



**INFORMATION  
TECHNOLOGY  
FACULTY**

# **BUILDING TRUST IN THE DIGITAL AGE: RETHINKING PRIVACY, PROPERTY AND SECURITY**

**MAKING INFORMATION SYSTEMS WORK INITIATIVE**



*Building Trust in the Digital Age: Rethinking Privacy, Property and Security* forms part of the *Making Information Systems Work* thought leadership programme of the ICAEW IT Faculty.

New technology has transformed the way we interact and do business. However, as the number of technology opportunities grows, so too do the challenges of successful implementation. The *Making Information Systems Work* programme considers these opportunities and challenges, engaging all sectors of the economy in the debate.

This initiative is not just about making technology work. It is about making technology work with the wider systems around us. In order to do this, information systems need to be based on:

- value: the economic case for IT investment;
- trust: a secure environment to transfer information; and
- standards: a sound technical basis for the exchange of information between parties.

*Building Trust in the Digital Age: Rethinking Privacy, Property and Security* considers the actions that individual businesses can take to address concerns about the security and use of digital information, as well as the wider social and legal implications of digital technology. This builds on the first report in the programme, *Measuring IT Returns*, which considers the opportunities to create value through IT and the challenges faced by many businesses in applying financial analysis to these opportunities.

ICAEW operates under a Royal Charter, working in the public interest. As a world-leading professional accountancy body, ICAEW provides leadership and practical support to over 136,000 members in more than 160 countries, working with governments, regulators and industry to ensure the highest standards are maintained.

The ICAEW IT Faculty is a network of chartered accountants and other professionals who have an active interest in IT. The faculty provides help and support to its 3,000 members regarding best use of IT. It also has a wide-ranging public interest role and a thought leadership programme which promotes debate and research.

We welcome views and comments on this work and the other themes of the *Making Information Systems Work* programme. To contact us, please email [informationssystem@icaew.com](mailto:informationssystem@icaew.com) or telephone Kirstin Gillon on +44 (0)20 7920 8538.

**For more information on *Making Information Systems Work* and to download reports, visit [icaew.com/informationssystem](http://icaew.com/informationssystem). Alternatively, visit our community site [IT Counts at ion.icaew.com/itcounts](http://ion.icaew.com/itcounts), follow us on Twitter [@ICAEW\\_ITFaculty](https://twitter.com/ICAEW_ITFaculty) or join our LinkedIn group [ICAEW IT Faculty](#).**

# **BUILDING TRUST IN THE DIGITAL AGE: RETHINKING PRIVACY, PROPERTY AND SECURITY**

**MAKING INFORMATION SYSTEMS WORK INITIATIVE**



# CONTENTS

<b>TABLE OF FIGURES AND PANELS</b>	<b>iii</b>
<b>EXECUTIVE SUMMARY</b>	<b>v</b>
<b>1. ADDRESSING CONCERNS ABOUT IT</b>	<b>1</b>
1.1 Aims of the report	2
1.2 Generating value through IT	2
1.3 Risks surrounding information security	3
1.4 Risks surrounding information use	6
1.5 Information security, privacy and intellectual property	6
1.6 Our approach to building trust	7
1.7 Summary	9
<b>2. RIGHTS OVER PERSONAL INFORMATION</b>	<b>11</b>
2.1 The business value of personal information	12
2.2 Legal considerations	13
2.3 Market considerations	17
2.4 Underlying questions about privacy	19
2.5 Collecting and retaining personal information	26
2.6 Using personal information in the private sector	28
2.7 Sharing personal information across the public sector	30
2.8 Summary	32
<b>3. RIGHTS OVER INTELLECTUAL PROPERTY</b>	<b>33</b>
3.1 The business value of intellectual property	34
3.2 Legal considerations	35
3.3 Market considerations	36
3.4 Underlying questions about intellectual property	37
3.5 Strengthening intellectual property rights	41
3.6 Encouraging open approaches	42
3.7 The push for transparency	45
3.8 Co-creation of intellectual property	47
3.9 Summary	48
<b>4. INFORMATION SECURITY PRACTICES</b>	<b>51</b>
4.1 Principles of information security	52
4.2 Established information security practices	53
4.3 Making decisions about security measures	57
4.4 Building skills and organisational structures for security	58

4.5	Embedding good practices throughout the business	59
4.6	Securing information beyond business boundaries	60
4.7	Personal information practices	62
4.8	Intellectual property practices	67
4.9	The growing regulatory agenda	68
4.10	Summary	69
<b>5.</b>	<b>BUILDING TRUST</b>	<b>71</b>
5.1	Impact of new technology	72
5.2	Trust in business	74
5.3	Recognise and debate issues	75
5.4	Develop new theoretical thinking	76
5.5	Balance control and use of information	79
5.6	Create supportive institutions	82
5.7	Summary	85
	<b>APPENDIX – AREAS FOR RESEARCH</b>	<b>87</b>
A.1	The role of academic research	87
A.2	Sharing business experience and knowledge	87
A.3	Supporting collective actions	89
A.4	Research challenges	90
	<b>ACKNOWLEDGEMENTS</b>	<b>92</b>
	<b>BIBLIOGRAPHY</b>	<b>93</b>

# TABLE OF FIGURES AND PANELS

## FIGURES

Figure 1.1: ICAEW approach to building trust in the digital age	7
Figure 5.1: Information supply and demand curves	73
Figure 5.2: Impact of IT on information quantity	73

## PANELS

Panel 1.1: Hacking a security business	4
Panel 1.2: Attack on Estonia's infrastructure	5
Panel 1.3: Hacking and blagging	5
Panel 2.1: OECD Fair Information Principles	13
Panel 2.2: The EU regime of data protection	14
Panel 2.3: US privacy laws	14
Panel 2.4: Privacy as a human right	15
Panel 2.5: English super injunctions and the internet	15
Panel 2.6: US Federal Trade Commission approach	16
Panel 2.7: Information accountability and the Fair Credit Reporting Act	17
Panel 2.8: Losing investor confidence: the case of Phorm	18
Panel 2.9: HP's position on privacy	18
Panel 2.10: Approaches to privacy	20
Panel 2.11: Genocide in Rwanda and identity cards	22
Panel 2.12: Balancing privacy and security	23
Panel 2.13: US and European attitudes to privacy	23
Panel 2.14: The varied reaction to Google's Street View	24
Panel 2.15: 'The internet of things' and privacy	26
Panel 2.16: Losing the power to forget	27
Panel 2.17: Behavioural advertising	29
Panel 3.1: UK intellectual property law	35
Panel 3.2: Alternative business models: Spotify	37
Panel 3.3: Welfare economics of intellectual property rights	38
Panel 3.4: The newspaper industry and the internet	39
Panel 3.5: The role of the Internet Service Provider	41
Panel 3.6: The Creative Commons	42
Panel 3.7: The Open Data movement	45
Panel 3.8: YouTube copyright requirements	47
Panel 3.9: Crushpad business model	48
Panel 4.1: Types of authentication	52
Panel 4.2: Security standards: ISO 27001/2 key provisions	53
Panel 4.3: Breach notification laws	55

Panel 4.4: Payment Card Industry Data Security Standard (PCI DSS)	56
Panel 4.5: Information security governance	58
Panel 4.6: The consumerisation of IT	59
Panel 4.7: HMRC data loss	60
Panel 4.8: Cloud computing	61
Panel 4.9: Gaining comfort over service providers	61
Panel 4.10: Privacy impact assessments	63
Panel 4.11: Facebook's privacy settings and controls	64
Panel 4.12: The controversial launch of Google Buzz	65
Panel 4.13: Privacy audits	65
Panel 4.14: The problems of anonymity: the Netflix data prize	66
Panel 4.15: Information security regulation and the House of Lords report	68
Panel 5.1: Building business trust	74
Panel 5.2: Contentious questions	76
Panel 5.3: Information ethics	77
Panel 5.4: The cases of TJX and ChoicePoint	77
Panel 5.5: Differences between tangible and intangible property	78
Panel 5.6: Encouraging innovation with IT	80
Panel 5.7: Private property rights	80
Panel 5.8: The tragedy of the commons	81
Panel 5.9: The tragedy of the anti-commons	81
Panel 5.10: The Internet Governance Forum	82
Panel 5.11: Requirements for good regulation	83
Panel 5.12: Standards and informal regulation in the technology industry	84
Panel 5.13: Building effective market pressures	84
Panel A.1: Suggested research topics on information practices	88

# EXECUTIVE SUMMARY

## Addressing concerns about IT

Information technology (IT) transforms the way that many businesses operate and presents tremendous opportunities to increase revenues, cut costs and create new customer value. However, alongside these opportunities, there are growing concerns about the control and security of digital information which a business needs to manage in order to capture and retain value from IT. These concerns are fuelled by:

- high-profile data breaches and the growth of cyber attacks;
- individual experience of identity theft, phishing emails, spam and computer viruses;
- controversial use of personal information by governments and businesses; and
- repeated failures to secure intellectual property and prevent others from exploiting it.

These incidents can result in substantial financial losses for businesses, governments and individuals, damaged reputations and reduced confidence in IT systems more broadly. Therefore, this is an area of growing importance for business and economic success. Furthermore, these issues affect all of us as individual consumers or citizens.

Trust is an important feature of any economy and society. It enables businesses and individuals to carry out economic transactions and social interactions in the belief that other parties will behave in a non-harmful way. Building trust that other parties will secure and use digital information in acceptable ways is therefore an important element of addressing concerns about, and building confidence in, a digitally-based economy.

Our approach to addressing concerns is based on the belief that businesses cannot build trust in isolation. While they are necessary, today's good practices are not enough. Businesses operate within a network of formal and informal norms which influence and limit their actions. As a result, good information practices are ultimately grounded in clear rights and duties over information and need to be built on an accepted framework of social expectations and laws.

Digital technology is disrupting and challenging many aspects of the existing social and legal environment. Consequently, it is not enough for businesses to implement today's good practices in isolation. We also need to encourage widespread engagement, understanding and debate of the issues presented by digital information to build a social and legal framework which is broadly accepted and can underpin individual business actions

By summarising a wide range of business practice, underlying theory and new areas of debate, this report aims to achieve two principal benefits:

- to help management make better decisions about digital information and improve business performance in relation to information risks; and
- to inform widespread public debate about digital information and thereby support the development of a variety of regulatory, industry and social solutions.

In the process, it brings together three areas of thinking that are often looked at separately: privacy, intellectual property rights and information security. While these continue to be distinct fields, the digital environment brings them closer. As a result, this report takes a first step in bringing together key elements of a disparate and complex literature to support more integrated business practices and policy-making.

## Rights over personal information

Personal information is information that is associated with an identifiable individual. Most businesses hold personal information about employees and customers as part of their day-to-day operations.

Personal information can also be used to generate revenue. As a result, personal information can be important intellectual property, especially for consumer or advertising-based businesses.

While many businesses may want to make extensive use of personal information, individuals retain rights over information about themselves and businesses have a range of duties regarding their use and treatment of personal information. In Europe in particular, personal information is subject to substantial regulation. Personal information can also be protected through laws targeted on sensitive pieces of personal information or based on the human rights framework, including the right of privacy. It can also be protected through commercial pressures.

The notion of a private space has been established since Aristotle's *Politics*. However, it remains a nebulous idea which is subject to diverse views on its scope and importance. We summarise some of the key theoretical ideas about privacy around the following questions:

- What is the scope of privacy?
- What is the role of consent?
- What are the benefits of privacy?
- What harm is caused by breaches of privacy?
- How should privacy be balanced with other interests?
- How can different cultural views be reconciled?
- How can we understand fragmented and inconsistent behaviour?

IT increases the value of personal information, leading to greater business use and commercial exploitation of it. This is also leading to growing contention about the limits of business use of personal information and the ways in which individuals can retain control over it.

**More is known and remembered.** While data protection principles limit the personal information that can be collected and retained, emerging practices and technologies enable businesses to gather increasing amounts of user and location data. Regardless of its ultimate use, the extensive collection and retention of information in itself may cause individuals concern and discomfort. Furthermore, the inability to 'forget' personal information may have long-term effects on society as individuals become more conscious of their actions and inhibit their behaviour accordingly or suffer disproportionate consequences.

**Businesses are extensively profiling individuals.** While profiling has been a business practice for many years, the sophistication of analytical systems, combined with the vast digital footprint created by most people, is making profiling much more powerful. This can provide benefits by targeting products and services to specific individuals. However, profiling can result in unequal treatment and can offend deeply-held perceptions of fairness. There is often a lack of due process and accountability about decisions. There are also concerns about the long-term impact of filtering information or services to narrow audiences based on this segmentation.

**Governments are connecting information about citizens.** The opportunity to share information more effectively across governments is often essential to increasing the efficiency and quality of public services. However, it raises practical concerns about the quality of information and how it is managed. It also leads to many questions about the degree of governmental power and control gained through centralising personal information.

## Rights over intellectual property

To generate revenue, businesses rely on intellectual property and confidential information which can include inventions, formulae, novel processes, creative content, brand names, designs and customer lists.

Intellectual property rights aim to secure the cash flow benefits from the exploitation of information resources for the rights-holder. Business will sometimes use intellectual property rights to keep information secret. However, in many cases, intellectual property rights enable a business to sell access to information products and services and keep the related revenue stream.

