can be achieved if a service relies on data provided by the customer and the customer finds s/he cannot transfer this data from one service provider to another.

The potential restrictions of poor interoperability and lack of data portability are potentially enhanced by the widespread adoption of cloud computing.

References and resource

Data portability is the subject of a long-running row between Google and Facebook.

Rights and responsibilities

Understanding rights and responsibilities regarding data sharing is becoming more complex; consumers may unintentionally infringe laws and contracts, and make spending commitments.

The global online environment also makes understanding rights and responsibilities difficult for organisations as well as consumers.

Primary detriment

Regulatory bypass.

The internet is a global phenomenon that can, and often does, make a mockery of local regulation and legislation. This raises many profoundly important questions as to how consumer protection regulation and legislation is supposed to operate in this new global environment.

References and resource

The Information Commissioners Office which provides independent advice and guidance about data protection and freedom of information to consumers, is dependent on reacting to consumer complaints. Consumers or organisations can't proactively conduct audits for example.

However, the Office of Fair Trading does have investigatory powers.

Poor regulation of data sharing.

Traditionally, issues of personal data sharing are covered by privacy legislation. This legislation is: hard to understand; leaves issues of 'property rights' and commercial value open to abuse by organisations; and makes redress difficult.

References and resource

The SOPA, PIPA and ACTA agendas are creating uncertainty and tension between rights holders and law enforcement on the one side and consumers on the other.

Regulation behind the times.

There are many ways in which consumer protection legislation and regulation have failed to keep pace with what's happening online.

Digital products delivered in the process of downloading or streaming are not considered to be 'tangible goods' and so are exempt from the consumer's right to redress. As a result, consumers buying digital goods and services are exposed to risks where products are not fit for purpose or undelivered. This exacerbates the issues highlighted below.

There may also be questions around who owns management of the security of a service, and where the responsibility for this lies ("Verified by Visa" is an example of such a transfer of responsibility).

References and resource

A Consumer Focus project underlines the many ways in which online shopping fails to give consumers the protection they enjoy elsewhere.

Areas needing updating include information requirements on terms and conditions, product specification and complaints systems. See also 'Consumer Rights in Digital Products'.

Incomprehensible small print.

Unintentional and contractual legal breaches can arise simply because people find reading and understanding terms and conditions, which can sometimes be excessively complex, difficult.

Liability avoidance.

As banking went electronic banks tried to shift the burden of responsibility away from themselves, and on to the consumer when online fraud is committed. In the new Banking Code, 'customers [are] regarded as liable for losses from their bank (e.g. from hackers gaining access to their account) if they do not act with reasonable care.' But how do you define, 'reasonable care'? Now similar issues are being raised with mobile phone payments, especially relating to subscriptions and gift card payments.

Evasion of product liability and consumer rights legislation.

Products are increasingly becoming reliant upon services to back them up, e.g. the apps which help a smartphone fulfill its potential, or where a purchaser does not possesses the material object, merely has access to its service, such as types of computer software.

This may impact and cause a loss of consumer rights in terms of product quality, second-hand resale, loaning, returns, or refunds. Also in such instances, does the consumer actually own the product they have bought?

Consumer 'lock in'.

When services use proprietary technology, this can cause unnecessary 'lock in' for consumers.

References and resource

See Cory Doctorow, 'The Coming War on general purpose computation'.

Over-complex service agreements.

Use of Service agreements are often very hard to understand. Individuals only discover what they have 'agreed' to after buying the product, and must accept to use it (e.g. the iPhone OS 4.0 Terms of Service, released in April 2010, prevented developers from using non-approved code). Again, do consumers also always own the product they've bought?

References and resource

Sony has tried to take legal actions over Playstation owners who have tried to modify their playstations, raising the issue of who owns the product you've bought.

Small print contract commitments.

There are instances when organisations link consumer 'free' offers to a commitment to purchase in the future. Consumers may opt-out online to such an agreement, but sometimes there are no obvious reminders and unintended purchases are undoubtedly made.

Legal jurisdictions.

When buying online it's not always obvious where the seller is based or what legal jurisdiction they operate under. If the seller is based outside of the UK or EU, consumers may not have the legal protections they believed they had.

Exploiting social CRM.

Companies are increasingly using social CRM to engage customers via using social media. For companies, harnessing the power of the customer voice to improve customer service can both improve service and cut costs. However, at a certain point it can become a way of outsourcing the cost of customer service back to customers.

Exploiting crowd-sourcing.

Wikipedia defines crowd-sourcing as "the act of sourcing tasks traditionally performed by specific individuals to an undefined large group of people or community (crowd) through an open call". Enabled by Web 2.0 technologies many companies now routinely canvass their customers for opinions and suggestions relating to current and future products and services. This feedback can be very valuable; some of these ideas may be commercially valuable, even patentable. At a certain point, this sort of crowd-sourcing can become a highly profitable way of appropriating the value of other people's ideas for free.

References and resource

See Crowdsourcing: 5 reasons it's not just for start-ups anymore for an overview of how crowd-sourcing can be used.

Dell conducts online conversations and crowd-sourcing with its customers via IdeaStorm.