In many cases, intellectual property rights are clear and the related business challenges are largely practical in nature. However, this clarity can mask deep differences of opinion about the benefits of strong intellectual property rights compared to the benefits that can be obtained from the free flow of information.

As the opportunities to share information for a wide range of social and economic benefits grow, debates touch on complex underlying questions, including:

- What are the net economic benefits of intellectual property rights?
- What is the moral basis of intellectual property rights?
- What is the impact of changing consumer attitudes to paying for content?
- Are breaches of intellectual property rights morally wrong?

We consider three areas of particular debate which stem from the changes brought by digital technology.

**There are alternatives to strong rights.** Intellectual property rights have been substantially strengthened in recent years to enable businesses to generate more revenue from their information content or inventions. However, there are alternative approaches which put a greater emphasis on information sharing. Supporters of these approaches argue that businesses should develop business models which embrace the new technological opportunities and the openness that these enable, rather than retain models which are no longer effective in the digital environment.

**There is greater openness in the public and private sectors.** The push for transparency is seen most prominently in the public sector, where the Open Data movement is pushing for the widespread release of government data to drive a variety of economic and social benefits. As technology has improved, pressures have also grown in corporate reporting for more comparable and timely data from businesses. However, while there are great benefits to transparency, it also potentially creates new risks, especially when changes in incentives change the behaviour of individuals.

**Businesses are interacting more with each other and their customers.** This is resulting in co-creation of intellectual property across supply chains and with customers. While businesses may want to maximise their rights over intellectual property, there also may be new questions about how the benefits of this collaboration are shared and growing perceptions of unfairness where businesses exploit the creativity of others.

## Information security practices

In many cases, information rights are well established and clear. Therefore, the business imperative is to secure those rights effectively. The field of information security deals with the protection of valuable and/or sensitive information and is built around three key principles, namely confidentiality, integrity and availability.

The principles of information security are reflected in a wide range of established information security practices. Business processes and management techniques are a central part of any information security strategy. Given the dominance of IT, technical computer security is also a very important component of information security.

Despite the existence of a wide range of good practices, many businesses struggle to implement effective information security. One reason for continuing security failures is that it is often difficult to connect security measures to business priorities and thereby gain sufficient management and employee attention.

It can be difficult to make good decisions about information security investments. Good practice suggests that management should assess the risks surrounding information and balance the costs of security measures against the possible impact of security failures. However, the difficulty of quantifying these matters limits the effectiveness of structured decision-making processes in practice.

While many information security measures are technical, a business is also likely to benefit from techniques which integrate security skills and knowledge across technical and business functions. Information governance is a set of management practices which aims to protect the quality and control of information throughout the organisation and integrate accountability accordingly

IT has enabled information to be more dispersed, putting greater emphasis on individual behaviour and making it more important to embed good security practices. As employees increasingly use consumer devices, and frequently their own personal devices, to store or access corporate data, embedding good behaviour will become ever more important. Training can help raise employee awareness of security policies and processes. Culture and senior-level commitment are also important factors and, where security can be aligned with the objectives and brand of the business, it is more likely to become central to business activities.

A growing security challenge concerns the explosion in outsourcing and collaboration across supply chains. As a result, information rarely sits in one organisation as a static resource but instead is the subject of continual flows between different parties. This may lead to a shift in security thinking, away from establishing a secure perimeter around the organisation to a more dynamic model which emphasises security across a supply chain.

Finally, as security failures increasingly impact on individual consumers and citizens, there is a developing regulatory agenda, particularly around the security of personal information. As a result, a business may need to shift its thinking from internal risk management to meeting external demands.

## Building trust

New technology is a central part of economic development. However, transformation in economic possibilities through new technology often creates social tensions and new questions in parallel. Unless we recognise and address the social challenges related to digital information, there is a risk that opportunities to use it are missed.

Trust is an important feature which underpins the use and value of new technologies and therefore can support the development of a digital economy. Businesses can build trust at an individual level by implementing good practices. However, good practices need to be underpinned by clear social expectations and legal obligations. We identify four essential elements to building broader trust around digital information.

**Recognise and debate issues.** Regulators, law makers and the technology industry have a major role to play. However, all businesses are affected by some of the issues raised in this report, as are all individual consumers and citizens. Therefore, debates need to engage broadly across all sections of society in order to take account of different interests and perspectives.

**Develop new theoretical thinking.** While technology is the direct cause of the difficulties outlined in the report, it is radical changes to the economics of information which are at the heart of the social tensions. Therefore, we need to encourage a variety of new thinking which is rooted in the economics of digital information.

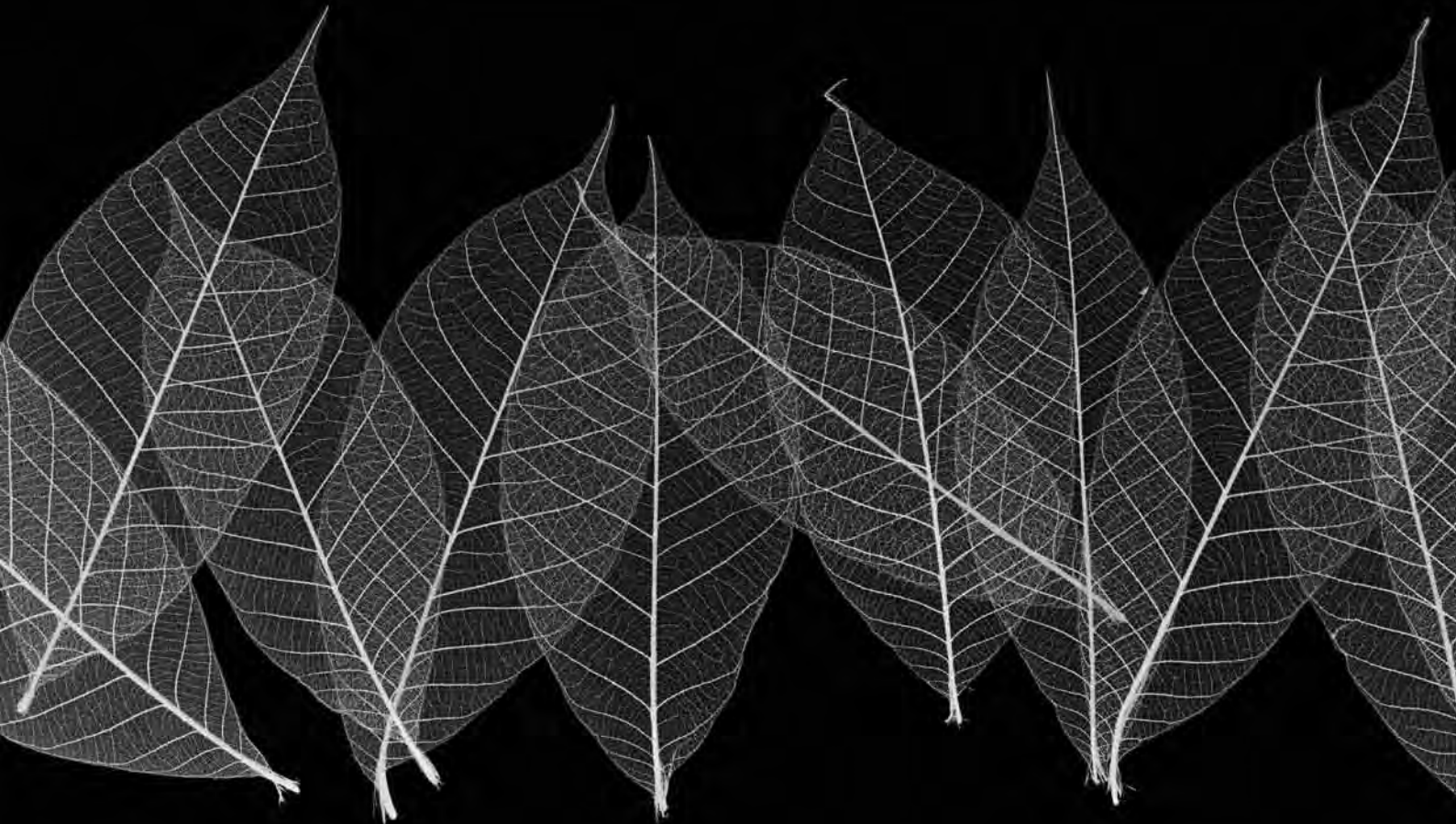
**Balance control and use of information.** There needs to be clear rights over information to enable parties to form expectations about its use and protection. However, this control needs to be balanced with the ability of different parties to use and share information for a wide range of benefits.

**Create supportive institutions.** A variety of institutions are needed which can address this broad range of issues and develop robust and flexible solutions. Institutions need to include many participants, including regulators, businesses, individual consumers and the technology industry and promote common approaches, as far as is possible.

Although each of these elements is essential, they are also fraught with difficulty which may limit realistic progress. Academic research can play an important role in developing deeper understanding of the challenges of the digital environment and supporting each of these elements.

# 1. ADDRESSING CONCERNS ABOUT IT

There are growing concerns about the control and security of digital information, fuelled by high-profile security breaches and controversial uses of personal information. But how much do these concerns matter? And what can individual businesses do about them?



# 1. ADDRESSING CONCERNS ABOUT IT

## 1.1 Aims of the report

Information technology (IT) transforms the way that many businesses operate and presents tremendous opportunities to increase revenues, cut costs and create new customer value. However, alongside these opportunities, there are growing concerns about the control and security of digital information which a business needs to manage in order to capture and retain value from IT. These concerns are fuelled by:

- high-profile data breaches and the growth of cyber attacks;
- individual experience of identity theft, phishing emails, spam and computer viruses;
- controversial use of personal information by governments and businesses; and
- repeated failures to secure intellectual property and prevent others from exploiting it.

These incidents can result in substantial financial losses for businesses, governments and individuals, damaged reputations and reduced confidence in IT systems more broadly. Therefore, this is an area of growing importance for business and economic success. Furthermore, these issues affect all of us as individual consumers or citizens.

By summarising a wide range of business practice, underlying theory and new areas of debate, this report aims to achieve two principal benefits:

- to help management make better decisions about digital information and improve business performance in relation to information risks; and
- to inform public debate about digital information and thereby encourage the development of a variety of regulatory, industry and social solutions.

In the process, it brings together three areas of thinking that are often looked at separately – privacy, intellectual property rights and information security. While these continue to be distinct fields, the digital environment brings them closer. As a result, this report takes a first step in bringing together key elements of a disparate and complex literature to support more integrated business practices and policy-making.

## 1.2 Generating value through IT

IT systems and the internet have become a major source of economic and social value across the world. ICAEW's 2008 report *Measuring IT Returns* highlights a wide range of evidence as to the financial and social impact of IT, including:

- growing world-wide expenditure on IT, with sales on IT and telecoms expected to top \$3.6 trillion in 2011;<sup>1</sup>
- widespread academic research attributing substantial economic growth in the 1990s to IT investments;<sup>2</sup>
- continuing investments in IT by business and government, as well as growing consumer markets, leading to a pervasive influence of IT on all our activities and interactions; and
- the emergence of major new businesses based on the internet, such as Google.

IT transforms the economics of information by reducing its costs massively while also increasing the benefits that can be obtained through its use. As a result, it becomes economically viable or beneficial to collect, store, use and share vast amounts of information.

<sup>1</sup> Amanda Andrew, 'iPad to boost 2011 IT spend to \$3.6 trillion'.

<sup>2</sup> See, for example, Erik Brynjolfsson and Loren Hitt, 'Computing productivity: firm level evidence' and Dale Jorgenson and Khuong Vu, 'Information technology and the world economy'.

This shift is particularly important because information is an enormously powerful resource. It underpins all our activities and interactions, making the impact of IT profound.

By using IT systems effectively, businesses have seen many opportunities to generate greater value through:

- improved efficiency of operations;
- new and enhanced products and services;
- different ways of working, such as outsourcing and globalisation; and
- the ability to reach and service new markets.

While potentially creating value for shareholders, these changes have also resulted in substantial customer benefits, with lower costs, improved services and greater choice in many industries.

These trends will continue in future. Computing power keeps growing, enabling businesses to collect and store more and more information, as well as undertake more sophisticated analysis. Mobile and other technologies such as RFID will provide further opportunities for data capture, leading to new products and services and transforming the way we do things. As more and more people become connected, the benefits of the internet will further increase, reflecting the economic phenomenon of network effects.

### 1.3 Risks surrounding information security

However, these benefits are not without risks to businesses and individuals. As the use of IT and the internet has grown, so too have concerns about the security of information, fuelled by regular incidents of security failures.

These incidents have a significant cost to businesses, such as:

- costs related to investigating and fixing problems;
- lost revenue or productivity from system downtime;
- lost revenue from the theft of intellectual property; and
- fines from regulatory failures.

The 2010 survey on information security breaches by InfoSecurity Europe and PwC reported that the average cost of the worst information security incidents in large businesses was £280,000-£690,000. For small businesses, the average cost of the worst security incidents was reported to be £27,500-£55,000.

Failures can cause significant reputational damage to a business and a catastrophic security failure could even threaten the survival of a business which relies heavily on confidence in its security practices. Academic research suggests that there is a direct impact on market value from such reputational damage. For example, in a study from 2004, 'The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers', Huseyin Cavusoglu et al showed that the announcement of internet security breaches had an immediate negative effect on market valuation of approximately 2%. Another survey by Paul Bolster et al, 'Security breaches and firm value' (2010), found significant and negative effects on market value when a security breach is reported by major news outlets. When reported elsewhere, though, the impact is minimal.

While many security failures stem from human error or carelessness, the growth of cybercrime is causing significant concern, as cybercrime has become a major and, in some cases, highly organised, criminal industry. An estimate by security firm Detica, in conjunction with the UK government's Cabinet Office in 2011, put the total annual loss in the UK due to cybercrime at just over £26bn.<sup>3</sup> This broke down into:

- £21bn loss for business;
- £3.1bn loss for citizens; and
- £2.2bn loss for government.

Hackers may be driven by non-financial motives. They may want to claim credit for high-profile attacks and demonstrate their technical prowess to other hackers or the world more broadly.

<sup>3</sup> Detica, *The Cost of Cyber Crime: a Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*.

They may also have political reasons for attacking particular targets, a growing phenomenon known as 'hacktivism'.

It is notoriously difficult to gain accurate statistics around this kind of criminal activity. There are few formal reporting requirements on businesses and they are likely to minimise their reporting of incidents to avoid bad publicity. In practice, many statistics are based on surveys which draw on small samples of security specialists.

Regardless of the exact figures, though, there is little doubt that the impact of security failures today is potentially severe given our reliance on IT systems throughout the economy and government.

## Theft of intellectual property and industrial espionage

The theft of intellectual property and other industrial secrets is a major concern of many businesses. The Detica/Cabinet Office report estimated the annual value of such theft at £16.8bn, making it the biggest component of the £20bn business losses.

Anecdotal evidence suggests that attacks on businesses are becoming increasingly prevalent and sophisticated. While the threat from insiders selling business secrets remains significant, many businesses are also facing highly targeted attacks on their intellectual property from organised cyber criminals. Attacks may be carried out to order. In some cases, there are suspicions of state sponsorship. Frequently, attacks are so covert that businesses only become aware of the theft at a much later date, when they discover copies of their technology in the marketplace. For example, senior employees may be sent highly personalised emails which appear to be from a colleague or other close contact. These emails encourage them to follow links which infect their computer with various types of malware, thereby giving criminals access to internal systems. Known as 'spear-phishing', attacks like these often draw on information posted on social websites to convince the victim that the email is authentic.

Even information security businesses can be the victims of attacks, as shown by the experience of RSA.

### Panel 1.1: Hacking a security business

Information security firm RSA sells tokens which customers use to authenticate, or validate, their identity when logging onto a system. Each token is associated with a specific individual and provides a unique passcode which needs to be used, along with a system password, when users log on. This strengthens the security around systems as the passcode is based on an advanced cryptography process.

In March 2011, RSA suffered a highly sophisticated hacking attack in which criminals stole information which pertained to the token system and weakened the protection which the tokens provided.<sup>4</sup> The company subsequently admitted that information stolen in this attack had been used to attack one of its customers, defence company Lockheed Martin.

As a result of the breach, RSA offered to replace all tokens in circulation, which totalled up to 40 million. It also suffered reputational damage and the long-term impact of the breach remains to be seen.

## Availability and integrity of services

Another area of business risk concerns the availability and integrity of services.

Denial of service attacks have become an established tool of extortion against businesses. In these attacks, criminals send a huge volume of traffic to a website in order to overwhelm it and ultimately take it offline. This can cause reputational damage to a business, as well as financial losses. Therefore, criminals may aim to get payment from the business in order to cease the attack. They may also get large amounts of publicity in the process.

Furthermore, there are major concerns about attacks on utilities or critical pieces of national infrastructure which would disrupt essential economic or social services. Utilities such as water or banking systems, for example, could be targeted by terrorists. Attacks on a country's internet infrastructure could also have a potentially devastating impact on all services based around the internet, as experienced by Estonia.

<sup>4</sup> Robert McMillan, 'Is it time for RSA to open up about Securid hack?'

## Panel 1.2: Attack on Estonia's infrastructure

In April 2007, Estonia suffered a concerted attack on its internet infrastructure.<sup>5</sup> The websites of the Estonian Parliament, banks, newspapers and broadcasters were all targeted. This was largely through denial of service attacks, although some defacement of websites was also seen. Estonia was particularly vulnerable to such attacks as it had made extensive use of the internet for government and banking services.

Estonia claimed that the attacks had the state backing of Russia, due to their scale and sophistication. However, Russia denied responsibility and it has proved difficult to identify where the attacks originated from.

## Identity theft and cybercrime against individuals

There have been many high-profile information security breaches which have exposed the personal details of citizens and consumers, from the UK government's loss of data concerning 25 million child benefit recipients to TJX's exposure of 45 million customers' credit card details.<sup>6</sup>

Where personal information is appropriated by criminals, it can be used for financial gain in identity theft cases or credit card frauds. Individuals may be sent emails which contain viruses or lead them to fake sites which aim to extract further personal information from them. Criminals may send emails which aim to deceive individuals into giving money to them directly. The Detica/Cabinet Office survey estimated individual losses from identity theft at £1.7bn per annum, with losses of £1.4bn from other online scams.

Criminals may also target individuals to gain access to personal computers for use in other attacks. A botnet, for example, is a large network of computers which criminals control. This type of network is used for activities such as denial of service attacks or sending out spam emails. In many cases, the individual will be unaware that their computer is part of a botnet.

The range of methods used to access personal information illegally was extensively highlighted in 2011 through the News of the World phone hacking scandal.

## Panel 1.3: Hacking and blagging

There are a number of techniques which can be used to access personal information illegally.

Hacking phone messages, for example, has been the subject of substantial controversy in the UK. Blagging, where individuals pretend to be someone else in order to gain confidential and sensitive information, is also a well-known illegal practice. These activities are typically undertaken by private investigators, who then sell the information to a variety of interested parties.

The UK Information Commissioner undertook a study in 2006 which considered these illegal practices, entitled *What Price Privacy Now?* It documented what it termed 'an unlawful trade in confidential personal information', based on information held both by public bodies, including the National Health Service, the tax authorities and the police, and private businesses, such as banks and telephone companies.

The report cited five main clients for this kind of information:

- the media;
- insurance companies;
- lenders and creditors;
- those involved in matrimonial disputes; and
- criminals.

Anecdotal evidence suggests that the media use of such techniques has diminished since the jailing of a journalist and private investigator for phone hacking in 2007. However, it appears that the trade continues in earnest in other areas. Following the revelations about phone hacking at the News of the World in 2011, Christopher Graham, the UK Information Commissioner, called for prison sentences for such offences, a recommendation from the 2006 report which was not fully implemented at the time.<sup>7</sup>

<sup>5</sup> BBC News, 'The cyber raiders hitting Estonia'.

<sup>6</sup> BBC News, 'UK's families put on fraud alert'; Jaikumar Vijayan, 'TJX data breach: at 45.6M card numbers, it's the biggest ever'.

<sup>7</sup> Erik Larson, 'Phone-hacking shows jail needed for data theft, U.K. Privacy Chief says'.

## 1.4 Risks surrounding information use

In addition to risks around information security, there are also growing concerns about how information is used and shared by different parties.

Internet-based businesses are in the vanguard of pushing the commercial exploitation of personal information, regularly courting controversy in the process. Governments have also been high-profile users of personal information, sharing it widely across departments and making use of it on broad public interest grounds, such as safety and security. This has resulted in many projects with high-profile opposition, including national identity cards and centralised medical records in the UK.

Many businesses are concerned about the extent to which they can successfully exploit their own valuable information. As the online piracy of copyright-protected content has exploded, the creative industries have been pushing for stronger legislation in the enforcement of their legal rights. Pressures for openness and transparency may also affect the ability of businesses and governments to keep sensitive information confidential.

These concerns are reflected in significant disorientation about digital information. While there are many new opportunities to share information and enjoy valuable and innovative services, many businesses and individuals also feel uncomfortable as they sense a loss of control over pieces of information that they have traditionally controlled.

As a result, we see growing pressure for new laws and regulations to strengthen rights over information. We also see inconsistent attitudes and behaviour as people grapple with the new opportunities from digital information, for example:

- extensive sharing of personal information on the internet, alongside growing concerns about privacy;
- widespread breaching of copyright protections by generally law-abiding citizens; and
- deeply divergent attitudes on the provision of new internet-based services.

These concerns and uncertainties create significant risks for businesses trying to innovate with IT and digital technologies. They also make it harder to build trust in business behaviour regarding digital information. As a result, it is vital that these concerns are addressed.

## 1.5 Information security, privacy and intellectual property

In order to capture a broad range of concerns about IT and digital information, this report brings together three areas of thinking that are often looked at separately.

- Information security focuses on the protection of valuable or sensitive information of any kind, based around the principles of confidentiality, integrity and availability.
- Privacy asserts the rights of individuals over information about them.
- Intellectual property is concerned with rights over information which a business or individual has created.

Each of these areas is well established and benefits from high degrees of professional expertise as well as respected academic research. They all link to the notion of confidentiality, which is central to the accounting and many other professions. However, each area is served by a variety of different specialists who may approach the risks from diverse perspectives, including:

- technologists;
- lawyers;
- business managers;
- marketing specialists; and
- consumer or civic groups.

While all of these perspectives are important, this diversity of expertise presents a real challenge for businesses which need to develop a coherent understanding of their different information risks. This difficulty is compounded by the fact that some of these disciplines maintain a sharp distinction between personal information and intellectual property issues.

However, while these continue to be separate fields, the digital environment brings them closer together. As a result, we see growing conflicts or overlaps between policy solutions in these three areas.

- Options to improve information security around identity may require the central collection of sensitive personal information, potentially undermining privacy rights.
- Conversely, the desire of privacy advocates to maintain high levels of anonymity in transactions may cause discomfort to security specialists.
- The owners of intellectual property rights increasingly want to monitor the activities of consumers in order to enforce their rights, a move which is strongly opposed by privacy advocates.
- Some technical solutions for personal information problems build on solutions already in place for intellectual property, such as digital rights management systems.

The relationship between privacy and information security exhibits particular tensions. They both rely on the notion of confidentiality and, without effective information security, privacy is severely undermined. However, while a system may be highly secure, it can still fail to respect privacy rights by retaining personal information, using it in inappropriate ways or collecting personal information that is not required.

It is also becoming increasingly difficult to draw clear distinctions between intellectual property and personal information. Historically, pieces of intellectual property, such as a pharmaceutical formula, a piece of music or a book, were clearly different to pieces of personal information such as a name, address or date of birth. However, as information has become increasingly digitized, it has become harder to maintain an unequivocal boundary between different types of information. For example, online blogs or profiles typically mix personal information and intellectual property, with photos and creative writing sitting alongside profile and location information.

Furthermore, personal information is becoming an increasingly important asset of many businesses. Indeed, it may represent a significant part of a business’s intellectual property, especially in consumer or advertising-based businesses. Consequently, there are sharply different interests which need to be considered, as individuals look to assert control over their personal information and businesses look to exploit it as their intellectual property.

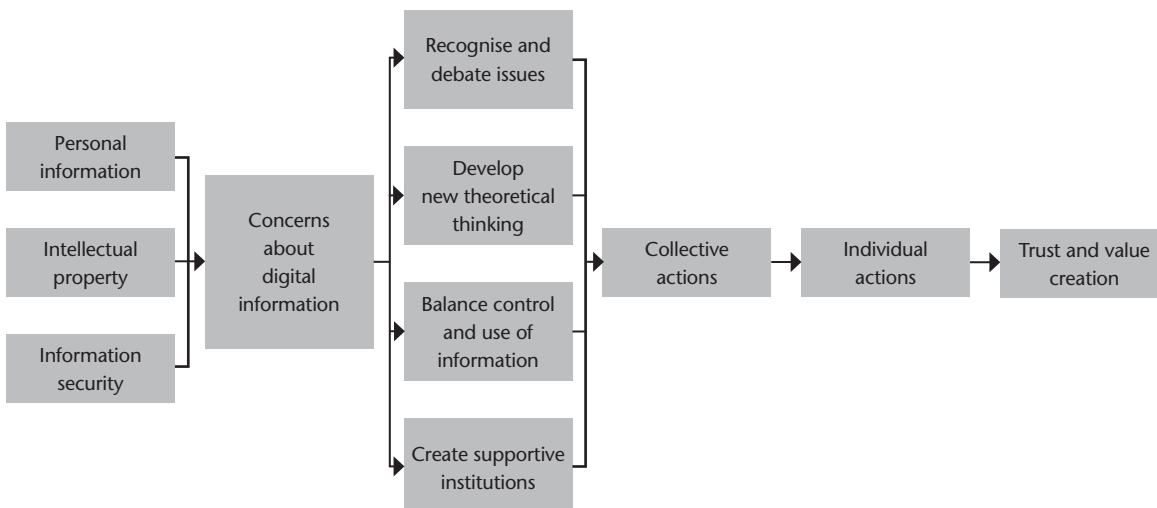
Finally, the changed economics of information is at the heart of all these issues. The opportunities to collect, use and share almost unlimited amounts of information transform the economic incentives around information and increase the risks around it significantly. They also raise profound challenges to established rights over information, such as who should benefit from the commercial exploitation of personal information or user-generated intellectual property.

## 1.6 Our approach to building trust

Trust is an important feature of any economy and society. It enables businesses and individuals to carry out economic transactions and social interactions in the belief that other parties will behave in a non-harmful way. Building trust that other parties will secure and use digital information in acceptable ways is therefore an important element of addressing concerns about, and building confidence in, a digitally-based economy.