First Direct bank overhauled its website after collecting ideas from customers through its crowdsourcing portal.

Living virtually

Spending too much time online could become a substitute for having a meaningful life in the real world leading to problems for the individuals and for society at large.

Primary detriment

Compulsive internet use.

Some people argue that compulsive internet use can interfere with daily life, work and relationships and has been described as an addiction, similar to a drugs or alcohol habit.

References and resource

A UK study has found a strong link between heavy internet use and depression. The study, reported in the journal Psychopathology, found 1.2% of people surveyed were "internet addicts", and many of these were depressed. The addicts were significantly more depressed than the non-addicted group, with a depression score five times higher.

Accurate estimates are hard to find as the internet tends to be accessed from home. However in Asia, where internet cafés are frequently used, some data does exist. In South Korea, which has the greatest use of broadband in the world, 10 people died from blood clots from remaining seated for long periods and another was murdered because of an online game. South Korea now "considers internet addiction one of its most serious public health issues".

Overuse of social networking sites.

Some people argue that social networking could become a substitute for friendships in the real world. It could also increase the pressure on individuals to conform.

References and resource

See 'Alone Together' by Sherry Turkle, which argues that social networking provides "the illusion of companionship without the demands of intimacy". The book argues that "the relentless connection" of online is actually leading "to a new solitude".

The number of people using social networking sites is huge. Nielsen' Global Faces and Networked Places report found that two-thirds of the world's internet population visit social networking or blogging sites. As of June 2011, social networking accounts for one of every six minutes spent online. Facebook has increased average U.S. visitor engagement from 4.6 hours to 6.3 hours per month over the past year. In March 2011– LinkedIn reached 100 million professionals worldwide and is growing at roughly one million new members every week. Facebook has 640 million users worldwide, Twitter has 175 million registered users ands Flickr hosts more than five billion images.

Deskilling.

Speed of communication using technology encourages people to use shorthand, for example when sending text messages. Some argue this degrades the quality of communication: peoples' vocabulary is decreasing and use of 'correct' grammar is deteriorating.

References and resource

For example, in his book 'The Shallows', Nicholas Carr argues that "the Net is literally re-wiring our brains inducing only superficial understanding."

Secondary detriment

Inability to convey complex messages.

Communicating simple ideas can become easier using technology but conveying more complex or subtle messages can be harder.

Cheating.

Ease of access to information on the internet can decrease the need for people to understand or create answers for themselves. Cheating during exams using mobile phones is increasing, for example.

References and resource

See high tech exam cheating is on the rise says Ofqual.

Primary detriment

Weakening of society's rules.

Concern has been expressed in some quarters that the internet enables and/or encourages anti-social and harmful attitudes and malicious behaviours. Issues raised include: online bullying; trolling or posting inflammatory provocative comments; easy and free access to pornography; child sex grooming via social media sites; and recruitment to suicide clubs. There is an important and ongoing debate to be had about how online environments affect socially accepted norms and rules and how they change these rules and norms.

These issues can be particularly acute for young people who are able to participate in new online services through technology advances, but who may not understand how to conduct themselves safely and securely.

Online anti social behavior can also cause a 'crisis in engagement' preventing people from enjoying and maximising the opportunities created through digital technologies.

References and resource

E-safety is an important part of safeguarding children in schools. The focus is on educating children to understand about safe use of the internet.

Facebook promotes peace through 'Peace on Facebook'. "By enabling people from diverse backgrounds to easily connect and share their ideas, we can decrease world conflict in the short and long term."

Exercise of power

Technology is reinventing the ‘rules of the game’ and there are new organisations emerging, different in character to the old ones, wielding an unaccountable hold over individuals.

Primary detriment

New web monopolies.

In many markets Google and Facebook are de facto monopolies (depending on how ‘monopoly’ is defined in local law). They now include a sprawling range of activities. But how are they monitored and regulated? For example, the algorithms Google uses to serve up search results are a closely guarded secret. This secrecy is designed to stop the gaming of search. However, in doing so, it arguably concentrates more power in the hands of the algorithm developers than any former media magnates’ ability to control the news: the algorithm decides what you see, but you cannot see what’s inside the algorithm.

References and resource

See ‘The time has come to regulate search engine marketing and SEO’; this is in stark contrast to the opinions of Facebook and Google CEOs who warn against any attempts to regulate the internet.

Existing competition regulation has struggled to keep up because of the speed, complexity and blurring of industry boundaries (although this does beg the question of how online market dominance should be measured). In some cases Vertical Agreements Block Exemptions (VABE) make regulation online more complicated. For information on VABE see an overview by legal firm Pinsent Masons.

See also the plenary session of ITU Broadband Commission where the issue of regulation was discussed.

See ‘Google Reveals 10 Tweaks to Search Algorithm’.

See ‘The Master Switch’, by Timothy Wu. In this book Wu shows how every ‘new media’ has started with a wave of optimism and openness only for it, in time, to “become a closed and controlled industry”. His analysis suggests that this is already happening apace with the internet. He concludes: “we have evolved into a society in which electronic information represents the substrate of much of daily life … Let us, then, not fail to protect ourselves from the will of those who might seek domination of those resources we cannot do without”.