Our approach to building trust in the digital age is represented in Figure 1.1.

Figure 1.1: ICAEW approach to building trust in the digital age



Concerns about digital information can stem from three sources – personal information, intellectual property and information security.

In order to address these diverse concerns, we need to underpin specific actions and solutions in four ways:

- recognise and debate issues which arise around the collection, use, sharing and exploitation of digital information;
- develop new theoretical thinking which addresses the radically changed economics of the digital environment;
- balance control and use of information so as to maximise the benefits which can be realised from it; and
- create supportive institutions that can develop a variety of practical solutions and encourage the evolution of new social norms.

These elements underpin the collective actions that can be taken by governments, businesses, the technology industry and individuals to address concerns about digital information. Collective actions could include regulation, voluntary codes of conduct and consumer pressures on businesses.

In turn, collective actions inform the individual actions that a business can take around digital information. These actions are reflected primarily in good practices in information security and personal information.

All of these different elements contribute to building trust in the behaviour of individual businesses and the wider social and legal framework which surrounds digital information. This will ultimately enable businesses, individuals and economies more broadly to achieve sustainable value creation through digital technology.

Our approach to addressing concerns is therefore based on the belief that businesses cannot build trust in isolation. While they are necessary, today's good practices are not enough. Businesses operate within a network of formal and informal norms which influence and limit their actions. As a result, good information practices are ultimately grounded in clear rights and duties over information and need to be built on an accepted framework of social expectations and laws.

Digital technology is disrupting and challenging many aspects of the existing social and legal environment. The economic effect of IT is playing a powerful role in undermining and challenging established expectations around information and this uncertainty has a significant impact on businesses.

Where the wider legal and social environment is not clear, business practices are weakened, often becoming 'tick box' compliance exercises without clear reference to an underlying framework of rights and duties. The resulting uncertainty presents businesses with difficult decisions on how to innovate with information in ways which are socially acceptable.

Consequently, it is not enough for businesses to implement today's good practices in isolation. We also need to encourage widespread engagement, understanding and debate of the issues presented by digital information to build a social and legal framework which is broadly accepted and can underpin individual business actions.

## Report structure

This report consolidates and summarises a wide range of academic and business literature to map out:

- current understanding of information rights and good practices; and
- areas which are testing the limits of knowledge and practice.

It is structured in the following way.

Chapters 2 and 3 consider the current business environment for personal information and intellectual property in turn and therefore set out the context for individual and collective actions in these areas. Each chapter:

- summarises what we know about information rights, outlining key legal and commercial considerations for businesses; and
- outlines areas of growing contention, highlighting the underlying philosophical and economic debates about information rights and considering new practices which are testing the limits of established thinking.

Chapter 4 focuses on information security. It also includes good practices around personal information and intellectual property.

Finally, Chapter 5 goes on to consider collective actions and outlines the elements we think are needed to underpin broad trust in digital information, namely recognising and debating issues, developing new theoretical thinking, balancing the control and use of information and creating supportive institutions.

Throughout this report, we refer primarily to businesses. However, we believe that much of our analysis is also relevant to government and not-for-profit organisations, both of which need to balance the opportunities and risks that technology brings. In addition, we recognise that there are some specific issues for governments which we highlight specifically in Chapters 2 and 3.

We also focus our analysis on business risks related to digital information. While we recognise that there are serious risks related to national security and critical infrastructures, for example, from information security failures, this report focuses on business-related aspects of security. We also recognise the important contribution that technology will make to resolving these issues. While we have not highlighted these aspects in detail and are skeptical that technology can solve all of the problems around digital information, technological solutions form an important aspect of building trust.

## 1.7 Summary

Information technology (IT) transforms the way that many businesses operate and presents tremendous opportunities to increase revenues, cut costs and create new customer value. However, alongside these opportunities, there are growing concerns about the control and security of digital information which a business needs to manage in order to capture and retain value from IT. These concerns are fuelled by:

- high-profile data breaches and the growth of cyber attacks;
- individual experience of identity theft, phishing emails, spam and computer viruses;
- controversial use of personal information by governments and businesses; and
- repeated failures to secure intellectual property and prevent others from exploiting it.

These incidents can result in substantial financial losses for businesses, governments and individuals, damaged reputations and reduced confidence in IT systems more broadly. Therefore, this is an area of growing importance for business and economic success. Furthermore, these issues affect all of us as individual consumers or citizens.

Trust is an important feature of any economy and society. It enables businesses and individuals to carry out economic transactions and social interactions in the belief that other parties will behave in a non-harmful way. Building trust that other parties will secure and use digital information in acceptable ways is therefore an important element of addressing concerns about, and building confidence in, a digitally-based economy.

Our approach to addressing concerns is based on the belief that businesses cannot build trust in isolation. While they are necessary, today's good practices are not enough. Businesses operate within a network of formal and informal norms which influence and limit their actions. As a result, good information practices are ultimately grounded in clear rights and duties over information and need to be built on an accepted framework of social expectations and laws.

Digital technology is disrupting and challenging many aspects of the existing social and legal environment. Consequently, it is not enough for businesses to implement today's good practices in isolation. We also need to encourage widespread engagement, understanding and debate of the issues presented by digital information to build a social and legal framework which is broadly accepted and can underpin individual business actions

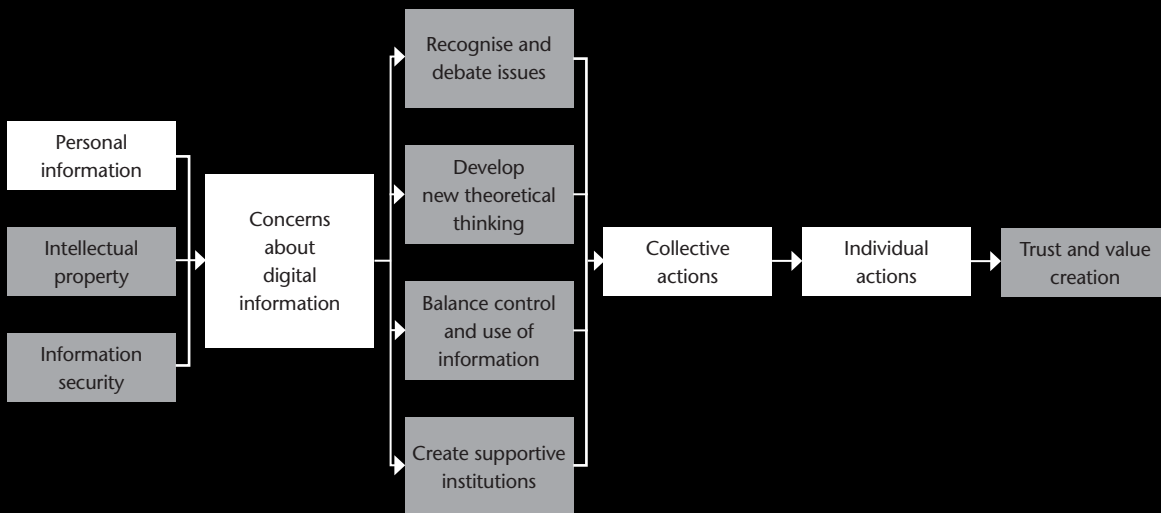
By summarising a wide range of business practice, underlying theory and new areas of debate, this report aims to achieve two principal benefits:

- to help management make better decisions about digital information and improve business performance in relation to information risks; and
- to inform widespread public debate about digital information and thereby support the development of a variety of regulatory, industry and social solutions.

In the process, it brings together three areas of thinking that are often looked at separately: privacy, intellectual property rights and information security. While these continue to be distinct fields, the digital environment brings them closer. As a result, this report takes a first step in bringing together key elements of a disparate and complex literature to support more integrated business practices and policy-making.

## 2. RIGHTS OVER PERSONAL INFORMATION

Rights over personal information enable individuals to control information about themselves for a range of individual and social benefits. However, personal information is also a valuable business resource. As IT increases the ability of businesses to gather, aggregate, analyse and share personal information, what are the risks to individuals and society from greater use of personal information?



## 2. RIGHTS OVER PERSONAL INFORMATION

### 2.1 The business value of personal information

Personal information is information that is associated with an identifiable individual, such as name or address. It can also include information which is less specific but which, when combined with other data, can be used to identify an individual, for example combinations of age, workplace and gender.

Most businesses hold personal information about employees and customers as part of their day-to-day operations. Personal information can also be used to generate revenue, for example:

- tailoring products and services to individual customers based on known preferences;
- marketing products to existing or potential customers;
- giving advertisers access to customers or service users; and
- selling it to third parties for marketing or advertising purposes.

As a result, personal information can be important intellectual property, especially for consumer or advertising-based businesses. However, IT has vastly increased the value that a business can derive from it.

#### Increased volume of personal information

The reduced costs of information achieved through IT mean that businesses and governments can collect and store vastly more personal information than was previously possible. This trend is aided by the digitisation of activities, with social and economic interactions increasingly carried out on the internet or underpinned by IT systems.

Information about our characteristics, location and activities can be captured through a wide range of technologies, such as:

- CCTV cameras which capture images of individual movements and activities;
- road traffic technologies which recognise number plates and record the movements of vehicles;
- transport technology systems which record when and where individuals access public transport systems;
- credit card systems which record the time and location of all purchases;
- social security and tax records which record income and other financial information;
- smart energy meters which track individual consumption of energy;
- entry cards to workplaces which record when employees enter and leave buildings;
- electronic patient records which capture details of patients' illnesses and treatments;
- mobile phone records which log the calls and locations of individuals; and
- passports and other identity documents which record when individuals cross borders.

#### Greater value from personal information

The power of IT goes beyond simply collecting information. It allows sophisticated searching, matching, aggregation and analysis of information that would have been impossible using paper-based systems.

Aggregation techniques in particular radically change the impact of the information gathered. They shift the context of information and transform what may have historically been relatively innocuous data, much of which is already public, into something far more powerful.<sup>8</sup>

<sup>8</sup> Helen Nissenbaum, 'Protecting privacy in an information age: the problem of privacy in public'.

By piecing together disparate pieces of information about individuals, their locations, activities and preferences, it becomes possible to develop rich profiles which can then be used for many purposes, such as:

- segmenting audiences to personalise and target products, services, marketing and advertising; and
- differentiating between customers in the delivery or pricing of products and services.

This leads to a wide range of potential benefits for businesses and is resulting in many new business models based on the analysis and commercial exploitation of personal information. It can also generate greater value from services for customers.

## 2.2 Legal considerations

While many businesses may want to make extensive use of personal information, individuals retain rights over information about themselves and businesses have a range of duties regarding their use and treatment of personal information. In Europe in particular, personal information is subject to substantial regulation. Personal information can also be protected through laws targeted on sensitive pieces of personal information or based on the human rights framework, including the right of privacy. It can also be protected through commercial pressures.

### Data protection laws

Data protection regulation protects the rights of individuals around the collection, processing and sharing of their personal data. Principles of data protection were originally developed in the 1970s and were followed in the early 1980s by the declaration of the Fair Information Principles by the OECD and the Council of Europe.

#### Panel 2.1: OECD Fair Information Principles

The OECD's eight basic principles were stated in its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These principles have been hugely influential and form the basis of many national laws in this area, such as the UK Data Protection Act 1998 and EU Directive 95/46/EC on data protection.

The principles can be broadly described as follows.

- Collection limitation principle: data should be collected legally with the consent of the data subject where appropriate and should be limited to the data that is needed.
- Data quality principle: data should be relevant and kept accurate.
- Purpose specification principle: the purpose should be stated at the time of data collection.
- Use limitation principle: personal data should not be used for other purposes unless with the consent of the individual.
- Security safeguards principle: personal data should be protected by a reasonable degree of security.
- Openness principle: individuals should be able to find out what personal data is held and how it is used by an organisation.
- Individual participation principle: an individual should be able to get details of all information held by a data controller about them and challenge it if incorrect.
- Accountability principle: the data controller should be accountable for complying with the principles.

The European Union has taken a lead role in this area in order to pursue dual objectives. First, harmonisation of the rules aims to facilitate the free flow of personal information across Europe and support the single market. As such, it provides a broad framework to enable the sharing of personal information across Europe without the need for individual contracts. Second, it views the protection of personal information as a fundamental right and the legislation aims to support the observation and enforcement of this right.

## Panel 2.2: The EU regime of data protection

In EU Directive 95/46/EC, the EU implements the Fair Information Principles, along with some key additional requirements. Particular features include:

- the establishment of an oversight and enforcement body, such as the UK's Information Commissioner's Office (ICO);
- additional requirements relating to electronic files; and
- limits on the international transfer of personal information.

This regime therefore provides strong protection of personal information, with clear rights given to individuals and mechanisms for enforcement. It also enables the transfer of personal information across the EU.

However, critics argue that it is a cumbersome, inflexible and administrative approach that has been implemented inconsistently across member states.<sup>9</sup> Obligations regarding the transfer of data outside the EU are often described as particularly dated, given the high degree of international working in many businesses. Workarounds have been put in place to overcome some of these challenges, such as safe harbours, Binding Corporate Rules (BCRs) and model contract clauses. These mechanisms provide ways for multi-national businesses to adhere to acceptable standards and move personal information around the world. They are, though, difficult to apply and few countries or businesses have been successful in being accepted through these mechanisms.