Potential abuse of dominant positions.

Strong commercial market players are trying to dominate the online market and spread their footprint. This could stifle competition and have a long-term impact on consumer choice and value for money.

References and resource

See Amazon’s profits fall sharply in third quarter

“Founder and chief executive of Amazon.com Jeff Bezos has increasingly used Amazon’s cash to expand the business into the digital domain. As well as the new Kindles this quarter Amazon struck deals with Twentieth Century Fox and PBS to stream movies and TV shows from their vast libraries. It already has deals with CBS, Sony, Warner Bros and others.”

Threats to internet neutrality.

People assume the internet is neutral, with no restrictions by Governments or ISPs on content, sites, traffic or forms of communication. But the internet runs on software and hardware owned by large businesses and it’s their job to make money. Current US regulations prohibit wired broadband providers from blocking lawful content, applications, services, and non-harmful devices. They are also forbidden from discriminating in the transmission of lawful network traffic. Wireless providers are also barred from blocking lawful websites or applications that compete with voice or video services. These rules take important steps to ensure that the internet remains an open marketplace, but the rules and their creators have critics who say they don’t do enough to stop the phone and cable companies from dividing the internet into fast and slow lanes and they fail to protect wireless users from discrimination that is already occurring in the marketplace. The potential detriment for consumers is that unless internet neutrality can be guaranteed, those who run it may try and control it.

References and resource

See FCC Publishes Net Neutrality Rules.

Changing technologies

People are living in a period of exponential technology change and this is likely to continue for the next ten or 20 years. Moore's law states the power of computers is doubling ever 18 months. The capacity of the backbone of the internet, the fibre, is increasing, as is storage capability whilst maintaining the same cost. But can consumers (and policy makers) keep up with and capitalise on the opportunities brought about this growth? Do we have the cognitive capacity to cope with the scale of new information challenges in a digital world?

Primary detriment

Artificially created needs.

As technology advances driving new capabilities consumers are encouraged to buy the next 'best thing' when perhaps they don't always 'need' it. For example upgrading smart phones.

Excess obsolescence.

Technology advancements make some products and services obsolete so quickly people are forced into repeat purchases, spending money just to keep up.

Inadequate regulation.

Technology is advancing so fast that regulators may not be able to understand what it is being achieved and what the implications for consumers are.

Technology advances may also help organisations find loop holes in regulation and exploit these to the detriment of consumers. History sniffing is an example of this.

References and resource

See 'What you should know about history sniffing'.

Digital divide.

The digital divide is invariably discussed in terms of those who have access or not to technology and digital devices. But there is also a digital divide in terms of people's digital literacy. People have differing: understanding of privacy issues and protections; awareness of availability of services; knowledge of where to look for information and advice; knowledge of how to use technology and services.

People with disabilities are also sometimes unable to access online information.

Issues relating to people's skills and capabilities all generate knock-on effects such as the obligation to use a particular service. There's a big difference between people wanting and choosing to use digital channels and them being the only option. Also personalisation of government services could, without meaning to, restrict access. Overcomplicated bespoke services could 'turn off' users.

References and resource

See A look behind the digital divide.

Organisations such as JISC work with universities to embed core digital skills into the curriculum because it gives students the best chance of success.

Raceonline2012 aims to inspire, encourage and support millions more people online by the end of the Olympic year 2012 through partnership with government, industry, charities and individuals.

Martha Lane Fox is UK Digital Champion. According to Raceonline, “Her remit includes advising government how to provide better, more efficient online public services and accelerating efforts to help more people benefit from the power of the internet.”

The dark web.

New technology is enabling virtually untraceable global networks used by criminals.

References and resource

See The dark web: Guns and drugs for sale on the internet’s secret black market

Additional reports

Please see the Future Consumer report from the Australian Communications Consumer Action Network. This was developed several years ago and helped to shape their strategic plan.

Analysis

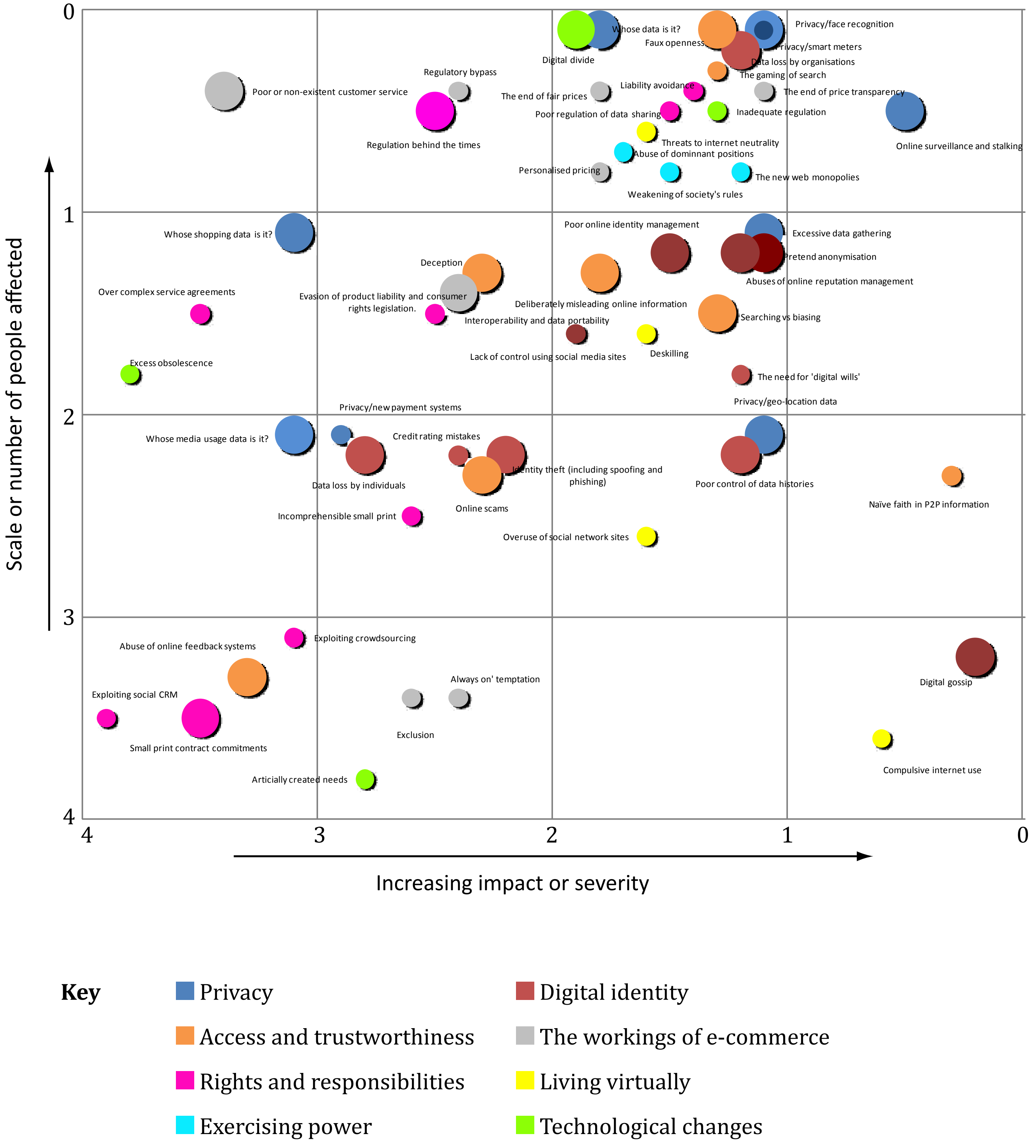


Figure 2 Digital Detriments Impact Assessment Framework

Mapping the detriments

Figure 2 gives an initial top line assessment of the impact of each detriment along two dimensions: the number of people affected by the detriment and how badly they are likely to be affected. The size of the dot represents immediacy: the bigger dots are 'clear and present' detriments, the smaller dots are dangers and risks which may or may not be realised in the future.

A quick glance reveals two things:

- first, there are a significant number of detriments and many of these detriments are real and important – a strong counter to naive enthusiasm ('if it's digital it must be good'); and
- second, it is a genuine scatter diagram. No single 'meta-issue' or theme dominates (although the broad issues of online 'stalking' and surveillance reaches the top right hand box affecting large numbers of people with high impact). According to this initial survey, it's not possible to say that one theme – such as privacy, or downsides of e-commerce – deserves to be prioritised ahead of others. A systematic approach is needed.

Conclusions

The online environment is a wonderful thing in many ways, bringing increased access to information, transparency, convenience and new means of communication to millions of ordinary people. New opportunities such as penny auctions, for example, can only thrive and operate using global internet technologies.

As this project shows, however, it also brings with it real and potential downsides that need addressing. New technologies have the potential to change power relationships – whether person to government, person to business, or person to person – rewriting rules and standards.

In many ways, today's situation online is similar to that of the early years of the industrial age. That too, brought immense benefits to consumers in the form of a much wider variety of increasingly good quality products at comparatively low prices. But it also brought its downsides in the forms of exploitation of the labour force including children, pollution, and sharp practices.

Some of these, such as pollution, were effectively new problems. It took decades for society to understand and begin to address them. Others, such as sharp practice in the market place, were not new but greatly exacerbated by new contexts and situations. For example, it's easy to forget that many of the shopping processes that we take for granted today (labelling of ingredients, weights and measures we can trust, product promises that are true) took decades to create and embed – the result of deliberate, sustained effort in the face of widespread adulteration of products, tampering with weights and measures, misleading and false claims (products that did not do what they claimed on the tin), and so on.

Our review of modern digital detriments illustrates a similarly wide range of issues. Some issues, such as the role and exploitation of personal data in modern commerce, are still new. We are struggling to understand their implications; they involve conflicting interests, values and agendas which can only be resolved by society wide debate. We need effective instigators, leaders and orchestrators of such debate. Others, such as sharp practice in e-commerce, are simply old tricks reinvented for new times, and perhaps magnified by digital technologies. In retrospect, we may look back and see them as temporary 'teething troubles' and excesses. But right now, they still need addressing.