Furthermore, critics argue that data protection regulation potentially gives too much protection to information that is not particularly sensitive, with no reference to harm or risk. As a result, data protection can place heavy duties on businesses to comply with rules which may not be justified by the benefits of regulation.

## Targeted laws

In contrast to Europe, the US does not have a comprehensive regime of data protection. Instead, it has a variety of laws which are targeted at the protection of particularly sensitive pieces of information.<sup>10</sup>

## Panel 2.3: US privacy laws

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, is one of the best-known pieces of US regulation in this area and concerns health records. One of the Act's key provisions concerns the strict privacy of health records and payment information. It also specifies a number of security measures that should be taken to protect health information. However, the Act has been criticised on the basis of its complexity, administrative burden and cost. Some doctors also argue that it has stifled research and follow up consultations.<sup>11</sup>

Another example is the law enacted by the State of Massachusetts which sets out appropriate standards for protecting the personal information of anyone resident in the state.<sup>12</sup> It applies to all businesses, wherever they are situated in the world. The law sets out a range of security standards which need to be followed, including authentication measures, encryption of all personal information stored on portable devices, up-to-date firewalls and virus protection and employee education on information security. While many of these measures could be seen as good security practices, some businesses have argued that compliance with the law has been onerous.

<sup>9</sup> Neil Robinson, Hans Graux, Maarten Botterman and Lorenzo Valeri give a summary of the strengths and weaknesses of the current approach in their *Review of the European Data Protection Directive*.

<sup>10</sup>For a good overview of the various protections in US law, see John T. Soma, J. Zachary Courson and John Cadkin, 'Corporate privacy trend: the 'value' of personally identifiable information ('PII') equals the 'value' of financial assets'.

<sup>11</sup>Jennifer F. Wilson, 'Health Insurance Portability and Accountability Act Privacy rule causes ongoing concerns among clinicians and researchers'.

<sup>12</sup>See 201 CMR 17.00 Standards for the Protection of Personal Information for Residents of the Commonwealth.

## Human rights laws

Personal information can also be protected through the human rights framework and the specific right of privacy.

### Panel 2.4: Privacy as a human right

The original statement of modern human rights is the 1948 UN Universal Declaration of Human Rights. This document was based on the experiences of World War II, where the collection and use of personal information about individuals' identity and ethnicity had such terrible consequences. As such, Article 12 of the Declaration reads:

'No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.'

This article is reflected in many subsequent human rights documents, including the European Convention of Human Rights, and national constitutions and charters of rights such as the UK Human Rights Act 1998.

In practice, the right to privacy is largely used by the rich and famous to protect themselves from photographers and journalists. As such, the main issues here frequently concern the balance between a right to privacy and the freedom of the press. In these circumstances, a privacy right may be outweighed by the freedom of the press where the public interest is deemed to be more important and justifies the publication of personal and sensitive information. This is especially the case for people in positions of public responsibility, although it can also be said more generally for those in the public eye.

However, the right to privacy may be developing broader application and was invoked in the 2011 News of the World phone hacking scandal in the UK by ordinary individuals, such as victims of high-profile crimes.

There is also growing difficulty in enforcing privacy rights in an environment of global media platforms. The case of super injunctions in England highlights some of these problems.

### Panel 2.5: English super injunctions and the internet

Following the implementation of an explicit right to privacy in the UK Human Rights Act, the English courts began to grant what became known as 'super injunctions' to stop the press publishing certain pieces of personal information about individuals. While injunctions have been available for many years, the super injunction was notable for the fact that the press were also prohibited from disclosing that an injunction had been granted.

However, super injunctions were only enforceable in England and media in other countries could publish the information freely. Furthermore, the apparent anonymity of many social media platforms encouraged the breaching of the injunctions.

A media storm erupted in the spring of 2011 as individuals posted information on global platforms, such as Twitter, about the identity of those holding super injunctions.<sup>13</sup> Once the information was released, it was impossible to enforce the prohibition in practice, regardless of the actual legal position.

## Informal regulation

While not a formal legal constraint, a business may want to comply with voluntary codes of conduct. Voluntary codes typically contain rules and regulations which are specific to the needs of particular industries. This can focus attention on areas which are particularly risky and can be a more flexible and responsive approach than formal regulation.

There is a danger, though, that informal regulation can become self-serving and fail to provide sufficient levels of protection to individuals. It can also be confusing if different codes of conduct apply to different industries, making it difficult to identify and enforce an individual's rights.

<sup>13</sup>BBC News, 'Twitter user in bid to break super-injunctions'.

## Panel 2.6: US Federal Trade Commission approach

The US Federal Trade Commission (FTC) developed an early version of Fair Information Principles which focuses on four key areas.

- Notice: before collecting personal information, a business should give consumers notice of its privacy practices.
- Consent: consumers should have a choice as to how their personal information is used, and should be able to opt out of secondary uses of their personal data by the business.
- Access: consumers should be able to access information held about them and make sure it is accurate.
- Security: a business should ensure that any personal information that it holds is secure.

In contrast to the EU, the FTC originally took a less formal approach in which businesses were left to adopt the principles on a voluntary basis. However, this approach seemed to have limited success. For example, in a survey from 2000, entitled 'Protecting privacy online: is self-regulation working?', Mary Culnan found that only 14% of privacy disclosures by online businesses constituted a full privacy policy, suggesting that most businesses were not following the principles fully.

The FTC has subsequently taken a more proactive approach, pursuing a number of high-profile data breach cases through the courts and obtaining substantial financial settlements in the process. Furthermore, in 2010-2011, it charged Google with privacy breaches surrounding the launch of its Buzz product. In the resulting settlement, Google was barred from misrepresenting its privacy policies, required to implement a comprehensive privacy policy and be subject to third party audits on its privacy practices every 2 years for 20 years.<sup>14</sup>

## The principle of accountability

The current regulatory framework is under pressure from two sides.

- There is pressure from individuals and consumer and civic groups to strengthen rights against the business use of personal information, especially around new practices such as behavioural advertising. This is seen in proposals to strengthen European laws, as well as proposals for legislation in the US.
- There is pressure from businesses to minimise regulation, especially regulation that they see as inflexible and process driven. There is also a desire to simplify the international regulatory environment.

To address these pressures, a different approach has been proposed which focuses on the principle of accountability as a means of protecting personal information in this complex environment. While accountability was included in the OECD's Fair Information Principles, it is being developed as an alternative approach to prescriptive regulation around personal information.

Advocates of the accountability approach maintain that it is no longer realistic in practice for an individual to have full and meaningful control over who has access to their personal information given the amount of data that is available, captured and exchanged by businesses. However, by making businesses more accountable for their use of personal information, individuals can develop greater confidence that businesses are respecting their privacy rights. Therefore, the notion of accountability takes a principles-based approach which focuses on outcomes, rather than laying down specific rules concerning exactly who can access information under what circumstances. This enables jurisdictions and businesses to develop their own approach to protecting personal information, depending on specific circumstances.

Daniel Weitzner, leading a group of academics which includes Tim Berners-Lee, has argued in favour of the concept of information accountability. In an article entitled 'Information accountability' (2008), he defines it as:

'the claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is used lawfully and appropriately by others.'<sup>15</sup>

<sup>14</sup>Federal Trade Commission, 'FTC charges deceptive privacy practices in Google's rollout of its Buzz social network'.

<sup>15</sup>Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler and Gerald Jay Sussman, 'Information accountability', p87.

## Panel 2.7: Information accountability and the Fair Credit Reporting Act

To provide an example, Weitzner et al highlight the Fair Credit Reporting Act (enacted in the US in 1970) as an example of regulation which focuses on outcome, and the use of the information, rather than controlling what information is collected or who has access to it.

Under this Act, credit agencies are able to collect whatever information they feel is relevant to making a credit report. They can also undertake whatever analysis they wish. However, their reports can only be used for the purposes of credit or employment checks and not for any other kind of profiling. Penalties are in place in the event of non-compliance and individuals have high levels of transparency around the process.

The Galway and Paris projects, which involved regulators, academics, lawyers, government representatives and IT industry experts, considered in more detail what accountability might look like in practice. Phase two of the project outlined nine core elements of implementing an accountability project:

- policies that reflect current laws and other relevant standards;
- executive oversight and responsibility for privacy;
- appropriate staff and delegation of responsibility to trained resources;
- education and awareness of the programme by staff and suppliers;
- ongoing risk assessment and mitigation relating to new products or processes;
- regular risk assessment and validation of the accountability programme;
- policies to manage major privacy events or complaints;
- processes to enforce policies internally; and
- a method of redress where privacy rights have been breached.

However, critics of this approach see it as a US-centric one, coming from a tradition of informal regulation and market-driven approaches, rather than recognising the human rights basis for privacy and the full scale regulation of Europe.

## 2.3 Market considerations

There may also be customer expectations and market pressures regarding the treatment of personal information. While market pressures do not have the force of regulation, they do drive organisational behaviour to some degree in market economies and support the observation of privacy. Indeed, where a business fails to protect privacy rights, market reactions and reputational damage are likely to be as harmful as direct financial losses arising from regulatory breaches.

There are two situations where market pressures are particularly important:

- where regulators and legislators are behind the latest business and technological innovations in personal information; and
- where businesses want to look beyond compliance and incorporate privacy as a brand value.

### Innovative use of personal information

One of the major economic success stories of recent years has been the tremendous growth of internet businesses, such as Google and Facebook. These businesses have typically made innovative use of personal information to create popular applications and platforms. However, many of these uses of personal information go beyond established regulatory or legal standards.

As a result, customer reaction can become an important limit on the business exploitation of personal information. Indeed, in many of the cases where businesses have changed their policies around personal information, it has been driven by consumer reaction and outrage, as much as by the threat of legal action. The impact of consumer outrage is demonstrated in the case of Phorm.

## Panel 2.8: Losing investor confidence: the case of Phorm

Phorm sells software which tracks the web activities of users and builds up a detailed picture of individual user preferences and interests. In order to generate revenue, it then uses this information to target advertising for its business clients. In 2008, Phorm signed deals with the UK's largest Internet Service Providers (ISPs) to give it access to the ISPs' customers and thereby build up an enormous database of profile information.<sup>16</sup>

This was an early example of behavioural advertising. Phorm had commissioned a report from Ernst & Young, which confirmed that its activities were legal. Consequently, its share price soared, given the lucrative opportunity which this appeared to present.

However, information emerged which suggested that Phorm had been trialling the system on the customers of one ISP, BT, without disclosing it to the individuals involved. While the legal advice had been clear that the practice was acceptable if consent was obtained, this scenario was more contentious. It also generated a substantial backlash from BT customers.

Phorm was never prosecuted by the UK regulators or the EU for breaches of the law, and privacy campaigners were not given permission to pursue a private prosecution. However, its reputation was badly damaged and investors deserted it.

## Privacy as a brand value

A business clearly has to comply with relevant regulations regarding personal information. However, it can choose to go beyond an approach of strict compliance and place strong respect for privacy rights as part of its wider corporate values and ethics.

By demonstrating good practices around personal information, a business may be able to earn greater returns in the long term. It may also be able to distinguish itself when competitors experience privacy failures and thereby avoid being tainted by association. Conversely, even if legally compliant, a perception of poor privacy practices can impact the reputation of a business. In this sense, privacy feeds into the wider brand value of a 'trustworthy business' and can play an important part in building this reputation.

## Panel 2.9: HP's position on privacy

The technology company HP has stated its position on privacy as one which goes beyond strict legal compliance. Linking privacy closely with wider corporate values and ethics, the HP Global Master Privacy Policy states:

'We follow privacy policies and data protection practices to comply with the law and to earn trust and confidence in HP and its business practices... All HP employees, board members, and contracted parties working on behalf of HP must comply with these policies, even if local law is less restrictive.'<sup>17</sup>

Based around the OECD Fair Information Principles, HP applies a single standard for privacy throughout its global business, which meets the stringent legal requirements of the EU and thereby applies stricter standards than are necessary in other jurisdictions, such as many parts of the US. To help in this, they have developed a highly contextual modelling tool which enables anyone working with customer information to design their processes and use of personal information to comply both with legal requirements and their broader privacy standards.<sup>18</sup>

The value of such an approach will depend on factors such as industry and brand positioning. Businesses that hold large amounts of information about individual customers, for example, are more likely to benefit from such an approach.

There is still limited evidence regarding the extent to which strong privacy protections are seen as a differentiating factor and many businesses continue to focus on the compliance aspects in practice. However, a study in 2006 by Acquisti et al suggests that privacy breaches do have a short-term effect on the market value of businesses.<sup>19</sup> This mirrors research on information security breaches highlighted in Chapter 1, which provides evidence for a reduction in market value when a breach is announced.

<sup>16</sup>Christopher Williams, 'BT and Phorm: how an online privacy scandal unfolded'.

<sup>17</sup>Available online at the HP Global Citizenship Center.

<sup>18</sup>The HP case study is outlined in *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices*.

<sup>19</sup>Alessandro Acquisti, Allan Friedman and Paul Telang, 'Is there a cost to privacy breaches? An event study'.

## 2.4 Underlying questions about privacy

The notion of a private space has been established since Aristotle's *Politics*. However, it remains a nebulous idea which is subject to diverse views on its scope and importance. We summarise some of the key theoretical arguments about privacy around the following questions:

- What is the scope of privacy?
- What is the role of consent?
- What are the benefits of privacy?
- What harm is caused by breaches of privacy?
- How should privacy be balanced with other interests?
- How can different cultural views be reconciled?
- How can we understand fragmented and inconsistent behaviour?

### What is the scope of privacy?

While it is a well-used term, the scope of privacy is hard to articulate and define. The idea of having a sphere of individual and family activity which is private dates back at least to Aristotle's *Politics*. Historically, the term referred primarily to physical privacy and protection from undue interference from the state. Therefore, it focused on protecting property from government search or seizure, as well as protecting the individual from physical searching or invasion.

Today, the prime focus of privacy is personal information. This was first illuminated in detail by Samuel Warren and Louis Brandeis in their seminal 1890 essay 'The right to privacy'. This essay was written against a backdrop of new photographic technology which was being used in an increasingly intrusive manner. Describing privacy as 'the right to be left alone', they argued in favour of a right of privacy in US law.

Through the 1960s, governments and businesses were increasingly using computers to process personal data. Mindful of this, in his book *Privacy and Freedom* (1967), Alan Westin developed the concept of information privacy into 'the ability to determine for ourselves when, how and to what extent information about ourselves is communicated to others'.<sup>20</sup> As a result, privacy became strongly linked with control over personal information.

Information privacy is an intrinsically subjective topic. As it is ultimately concerned with exercising choice about whether to keep information within a private domain or whether to share it with others, it will be strongly influenced by the psychology, social and political attitudes and personal experience of individuals. It is dependent on the specific context of information sharing. Sharing medical information with a doctor, for example, is qualitatively different to sharing it with an insurance company.

The scope of privacy has also changed substantially over time. Historically, privacy was largely a matter for the wealthy, who could afford to separate themselves physically from the poorer population and therefore develop an expectation of privacy. The rich may also have had an interest in keeping information about their wealth secret. In contrast, poorer sections of society who lived in overcrowded accommodation had little notion of privacy, little opportunity to exercise it and possibly less need for it.

Defining what behaviour is private or open to public scrutiny is another area grounded in a social context. For example, 50 years ago, homosexual acts and abortion were generally not seen as private matters which were left to the discretion of the individual. Instead, the state believed that it had a legitimate right to intervene and criminalise such behaviour. Attitudes have changed substantially since then and such actions are believed by many to fall within the private domain.

As a result, finding a singular definition of privacy has proved difficult at any point in time. While definitions such as those of Warren and Brandeis or Westin have been influential, they are quite distinct and demonstrate that the notion of privacy covers many different scenarios. Indeed, the number of distinct scenarios in which privacy is invoked is growing and includes:

- structured databases containing personal information for analysis and segmentation;
- the sharing of personal information across a range of businesses or government agencies; and
- the widespread and often voluntary sharing of public information and images about individuals.

<sup>20</sup>Alan Westin, *Privacy and Freedom*, p322.

In his article 'A taxonomy of privacy' (2006), Daniel Solove develops a taxonomy which defines four main types of privacy scenarios: information collection, information processing, information dissemination and invasion. Each of these types has a number of associated sub-types, such as information aggregation, surveillance, secondary use and exclusion. It may be that a taxonomy of this type could help to refine the analysis and discussion of privacy.

### What is the role of consent?

One important difference between privacy scenarios is the varying degree of individual consent over the use or sharing of personal information. Contrast, for example, scenarios where individuals have voluntarily shared information in return for benefits and where there has been opaque data gathering or sharing. Individuals are free to share what information they want with others. Consent is therefore an important solution to many privacy concerns. In practice, consent is usually gained through opt-ins and opt-outs relating to the capture, use and sharing of personal information.

However, the notion of consent is problematic. In many cases, especially in the area of law enforcement, security and police intelligence, consent is not relevant to the gathering of information. The state is entitled to gather information to protect citizens and they do not need to gain the consent of the suspect in order to do so. Other laws will set out the limits of what government agencies can do in this context.

Within the private sector, it is important to consider what really constitutes informed consent by an individual. Frequently, people click on a box to give consent without reading the terms and conditions and therefore without understanding exactly to what they are consenting. The amount of personal information that is being shared makes it potentially very cumbersome in practice to consent to every action.

People may consent to sharing information in order to obtain short-term benefits, without proper understanding or consideration of the full risks surrounding the long-term use of the information. It may be the case that if all businesses are operating in the same way, individuals have little choice in practice but to consent to the use of their personal information in order to benefit from the services offered.

Current conceptions of consent also focus on the initial decision to release information to another party. However, as information is increasingly aggregated and subject to radical shifts in context, an individual's consent may change over time as the implications of releasing information change.

### What are the benefits of privacy?

There are a number of different philosophical approaches which can be taken on the benefits of privacy. As a result, debates around the right to use or restrict access to personal information are often rooted in quite profound disagreements about the role of the state, the power of the market and the underlying foundations of society.<sup>21</sup>

#### Panel 2.10: Approaches to privacy

##### Human rights

Many promoters of privacy focus on its quality as a fundamental human right and its link with human dignity and personality. It also protects individuals from abuses of power.

##### Social value

Another way to approach privacy is to see its value in the broader context of society. As such, privacy can be seen to protect societal and democratic values, for example freedom of association. It can be associated with an innovative and creative culture, providing a private space to generate radical ideas and develop new things. It can also provide rules on how we treat one another, especially where there are competing interests.

##### Communitarian

By contrast, communitarians, led by Amitai Etzioni, argue against an individualistic approach that sharply distinguishes between the private and public spheres. Rather, they advocate a more community-based approach which does not accept a wholly private sphere of activity. Communitarians therefore dislike the idea of individuals separating themselves from the rest of society and minimise the role of privacy.

<sup>21</sup> Some of these are outlined in more detail in the online Stanford Encyclopaedia of Philosophy.

## Panel 2.10: Approaches to privacy (continued)

### Feminism

Some feminist thinkers are highly sceptical of the notion of privacy. Catherine MacKinnon, for example, argues that privacy represents the opportunity to hide the dominant behaviour of men behind closed doors and perpetuate existing power structures. However, other feminists see a strong role for privacy. Decisions such as *Roe v Wade* and *Griswold v Connecticut*, which affirmed a woman's right to abortion and contraception respectively in the US, were strongly grounded in privacy arguments.

### Economics

The Chicago Business School, and Richard Posner in particular, developed an economic approach to privacy in the 1980s. In economic theory, markets are efficient when each party has perfect information. More information improves the quality of the transaction, with lower transaction costs and a more accurate match between supply and demand. On this basis, buyers and sellers have no rational reasons for wanting to withhold information about themselves. If they wish to withhold information, it can only be to create a personal advantage. A buyer, for example, may not want a seller to know that he or she has a poor credit history. Many economists consequently see privacy as a barrier to efficient market transactions.

This deep divergence of views underlies many of the contentious debates seen today, making it difficult to find consensus about the scope and strength of privacy rights.<sup>22</sup>

## What harm is caused by breaches of privacy?

The variety of justifications for privacy, combined with the different scenarios in which privacy rights may be invoked, means that a range of possible harms is seen as resulting from breaches of privacy. Some of these are clearer and may possess more weight than others.<sup>23</sup>

Looking at privacy as a human right, the harm from privacy breaches is essentially subjective. There could be a sense that an individual's autonomy has been infringed and this could be seen as harmful in itself. There could be a feeling of embarrassment or a loss of dignity, for example, if a neighbour learns of a sensitive medical condition or financial difficulties.

Systemic breaches of privacy can be seen to erode wider social values. They may reduce underlying levels of trust in the government or between individuals. They may make people more conscious of their actions and thereby inhibit individual behaviour and creativity. Therefore, breaches could result in long-term changes of behaviour and undermine democratic institutions.

Many concerns centre on how personal information will actually be used and the direct harm that this could cause individuals, for example:

- there could be financial loss where personal information is appropriated by criminals; and
- individuals could be discriminated against or targeted on the basis of personal characteristics or past behaviour.

Perceived harms from privacy breaches have strongly influenced the development of privacy protections. Privacy was recognised as a major issue following World War II, particularly in countries which had seen the targeting of particular groups or individuals based on personal information. In the Netherlands, for example, a detailed census which had been compiled about all citizens in the 1930s was immediately seized by the Nazis on invasion and used to identify and target Jewish citizens. As a result of this registration system and the accompanying identity cards, the Dutch Jews had the highest death rate of all Jews in Europe in World War II.<sup>24</sup> This direct link with human suffering led to the human rights framework of the late 1940s, which incorporated a right to privacy. Despite this experience, the use of national identity registers to target individuals has been seen on a number of subsequent occasions.

<sup>22</sup>For an interesting attempt to bring some of these ideas together, see Ann Cavoukian, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation*.

<sup>23</sup>For example the ICO categorises the harms as tangible harm to the individual, intangible harm to the individual and broader societal harm. See ICO, *Data Protection - Protecting People, a Data Protection Strategy for the Information Commissioner's Office*.

<sup>24</sup>William Seltzer and Margo Anderson, 'The dark side of numbers: the role of population data systems in human rights abuses'.

## Panel 2.11: Genocide in Rwanda and identity cards

A recent example of the use of national identity cards for horrific ends was seen in the Rwandan genocide of 1994, where an estimated 800,000 people were killed largely on the basis of their ethnic group.

The national identity card contained an ethnic group classification. Although it had been recommended to remove the classification, this had been ignored and identity cards were an important way of separating the ethnic groups. The identity cards of victims were then collected and handed to superiors.<sup>25</sup> Following the genocide, ethnic group was removed from identity cards.

Concerns about privacy grew substantially in the 1960s and 1970s as administrative tasks were computerised and governments and businesses started to store and analyse large amounts of personal information. At the same time, there was a growing distrust in governments, in particular, about how they may use personal information. As a result, there was increased regulation of the area to reflect these concerns.

The situation remained relatively stable until the explosion of the internet. Privacy became a major issue again as consumers left a growing digital footprint of activities and preferences.

However, the events of 9/11 and subsequent terrorist attacks round the world provide a stark counterbalance. The prevention of terrorist activities has become a key priority for all governments and privacy rights have often been eroded in the process.

### How should privacy be balanced with other interests?

Just as there are benefits to controlling access to personal information, there are also benefits to transparency and information sharing which need to be balanced in the application of privacy rights.

In his article 'Social and political dimensions of privacy' (2003), Alan Westin describes this clash between the benefits of transparency, surveillance and privacy:

'Though democratic societies value and institutionalize privacy, democracies must also provide for the disclosure of information necessary to the rational and responsible conduct of public affairs and to support fair dealing in business affairs. Officials must engage in surveillance of properly-identified anti-social activity to control illegal or violent acts. Managing this tension among privacy, disclosure and surveillance in a way that preserves civility and democracy, and copes successfully with the changing social values, technologies and economic conditions, is the central challenge of contemporary privacy definition and protection.'<sup>26</sup>

Different points of view reflect different economic interests. There are also deep differences which go to the heart of the relationship between the individual and the state. This section has highlighted a number of different arguments that can be used to promote or limit a right to privacy and central to each one is a particular view of the relationship between the individual, wider society and the state. Some approaches to privacy focus on the primacy of the individual. Other approaches highlight the social context of privacy and the need for privacy to work in conjunction with other rights and interests.

As a result, different weight may be put on different elements, for example, balancing privacy rights with:

- demands to protect security;
- opportunities to prevent harm to other individuals, for example through infectious diseases, child abuse and paedophilia;
- the need for medical and social research based on detailed individual information;
- financial benefits that can result from preventing tax or benefit abuse fraud; and
- opportunities for improved services, greater efficiency and lower prices.

<sup>25</sup>Jim Fussell, 'Group classification on national ID cards as a factor in genocide and ethnic cleansing'.

<sup>26</sup>Alan Westin, 'Social and political dimensions of privacy', p432. See also Kirstie Ball and David Murakami Wood, *A Report on the Surveillance Society for the Information Commissioner*.

## Panel 2.12: Balancing privacy and security

A major topic of debate is the potential conflict between privacy rights and the promotion of security, or the prevention of harm more broadly.<sup>27</sup> This is often couched in terms of ‘nothing to hide’ and the view that the only people who are worried about privacy are those who have something to hide. By contrast, innocent individuals who have done nothing wrong should have no objections to the government accessing information about them where these processes may increase security. This argument has been deployed increasingly since the 9/11 attacks as governments mine data about individuals and their activities to spot patterns, networks and suspicious activity.

Privacy advocates take a different approach. They argue that the ‘nothing to hide’ argument is based on a particular view of privacy, namely that it is concerned with hiding bad things rather than seeing it as a social value. The fact that an individual has done nothing wrong does not inevitably mean that they wish to share everything with the government. In his article “‘I’ve got nothing to hide’ and other misunderstandings of privacy’ (2007), Daniel Solove says:

‘The key misunderstanding is that the nothing to hide argument views privacy in a particular way—as a form of secrecy, as the right to hide things. But there are many other types of harm involved beyond exposing one’s secrets to the government.’<sup>28</sup>

He argues that there are many long-term effects on the relationship between state and citizen which also need to be considered in the debate. These could include the impact of discouraging individuals from acting freely and ‘chilling’ their behaviour. It could also lead to a breach of trust between individuals and the state.

Others argue that, in most cases, it is possible to make use of personal information to improve security while also recognising and respecting privacy. This requires clarity of objectives and methods so that only relevant information is retained or used. However, gaining clarity over information requirements often leads to increased costs and time, adding a further element to the decision-making process.