Impact assessment

In trying to assess the scale and impact of each detriment, it became clear very quickly how subjective our assessment of these issues can be. In one way, this is good – debating the issues and how to deal with them is an excellent form of education. However, it also highlights the need for more rigorous analysis: exactly what proportion of the population are affected? Are there some segments more affected than others? Can we develop robust measures for different types of detriment? Can we track and chart their evolution – to see if the threat is growing, diminishing or altering in nature?

We are also acutely aware that detriments in isolation may work differently to detriments in combination. Combining new 'digitally-dependent' lifestyles and new means of access to information, which seem far more robust and honest than they are, with new means of abusing personal data, can create significant opportunities for exploitation. More work needs to be done to see how the detriment 'components' so far identified may come together to create new social and consumer problems.

Mitigating the detriments

Reviewing the detriments in the round, it also becomes clear there is not one, single, way of addressing or mitigating their effects. Some approaches such as better consumer education may work well in some contexts, while others such as regulation will be needed in others. At another level however, we also need to develop a better understanding of how, and when, these different tools can be brought together to best effect. Bodies concerned with consumer protection also need to decide their priorities.

There are five different approaches, mostly needed in some form of combination, for reducing the impact of the detriments.

Consumer education/empowerment.

- Providing effective consumer education, including greater transparency, drawing on the insights of behavioural economics to include the right 'nudges', and the development of 'poka yoke' (mistake proof) consumer processes; and developing new ways for consumers to take collective, cooperative and collaborative action to identify, campaign against, avoid or mitigate certain detriments.

Research and understanding.

- There are a number of areas where experts genuinely differ and where even the experts don't fully understand what is happening or what the implications or possibilities are. In these cases, more research is needed. The anonymisation/pseudonymisation debate is one example.

Creating ‘real’ choice.

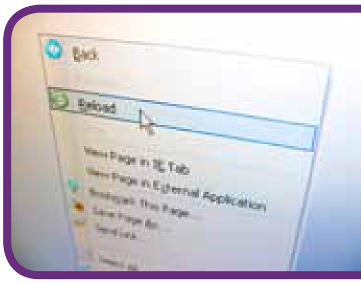
- In many cases, even if consumers are aware of a potential detriment there is little or nothing they can do about it. For example, they might not like what’s said in the privacy policy or terms and conditions, but they have no effective means of negotiating with the organisation concerned. Consumers only have one choice: to take it or leave it. As long as this gap between choice ‘in theory’ and choice ‘in practice’ remains, consumers will continue to suffer the detriment.

Technology.

- There are some areas where technology could be better deployed to protect and advance consumer interests – e.g. in privacy enabling services. In some areas, such as online surveillance, technology fixes are an essential ingredient of the answer, even if they are not the whole answer. This raises questions about incentives for technology developers in this area.

Regulation, including self regulation and industry standards such as kitemarks.

- Some of the issues raised such as ‘no standard price any more’ or the secrecy of Google’s search algorithm are highly complex, involving many different potential consumer benefits and risks. Any regulatory intervention in these complexities could generate multiple unintended consequences. These issues require very careful deliberation, at the highest level, often internationally. An review of the legislative framework needs to be comprehensive including: the revised EU Data Protection legislation; the Human Rights Act; Freedom of Information Act; Computer Misuse Act and others.



Recommendations

An agenda for consumer empowerment

An initial overview of this research reveals a number of central issues and common themes which need to be addressed over the coming years. These issues include:

- Consumers cannot be protected effectively or empowered in the emerging digital environment unless current approaches to agreeing terms and conditions and gaining 'informed consent' are radically overhauled. As long as individuals are deemed to have consented to a policy if they tick a box referring to small print they have not read and cannot change they are effectively disempowered. This issue lies at the heart of online stalking and surveillance which probably would not exist in its current form if it required genuine, prior informed consumer consent. The new EU Data Protection legislation requires a "freely given specific, informed and explicit indication" of the customer's wishes via either "a statement" or a "clear affirmative action". If implemented, it would not only make some current practices illegal, it would also put the data management/sharing process onto a new footing, ensuring 'genuine' informed consent.

- There is an urgent need to reframe and clarify the privacy debate. The word 'privacy' has multiple connotations, all of which tend to be bundled together in a confusing way so that often people end up talking at crossed purposes. Connotations include:
  - civil liberties (resistance to Big Brother states);
  - potential embarrassment from revelations about personal matters;
  - its opposite: a defence of 'openness' (e.g. privacy is only needed for those with something to hide)
  - irritation caused by intrusion (e.g. supposedly 'targeted' marketing messages);
  - arguments about rights (e.g. individuals' right to control how their data is collected and shared); and
  - rights to the economic value of personal data.

Furthermore, much of the debate is conducted on organization-centric assumptions – the focus being on what privacy policies organisations should adopt and pursue. In reality, **privacy is a personal setting**: only individuals know what information they feel happy sharing with who, for what purposes, in what contexts and circumstances. The real detriment today is that individuals have no effective mechanisms by which to express or assert their own personal privacy policies. There are no privacy rights per se, especially not in a sense that is accessible to the general public. As with terms and conditions and 'consent', without such mechanisms, the privacy debate is doomed to go nowhere.

The research has identified some themes which are both deeply disturbing and extremely complex, where there is an urgent need for much more informed debate, for society to make real choices as to where it wants to go, and (perhaps) for regulators to act. These themes include:

The end of price transparency.

- The unbundling of once-coherent products and services into multiple different conditional price points (e.g. air ticket) combined with dynamic pricing means that the notion of 'a price' for something is eroding. With it, so are individuals' benchmarks for assessing comparative value. This is creating a big space for unscrupulous operators to create complexity and confusion with a view to charging consumers more than is needed. It also imposing significant new decision-making and buying costs on consumers, trying to navigate their way through complex choice mazes, and new pricing games (should I buy now, or wait when the price may be lower?).

Ubiquitous face recognition.

- The new reality that an individual may be personally recognized (i.e. a name put to a face) wherever they go, both physically and online, has enormous social implications which are not yet fully understood and have hardly been debated. The potential abuses of face recognition technologies are huge.

The new web monopolies.

- The internet is creating new unaccountable concentrations of power, such as Google and Facebook. The implications of this power are both far reaching and largely uncharted. For example, it's not a big exaggeration to say that the information individuals access on the web is largely determined by Google's search algorithm, the content and workings of which are a closely guarded secret. When Google changes its algorithm, it changes the information the world sees. Is that acceptable? What are the implications of such power? It should also be born in mind that some of the less visible companies may be behind some of the most detrimental activity.

Personalisation.

- 'Personalisation' is transforming the way the web works, including its economics, at breathtaking speed – far faster than consumers or regulators realise. The new personalisation includes behavioural targeting (ad-serving based on tracking an individual's movements and activities across the web), personalised web experiences (page contents tweaked to fit data profiles collected by web owners) and personalised search results – being served results that fit a data profile collected by a search engine rather than some common 'objective' criteria. While the benefits of personalisation have been widely touted, the potential downsides of personalisation in its current form have not: control over consumers' web experience, including the information they are presented with, is effectively being transferred to unaccountable and largely invisible companies (such as BlueKai) driven by the sole purpose of monetisation.

The role and value of this overview

The above list of detriments is a 'starter for ten'. It's purpose is to generate awareness, stimulate debate, and to help create an action agenda – to identify issues that need addressing. It is not meant to be exhaustive. For example, it arguably underplays issues relating to the digital divide and digital exclusion. That reflects the terms of reference of this particular research project. Adding these considerations to the list/map is one of its potential uses. It's real value will be demonstrated over the coming years as the list is revised and extended and as we gain deeper understanding of the issues as they change: it needs to be a 'living document'. We strongly recommend that Consumer Focus uses it as a means of instigating and informing ongoing debate.

Stakeholder engagement

Consumer Focus held a series of roundtable discussions in January and early February 2012 to challenge, augment and prioritise the content of this research report in order to help shape consumer policy priorities. A number of academics and leading thinkers attended, along with analysts from Ctrl-Shift and the policy team from Consumer Focus.

Questions arising

During the sessions a number of questions arose that should be addressed. These are as follows:

- What is the required level of consumer protection concerning downloads of digital content (see 'Regulation behind the times' on page 27)?
- Are technical solutions such as 'interstitial pseudonymisation[1]' understood sufficiently by policy makers?
- Should some of the responsibility for understanding and ameliorating digital detriments be shifted onto consumers? (The premise for this suggestion is the fact that vendors will inevitably continue to gather more data and exploit it to maximum advantage.)
- Is anonymity truly possible anyway?
- What's the liability for vendors that use and trade personal data without consent? Are repercussions changing with the revised Data Protection legislation?
- Are some ways of managing identity online better than others? What does identity mean anyway (is 'proof of claims a more useful concept)? Can, or should, a person have multiple personas or identities?
- Who should carry out due diligence as to whether an organisation's terms and conditions are adequate and provide the correct level of 'informed consent'?
- There is a need for trusted brokers to manage information access and trustworthiness. However, how would these be managed and financed?
- Could online searches be regulated or controlled in any way?
- Does more openness really drive out bad practice?
- Should 'living virtually' really be included in this discussion? Surely this is just a reality of life now?
- How should online market dominance be measured? Should the focus be on specific service areas such as search or provision of cloud computing?
- There is a need to review the regulatory landscape, see how it fits together, reduce fragmentation and ascertain what role it plays in the new global online economy. Current fragmentation means contracts 'rule'. These are 'blunt' instruments possibly depriving consumers of choice. It might be possible from such as review to answer the question: could a single legislative regime be implemented?
- The rise of new bottom up collective consumer power is undeniable. How should this be encouraged and supported?
- What technology is required to enable 'informed consent' to develop and change as a person gets older and their requirements alter?

[1] This may refer to the capability of removing and creating gaps between data fields in order to create pseudoyminity for the data subject.