## How can different cultural approaches be reconciled?

Diverse views on the benefits and harms of privacy also reflect cultural groundings. Privacy, as outlined in this report, is largely drawn from Western political and philosophical traditions of individual liberty and other countries may have different concepts of privacy. Even between the US and Europe, though, there are major cultural differences over the meaning and basis for privacy.

## Panel 2.13: US and European attitudes to privacy

While there are strong notions of privacy in both the US and Europe, they reflect very different cultural and historical factors. As a result, the approaches are quite distinct, even though they all fall within the concept of ‘privacy’. In his 2008 article ‘The two Western cultures of privacy: dignity versus liberty’, James Whitman outlines distinct social and cultural contexts of privacy in the US, Germany and France.

In the US, privacy is strongly associated with protection from state interference and the right of an individual to do whatever they want within their private space. It is therefore libertarian in its focus and notions of privacy are at their strongest in connection with state-sponsored action. By contrast, privacy is not as strong in the commercial sector. Both the freedom of the press and the operation of the free market are equally strong pulls in the US. As a result, privacy is frequently of secondary importance when applied in the private sector, with market forces left to operate.

By contrast, in France and Germany, the notion of privacy is strongly tied to ideas of personality, dignity and control over an individual’s public image. In France, privacy laws descended from laws relating to insult. In Germany, they are drawn from Kantian ideas of personality and the right of all individuals to be treated equally and with dignity. As a result, privacy laws tend to be more restrictive of the press and focused on individual control over information which is made public. They are generally less concerned with state interference.

<sup>27</sup>For example, Information and Privacy Commissioner (Ontario) / Deloitte and Touche, *The Security – Privacy Paradox: Issues, Misconceptions and Strategies*.

<sup>28</sup>Daniel J. Solove, “‘I’ve got nothing to hide’ and other misunderstandings of privacy’, p767.

This complicates the protection of personal information by international businesses. Regulation around personal information is grounded in national legal systems, and therefore compliance is already complex for a business with operations in different countries. With different cultures, businesses also have to contend with potentially different attitudes and actions by employees, customers or suppliers.

### How do we understand fragmented and inconsistent behaviour?

One feature of changing technology is that social attitudes can become fragmented and inconsistent. While some people adopt new technology quickly, others are more cautious and recognise the risks that it may bring. Attitudes may also change quickly as more information about the technology becomes available.

It has even been suggested that different generations will take increasingly diverse approaches to the issues. Those who enjoy social networking sites, for example, suggest that the importance of privacy will shrink as people increasingly enjoy the benefits of widespread information sharing. Mark Zuckerberg, founder of the social network site Facebook, subscribes to this view:

'Privacy is no longer a social norm... People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people...That social norm is just something that has evolved over time'<sup>29</sup>

However, many individuals still exhibit significant concerns, especially when they believe that a business has gone too far in pushing services ahead of privacy considerations, for example in the case of Google's Street View service.

#### Panel 2.14: The varied reaction to Google's Street View

Google's Street View service was launched in 2007 and provides pictures of streets, buildings and other public features. Linked with Google's map service, it enables a user to view a street as if they were walking or driving along it.

It is primarily used for directions with some people also using it to help with activities such as house-hunting. In addition, it can showcase particular land marks. For example, VisitBritain, an agency which promotes the UK as a tourist destination, partnered with Google on Street View as a way to highlight a wide range of tourist hotspots round the country. Therefore, it can provide many benefits to a variety of users and Google has continued to expand the coverage of the service round the world on this basis.

Street View is simply utilising public information. It is taking photographs of public places, such as roads, cars and houses. Therefore, it is only capturing information that is available to anyone walking in the street.

However, Street View has been highly controversial.<sup>30</sup> Following a raft of complaints when it was launched, the UK's ICO subsequently ruled that the service is perfectly legal, provided that individuals cannot be specifically identified. Likewise, car number plates need to be blurred. Nevertheless, controversy continues and surveys show that people are particularly worried that the images could be used by burglars, although the police have no evidence of this. Furthermore, many feel that the service is an invasion of privacy, as they have not given consent for images of their property to be posted online.

As a result, it remains a controversial service which some people see as a valuable and fascinating resource, while others see it as a privacy violation. Reconciling these widely different reactions and expectations remains a challenge for businesses such as Google.

Hard evidence in this area is inconsistent. Surveys show that, despite a growth in information-sharing behaviours, individuals are increasingly concerned about the use of their personal information by businesses and governments. In a 2010 survey by the UK ICO, 92% of respondents were concerned about the protection of personal information.<sup>31</sup> This ranks second, just behind concerns about crime, and reflects an increase of more than 20% since 2004.

<sup>29</sup>Bobbie Johnson, 'Privacy no longer a social norm'.

<sup>30</sup>Sam Knight, 'All-seeing Google Street View prompts privacy fears'.

<sup>31</sup>Social and Market Strategic Research, *Report on the Findings of the Information Commissioner's Office Annual Track 2010*.

While these views should concern businesses, it should also be recognised that there has always been a section of public opinion which has strongly valued privacy irrespective of developments in IT.

This is brought out by Alan Westin's research on consumer attitudes on privacy. He describes three types of person:

- privacy 'fundamentalists', who are highly distrustful of organisations which collect personal data and exercise privacy controls as far as possible;
- privacy 'pragmatics', who weigh up the benefits of sharing information in particular cases, assess businesses on the basis of their privacy practices and want as much information as possible to support informed decision making; and
- privacy 'unconcerneds', who generally trust organisations in data gathering and have no significant concerns about the use of their personal information.

In the first of a series of surveys undertaken by Westin in 1990, approximately 25% of the US public were fundamentalists, 57% were pragmatics and 18% were unconcerned.<sup>32</sup> As a result, many concerns are not new. A significant proportion of the public were extremely concerned about the use of their personal information prior to the internet and the emergence of many of the issues raised in this report.

Furthermore, we frequently see inconsistent behaviour around personal information and people often do not act rationally in sharing personal information. Information sharing is a trade-off, whereby individuals get a benefit from handing over information about themselves. They therefore make a choice as to whether this is an acceptable trade-off.

The evidence suggests that people have difficulty in exercising choice effectively. In practice, they often give away significant information about themselves in exchange for fairly small rewards, despite affirming a strong belief in privacy. There is a growing stream of research in the field of behavioural economics which considers this apparent contradiction between a desire for privacy and a willingness to share information widely.<sup>33</sup>

The timing of costs and benefits are seen to be particularly important in this regard. On the one hand, individuals are passing over personal information for an immediate and specific benefit. The risks of privacy breaches, on the other hand, are both long-term and not certain. In most cases, there will be no direct cost or loss from sharing personal information with another party. As a result, individuals often underestimate and disregard the risks attached to privacy when offered an immediate gain.

However, there is a growing need to understand consumer and citizen views better, raise awareness of individual rights and responsibilities over personal information, and ensure that concerns are channelled appropriately. Consumer and civil society groups therefore have an important role to play in debates.

### Limits of the current framework for personal information

IT increases the value of personal information, leading to greater business use and commercial exploitation of it. This is also leading to growing contention about the limits of business use of personal information and the ways in which individuals can retain control over it.

Sections 2.5 to 2.7 highlight three examples where established rights and regulation are being stretched by new possibilities:

- The pervasive collection and retention of personal information means that **more is known and remembered**.
- The sophisticated use of personal information in the private sector means that **businesses are extensively profiling individuals**.
- Wide sharing of personal information across the public sector means that **governments are connecting information about citizens**.

<sup>32</sup>For a summary of Westin's studies over the years, see Ponnurangam Kumaraguru and Lorrie Faith Cranor, *Privacy Indexes: A Survey of Westin's Studies*.

<sup>33</sup>Alessandro Acquisti and Jens Grossklags, 'What can behavioral economics teach us about privacy?'

## 2.5 Collecting and retaining personal information

While data protection principles limit the personal information that can be collected and retained, emerging practices and technologies enable businesses to gather increasing amounts of user and location information. Regardless of its ultimate use, the extensive collection and retention of information in itself may cause individuals concern and discomfort. For example, simply collecting information in some circumstances could be seen as a breach of human rights, impinging on the dignity of individuals.

Furthermore, collecting and retaining information may have long-term social effects. The inability to 'forget' personal information, for example may have long-term effects on society as individuals become more conscious of their actions and inhibit their behaviour accordingly or suffer disproportionate consequences.

There are also practical concerns, for example:

- having large amounts of personal information increases the risks of a data breach as well as the costs of maintenance; and
- retaining personal information encourages its use in various ways, putting more pressure on privacy rights.

### Collecting information

In the course of any transaction, a business will potentially collect a variety of personal information. While a direct cash transaction will require no personal information at all, ordering goods on the internet, for example, will require some personal information, such as financial and delivery information.

In addition, a business can also collect information which is not strictly necessary for the completion of the transaction. While there may be regulatory requirements about the information that can be requested, a business may ask for information such as alternative contact details, demographic information or product and service preferences. An individual may also agree to provide a business with far more extensive information about themselves and their activities in return for discounts or other benefits. Store loyalty cards, for example, are voluntary schemes which enable a retailer to link financial transactions with particular individuals, thereby providing substantially richer information about customer preferences and trends which they can analyse.

In these two cases, the data collection has been consensual, for specific purposes and where there are established regulations. However, as data gathering goes increasingly beyond information associated with specific transactions, the limits are becoming less clear. This is especially the case where information has been aggregated with other pieces of data or where it is being used for a markedly different purpose.

Public and location-based data, for example, is increasingly captured by surveillance cameras, transport systems or phone companies via wireless and other technologies which are becoming embedded in everyday objects. In these cases, the individual may be unaware that data about them is even being collected. The opportunities presented by RFID technology, for example, highlight some of the risks here.

#### Panel 2.15: 'The internet of things' and privacy

The 'internet of things' is a term used to describe what is seen as the next generation of technology whereby chips are embedded into everyday physical objects and are able to transmit, capture and store information. As a result, all kinds of information about location, status and activity can be captured and transmitted. One such vision is outlined in a write up of an EC-sponsored workshop in 2008 which considered the implications of the internet of things:

'... an individual's mobile phone may consult any stationary sensor in the room about its location, the thermometer on the wall about the temperature and the hygrometer about the local weather, and communicate this to the person's friends; and their phones will play their friend's tune when the person is entering the same building.'<sup>34</sup>

The opportunities to change the way we do things are enormous. However, there are significant privacy concerns in this area, as so much information will be captured about locations and activities. While each piece of information may not be personally identifiable, it could be fairly easy to identify individuals from a combination of pieces of information. This raises questions about what information is being captured, what it could be used for and who can benefit from it.

<sup>34</sup>Output from European Commission / EPoSS expert workshop, *Internet of Things in 2020: Roadmap for the Future*, p5. See also ICAEW's response to the related EC-consultation on this topic.

There is also substantial tracking of the activities of individuals on the internet, frequently without their knowledge or consent. This kind of tracking supports behavioural advertising, which is discussed in more detail in panel 2.17.

How regulators should approach this widespread collection of information is not yet clear. As mentioned earlier in this chapter, those who support the approach of accountability may suggest that attempts to stem the tide of information capture are likely to fail and regulators should instead focus on how information is used. Others point to technical solutions which anonymise data or process transactions without disclosing identity details. This may enable businesses to capture information and realise some benefits from it while not identifying specific individuals.

The role of consent is another important underlying question. While this may be an appealing solution, and one that the EC is following in its e-privacy directive,<sup>35</sup> it presents many practical issues around what constitutes consent, how consent can be given and the extent to which individuals are informed about the risks attached to personal information. It raises serious challenges as the context and value of information shifts through aggregation or analysis techniques. Consumers also need to be presented with a real choice, and not feel that they have to consent simply to participate in the digital economy.

## Retaining information

Once a transaction is complete, a business may then delete related information, as it is no longer needed for the purpose of the original transaction. Alternatively, a business can look to retain and reuse the information, provided that it has complied with regulatory requirements, such as gaining consent from the data subject. Most commonly, this reuse would be for marketing purposes.

Like collecting information, retaining personal information in itself potentially has some implications of harm to individuals, regardless of how it is used. In particular, it potentially breaches what the European Commission has termed a 'right to be forgotten'. The EC sees that individuals should have an enforceable right for information about them to be deleted when they want, and thereby enable them to be 'forgotten'.<sup>36</sup> Such a right is central to any claims to be able to control personal information and concerns have arisen particularly in the context of social websites which do not delete the profiles of individuals who have deactivated their account.

Furthermore, keeping personal information forever potentially has long-term implications for the nature of society, as outlined by Viktor Mayer-Schönberger.

### Panel 2.16: Losing the power to forget

In his book *Delete: The Virtue of Forgetting in the Digital Age* (2008), Viktor Mayer-Schönberger argues that losing the power to delete information potentially has a massive impact on our society. While having all this information available may seem to offer many benefits, it may also have a 'chilling' effect on what people do and what information they are prepared to share.