Actions

- Consumer education regarding the use of cookies is necessary alongside implementation of legislation (the forthcoming Electronic and Communications Directive will be implemented in the UK in May 2012).
- A new code of conduct for comparison sites covering transparency and impartiality is required.
- A review the regulatory framework for mobile payments is necessary.
- Regulation is required that is timely, principle based, technology neutral, and, if possible, flexible to cover evolving requirements.

Appendix

Assessment informing the analysis

Section	Issue	Severity	Scale	Now/ Future	Comment
Privacy	Whose data is it?	2	1	Now	Everyone now leaves a digital trace, irrespective of whether they use the internet
Privacy	Privacy/ new payment systems	3	3	Future	If money or data is stolen it's likely to be a one-off event involving fairly minor amounts of money; does have privacy issues though (geo-location, below), for those people using this technology
Privacy	Privacy/geo-location data	2	3	Now	Loss of privacy, potentially long term, to that group which owns smartphones with geo-location apps, and enables those apps
Privacy	Privacy/face recognition	2	1	Now	Loss of privacy, which potentially affects everyone
Privacy	Whose shopping data is it?	4	2	Now	An irritant which could affect every internet user who shops online
Privacy	Whose media usage data is it?	4	3	Now	Irritating to have your viewing data monitored, only affects those with subscription services
Privacy	Online surveillance and stalking	1	1	Now	Affects almost everybody – not just a nuisance/intrusion, it's also about the financial value that's being skimmed off by the stalking operations
Privacy	Lack of complete awareness	4	4	Now	Full awareness of the extent of data sharing may affect some internet users, some of the time
Privacy	Privacy/smart meters	2	1	Future	Long-term privacy concerns for the entire population
Privacy	Unfair terms of data sharing	2	2	Future	Potential for long-term loss of privacy which affects millions of people who use social networking sites

Section	Issue	Severity	Scale	Now/ Future	Comment
Privacy	Excessive data gathering	2	2	Now	This has long-term privacy issues for all internet users
Digital identity	Identity theft (including spoofing and phishing)	3	3	Now	While *potentially* everybody is affected, and the *potential* negative impacts are great, in reality only a relatively small number of people *are* affected; and there are many easy ways to minimise the risk. Also, most people are aware of the risk – in fact, much of the actual detriment is the hassle you have to go through to avoid ID theft. So the actual detriment is not as big as we are suggesting.
Digital identity	Pretend anonymisation	2	2	Now	Significant long-term impairment and could affect millions
Digital identity	Data loss by individuals	3	3	Now	Losing access to passwords, logins for bank/credit card accounts due to a hard drive failure can lead to one-off impairment, mainly waste of time and hassle, and affects those specific groups who use these services
Digital identity	Data loss by corporations	2	1	Now	Having one's medical/financial or personal data lost, stolen or mislaid by corporations or government has the potential to affect everyone (even those without computers), and could lead to significant long-term impairment
Digital identity	Lack of control using social media sites	2	2	Future	Lack of understanding around how privacy setting work has the potential for loss of privacy, reputation etc, for the millions of people who use these sites

Section	Issue	Severity	Scale	Now/ Future	Comment
Digital identity	Poor control of data histories	2	3	Now	Potential for long-term reputation damage and loss of time in trying to correct it for those individuals who have uploaded embarrassing data in the past
Digital identity	Abuses of online reputation management	2	2	Now	As for digital timelines, but with the potential to affect a larger group of people, for example if reputation is called into question by a third party
Digital identity	Digital gossip	1	4	Now	Although likely to affect only a small number of people the repercussions for the individual have the potential to be severe, with online 'witch hunts' a possible outcome
Digital identity	The need for 'digital wills'	2	2	Future	Not having easy access to an individual's digital estate upon death has the potential to cause significant financial problems for millions of people
Digital identity	Poor online identity management	2	2	Now	The lack of a consistent approach to this has the potential to cause long-term ongoing detriment to millions of people
Digital identity	Credit rating mistakes	3	3	Future	Potential to cause significant one-off problems for a number of individuals
Access and trust	Naïve faith in P2P information	1	3	Future	At its worst, incorrect information could lead to serious health/financial risks for those who act upon incorrect information without obtaining further expert opinion

Section	Issue	Severity	Scale	Now/ Future	Comment
Access and trust	Deliberately misleading online information	2	2	Now	Significant long-term impairment and could affect millions
Access and trust	Abuse of online feedback systems	4	4	Future	Incorrect, uninformed or paid-for feedback can cause a one-off detriment to specific users, say searching a hotel review
Access and trust	Abuse of comparison sites	4	4	Now	Incorrect or manipulated information can cause a one-off detriment to specific uses
Access and trust	Fact or promotion	4	4	Now	The blurring of boundaries between what is fact and what is a paid-for promotion may cause a one-off detriment to a few people occasionally
Access and trust	Online scams	3	3	Now	Internet bait and switch scams lead to one-off financial loss and hassle, and affects a specific group of purchasers
Access and trust	Faux openness	2	1	Now	Assuming that 'everything' is on the internet, or that if it isn't there it's not worth considering, has potential for long-term damage to society, affecting everyone
Access and trust	Deception	3	2	Now	Deliberate deception has potential to cause significant one-off loss, and millions of people are at risk
Access and trust	The gaming of search	2	1	Future	Affects everybody, it actively hinders you finding the information you want – though if you work hard you can overcome it (hence below 50% severity)
Access and trust	Searching vs biasing	2	2	Now	Only ever receiving information which reinforces our beliefs has long-term problems for millions of users

Section	Issue	Severity	Scale	Now/ Future	Comment
Workings of e-commerce	The end of fair prices	2	1	Future	Affects virtually everybody and is a significant impact: making it potentially impossible to get the best or even decent deals.
Workings of e-commerce	The end of price transparency	2	1	Future	Affects virtually everybody and is a significant impact: making it potentially impossible to get the best or even decent deals.
Workings of e-commerce	Pricing pot luck	2	1	Future	Affects virtually everybody and is a significant impact: making it potentially impossible to get the best or even decent deals.
Workings of e-commerce	The death of the high street	2	1	Future	Loss of large numbers of high street shops could affect everyone – poorer choice, and higher prices for those without internet access
Workings of e-commerce	Exclusion	3	4	Future	Only a very small number of people are/will be affected and the nature/type of exclusion we are talking about is also limited
Workings of e-commerce	Poor or non-existent customer service	4	1	Now	As more organisations deal with consumers online more and more of us face the potential of encountering poor customer service
Workings of e-commerce	Always on' temptation	3	4	Future	The ability to shop all the time could lead to one-off financial problems for individuals with poor financial control
Rights and responsibilities	Poor regulation of data sharing	2	1	Future	Misuse of data could lead to long-term privacy issues for everyone, even those who do not use the internet (health, government records)
Rights and responsibilities	Incomprehensible small print	3	3	Future	Possibility of serious one-off detriment to a specific group of users

Section	Issue	Severity	Scale	Now/ Future	Comment
Rights and responsibilities	Liability avoidance	2	1	Future	Having responsibility for mistakes passed back to consumers could lead to serious financial loss, and has the potential to affect everyone
Rights and responsibilities	Evasion of product liability and consumer rights legislation	3	2	Future	Confusion around these issues with new technology has the potential for one-off detriment for millions of people
Rights and responsibilities	Consumer lock-in	4	3	Future	Services that lock people into using them may cause a minor detriment affecting a specific group of users
Rights and responsibilities	Over complex service agreements	4	2	Future	These agreements are confusing and affect potentially millions of people
Rights and responsibilities	Small print contract commitments	4	4	Now	An irritant to the relatively small number of people likely to be affected
Rights and responsibilities	Exploiting social CRM	4	4	Future	A low-level irritant to be asked for help, comments etc when using social media sites
Rights and responsibilities	Exploiting crowdsourcing	4	4	Now	Possibility of helping a commercial organisation to develop a product/service without getting any financial compensation
Living virtually	Compulsive internet use	1	4	Future	Although only small numbers of people are affected the effects on these people are severe, possible fatal in the long term
Living virtually	Overuse of social network sites	2	3	Future	Possible long-term social effects affecting certain types of individuals

Section	Issue	Severity	Scale	Now/ Future	Comment
Living virtually	Deskilling	2	2	Future	As more and more work and communication goes online there are long-term social effects around language, communication and social skills
Living virtually	Weakening of society's rules	2	1	Future	Long-term changes in what is deemed socially acceptable affect everyone
Exercise of power	The new web monopolies	2	1	Future	The potential for abuse by the likes of Google and Facebook (e.g. hidden tweaks to the search algorithm affecting what billions of people see when they make searches) is potentially far greater than the media barons of the past. However, at the moment it's not clear that these abuses have actually happened
Exercise of power	Market dominance	2	1	Future	Having large organisations hold a monopoly on information can damage society in the long term
Exercise of power	Threats to internet neutrality	2	1	Future	Whoever controls the medium controls the message
Changing technologies	Artificially created needs	3	4	Future	Some individuals will always feel the need to own 'the next best thing', needlessly upgrading their phones, tablets etc, occasionally leading to financial problems
Changing technologies	Excess obsolescence	4	2	Future	Advances in technology means that perfectly functional equipment soon becomes obsolete, requiring consumers to buy the next version of a product

Section	Issue	Severity	Scale	Now/ Future	Comment
Changing technologies	Inadequate regulation	2	1	Future	The ever-onward march of technology is changing society, and affects everyone
Changing technologies	Digital divide	2	1	Now	This could lead to serious long-term problems for society, with it divided into the 'haves' and 'have-nots', potentially affecting everyone
Changing technologies	The dark web	1	2	Now	Use by criminals of the dark web could have severe consequences potentially affecting millions of people

Ctrl-Shift

info@ctrl-shift.co.uk
020 7000 1907
www.ctrl-shift.co.uk

Consumer Focus

contact@consumerfocus.org.uk
020 7799 7900
www.consumerfocus.org.uk

Published May 2012

Consumer Focus is not responsible for the content of external websites and resources cited in this report.