As individuals, we forget embarrassing or stupid behaviour from our youth and we would choose not to share that information with potential employers, for example. Losing the ability to 'forget', and being continually aware of the possible impact of actions or activities in the future, may reduce our ability to act freely:

'Forgetting plays a central role in human decision-making. It lets us act in time, cognizant of, but not shackled by, past events. Through perfect memory we may lose a fundamental human capacity—to live and act firmly in the present.'<sup>37</sup>

We also forget as a society and enable individuals to have a second chance, for example in the cases of failed marriages or businesses. By retaining vast amounts of information about every individual, we potentially change some of these mechanisms and force individuals to live with the consequences of their actions forever.

An example of the direct harm to individuals from such data retention is found through the growing practice for employers to search the internet for potentially damaging information or photographs of employees or job candidates. A survey by Microsoft in 2010 even suggested that 70% of HR managers have rejected job candidates because of information they have found on social networking sites.<sup>38</sup>

<sup>35</sup>ICO, 'UK businesses must 'wake up' to new EU law on cookies, Information Commissioner warns'.

<sup>36</sup>European Commission Justice Directorate-General, 'European Commission sets out strategy to strengthen EU data protection rules'.

<sup>37</sup>Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, p12.

<sup>38</sup>Michelle Sherman, 'Social media research + employment decisions: may be a recipe for litigation'.

Of course, HR managers typically exercise high levels of common sense in reaching their decisions and are perfectly aware that a picture of a young person engaged in high-spirited activity at a party does not indicate that the person is incapable of holding down a job. It may also be that, in many cases, the decision to reject, or not to promote, on the basis of the particular information discovered was very sound and completely justified. However, it demonstrates that there are risks of disproportionate consequences from the long-term retention of some pieces of personal information.

While retaining personal information can potentially lead to harm, though, deletion is also problematic in practice. Information that has been openly shared on the internet may have been copied or tagged by others and therefore it may be impossible to delete it entirely. There are also philosophical arguments. While as a society we have allowed people to forget bad marriages or bankruptcy, there are other events which we do not allow to be forgotten, such as serious crime.

As a result, we need to consider what information should be retained for what purposes which balances the different interests and recognises the technological realities of digital data and its propensity to be copied. It again raises the question of consent regarding the voluntary posting of information on social websites and the extent to which individuals should be left to manage the risks surrounding their behaviour themselves. There are also questions regarding the long-term implications for individual behaviour which remain unexplored at this stage.

## 2.6 Using personal information in the private sector

While profiling has been a business practice for many years, the sophistication of analytical systems, combined with the vast digital footprint created by most people, is making profiling much more powerful. This can provide benefits by targeting products and services to specific individuals. However, profiling can result in unequal treatment and can offend deeply-held perceptions of fairness. There is often a lack of due process and accountability about decisions. There are also concerns about the long-term impact of filtering information or services to narrow audiences based on this segmentation.

This section considers two particularly controversial applications of profiling by businesses:

- internet advertising; and
- price discrimination.

### Internet advertising

In the last ten years, the economy has seen the rise of internet-based businesses. Their business models are usually based on two key elements:

- providing free services to users; and
- raising revenue through the use of advertising.

Early internet advertising focused on the search process, so that when users searched for information about a particular topic, they were presented with adverts that were relevant to that topic. While still an important part of internet advertising, the industry has evolved, with adverts increasingly targeted to specific users based on their internet activities.

Indeed, advertising is particularly attractive on the internet because adverts can be heavily targeted to specific users. As websites can gather a wealth of information about users' desires and preferences every time they visit, it is possible to make a more accurate match between consumers and advertisers.

This type of advertising generally works by providing the advertiser with access to particular profiles of users to display banners or other types of adverts. It does not provide details of individual users to a third party and therefore may not breach privacy regulations. However, such techniques generally gather and exploit an enormous amount of personal information in order to generate revenue.

## Panel 2.17: Behavioural advertising

Behavioural advertising, highlighted in the Phorm case study, is advertising which is based on past internet browsing and online activities.<sup>39</sup> A business captures information about its website users and then targets advertising on that basis, or sells the information to a third party for this purpose. For example, a user who has been searching for holidays may be displayed a range of adverts related to flights and hotels when they log onto their email. A user who has joined particular social networking groups may be displayed adverts on that topic. Emails are typically scanned for key words, which are then used to segment the user for advertising purposes. It therefore goes far beyond simply advertising based on search terms and develops a deeper understanding of the individual user.

On the one hand, advocates argue that this type of advertising is beneficial as it targets adverts much more accurately than has previously been possible. This helps both advertisers and the individual, as the individual is getting adverts which are likely to be of more interest to them. Opponents, though, argue that users are largely unaware of the amount of personal information that is being captured and analysed and they are not consenting or in control of their information. Furthermore, they are then subjected to intrusive advertising which they may not want.

In the UK, the Internet Advertising Bureau has developed a code of good practice concerning such techniques.<sup>40</sup> Based on three core principles of notice, choice and education, the code aims to help consumers understand what data is being collected and how it is being used. Nevertheless, such advertising is an area of growing interest to regulators as techniques become more sophisticated and businesses gather increasing amounts of personal information to use for such ends.

However, techniques such as behavioural advertising fund many free internet products and services and are creating substantial value for businesses and shareholders. Without them, businesses would need to find other ways to fund their activities and this could result in users having to pay to access even basic internet services. Indeed, advocates argue that the value delivered to consumers through internet services linked to behavioural advertising outweighs the benefits derived by advertisers or the businesses in question.<sup>41</sup> Therefore, framing legislation that balances the protection of personal information with business innovation is challenging. Furthermore, given the rapidly evolving technology, ensuring that regulation is not easily evaded or quickly out-dated will be important.

A somewhat different approach to this challenge is presented by economists who suggest that individuals should be given full ownership rights over their personal information, which could be stored in a central data store.<sup>42</sup> They would then have the choice to sell it to other parties for advertising or other purposes. In this way, the individual would financially benefit from the use of their data. They argue that this would contrast with the current position, where businesses potential benefit from the use and exploitation of the personal information of millions of consumers.

However, this solution raises concerns about the extent to which individuals would make rational decisions about their personal information, especially where there is a direct financial benefit from allowing others access.

### Price discrimination

Price discrimination is the economic practice of charging customers different prices which are not related to the costs of serving the customers.

The economics of price discrimination are simple and attractive to businesses. Customers are often willing to pay different amounts for the same products depending on their circumstances and characteristics. Indeed, some people actually like to pay a higher price for what is essentially an identical product because it shows other people that they can afford it.

A business would clearly like to capture the maximum amount that each customer is prepared to pay. By doing this, a business can maximise their profits while still delivering products and services to satisfied customers.

<sup>39</sup> Julia Angwin, 'The web's new gold mine: your secrets'; Emma Conners, 'Up close and too personal'.

<sup>40</sup> Available online, [www.youonlinechoices.com/good-practice-principles](http://www.youonlinechoices.com/good-practice-principles)

<sup>41</sup> McKinsey, *Consumers Driving the Digital Uptake: The Economic Value of Online Advertising-based Services for Consumers*.

<sup>42</sup> For discussion of this approach, see Corien Prins, 'When personal data, behavior and virtual identities become a commodity: would a property rights approach matter?'

There are many well-established examples of price discrimination. Airlines, for example, charge passengers very different prices for seats next to each other based on when they book and the precise timing of their journey. However, price discrimination has been hampered in practice by the difficulty in understanding what each customer will pay. IT and internet profiling can provide far more sophisticated information and analysis of this and therefore potentially open the door to far greater price discrimination.

In an article entitled 'Privacy, economics, and price discrimination on the internet' (2003), Andrew Odlyzko argues:

'The key point is that price discrimination offers a much higher payoff to sellers than any targeted marketing campaign. Adjacent seats on an airplane flight can bring in revenues of \$200 or \$2000, depending on conditions under which tickets were purchased. It is the potential of extending such practices to other areas that is likely to be the 'Holy Grail' of ecommerce and the inspiration for the privacy erosion we see.'<sup>43</sup>

Many people see price discrimination as a perfectly legitimate and economically sensible business practice. Libertarians, for example, argue that even where price discrimination is at play, it still represents a transaction between consenting parties and it is simply a matter of individual choice as to whether to make a purchase on these terms. A customer can decide not to purchase a good at a higher price.

Overt price discrimination, though, remains a controversial and difficult subject for businesses to confront directly because it undermines many deeply-held beliefs about fairness. Conceptions of justice, such as that described by John Rawls,<sup>44</sup> have equal treatment at their core. To achieve just decisions, Rawls describes a 'veil of ignorance', whereby decisions are made on the basis of no knowledge of individual characteristics. Therefore, decisions should not deliberately advantage one group over another, as the decision maker has no idea to which group he or she belongs.

Historically, the 'veil of ignorance' has been real in many cases, as businesses or governments knew very little about individuals. However, this is changed fundamentally by rich individual profiles. While it may make economic sense for a business to be highly discriminating in its products and services, there are deeper questions around whether that is acceptable to wider society, for example:

- charging individuals who have a genetic predisposition to a serious illness substantially more for health insurance, or refusing coverage entirely; or
- charging higher prices to poorer individuals on the basis that they are less desirable customers.

While such practices happen already to some extent, personal profiling enables far more extensive discrimination in price and service provision.

Given these broader social concerns, Odlyzko argues that while price discrimination may become increasingly common in business, it is likely to remain hidden and covert. Instead, he suggests that tools such as payment, or part-payment, via loyalty cards instead of cash, personalised offers based on previous dealings with a business and bundling products and services together are likely to become more prevalent as proxies for price discrimination.

## 2.7 Sharing personal information across the public sector

The opportunity to share information across governments is often essential to increasing the efficiency and quality of public services. However, it raises practical concerns about the quality of information and how it is managed. It also leads to many questions about the degree of governmental power and control gained through centralising personal information.

### Rationale for information sharing

In most governments, information has historically been collected by individual agencies for specific purposes. While this is entirely appropriate, it has often resulted in high levels of inefficiency and potentially reduced the quality of services and outcomes, for example:

- the same piece of information is collected multiple times for different agencies, so it then needs to be stored and maintained multiple times; and

<sup>43</sup>Andrew Odlyzko, 'Privacy, economics, and price discrimination on the internet', p112.

<sup>44</sup>John Rawls, *A Theory of Justice*.

- it is difficult to join together information on the same individuals, potentially resulting in poor decision making and service.

The opportunity to share information more effectively across governments, therefore, is a very attractive one and is often an underlying condition to increasing the efficiency and quality of public services. However, it raises many concerns.

There are practical concerns about the quality of information and how it is managed. Where information is inaccurate, for example, sharing it multiplies these problems and it becomes very difficult to correct the information fully. The information may also not be of a good enough quality to be used in a different way. It is particularly important to compare the context in which information was originally gathered with the context in which it is to be reused. The information may be gathered in an informal context, for example, where complete accuracy is not essential. As a result, the information may not be robustly verified and may remain slightly inaccurate. If it is to be reused in a context where accuracy is essential, this could be problematic. It could also be out-of-date, unless there are robust procedures in place for updating information.

There are further concerns about the degree of power and control a government may gain through the centralisation of personal information, and how it could use this information to abuse power. Many of the fears relating to government use and abuse of personal information are exemplified in George Orwell's novel *1984* and the concept of 'Big Brother'.

The dangers of a government knowing everything about citizens are seen by many as great. A government could cause harm to individuals through discrimination and different treatment. Feeling under constant surveillance may reduce trust in one another and make us more cautious in our activities and expression. Therefore, even where the intentions of a government are benign, many see dangers in large-scale government collection and consolidation of personal information. Of course, where intentions are less benign, there are even greater risks of abuse and harm to individuals.

Furthermore, in many cases, such as crime prevention or security, the citizen does not consent to information being collected or reused. The government can also be a monopolistic provider of services in many cases, so that citizens have no choice about whether to release personal information. This situation changes the balance of power significantly and contrasts with business, where customers can choose between competitors.

### Approach to government information sharing

In a report commissioned by the UK government in 2008, Richard Thomas, the then Information Commissioner, and Mark Walport of the Wellcome Trust undertook a review of information-sharing activities in the UK public sector to determine the opportunities and challenges. They identified three core areas of information sharing, namely to:

- enhance security and crime prevention and detection;
- improve the quality and efficiency of services; and
- support medical and other statistical research.

They concluded that all three areas could potentially provide many benefits. Sharing information relating to security and crime could prevent future incidents happening and help to detect criminals or terrorists. Improving the quality or efficiency of services could reduce the costs of public services and improve the citizen experience, as well as improve specific outcomes. Research could help to improve the quality of life and healthcare. However, each had its own set of challenges and therefore each also needed a distinct style of thinking.

Where consent is not the appropriate basis of information use, such as in the cases of crime or medical research, the legal framework is based on the notion of proportionality. This means that in order for information sharing to go ahead, the risks and potential harm are outweighed by the potential benefits. Clearly, this has to be considered on the basis of specific situations.

In responding to the Thomas and Walport report, the British Computer Society argued that a fundamental weakness in proportionality is the identity of those whose benefits and risks are being compared. The interests of the government and the individual data subject will be very different, which raises serious challenges in applying proportionality. They argued:

'In most government Departments information risk management is largely concerned with Departmental benefits and Departmental risk. Until a robust and transparent means of incorporating risks to citizens' interests in information

risk management methodology is agreed, it is hard to see how the “objective judgement” commended by the review can be effectively applied.<sup>45</sup>

Following on from the report and responses to it, the ICO published a *Code of Practice for Data Sharing* in 2011. This includes a definition of data sharing, an outline of the legal environment, factors to consider in deciding whether to share data with other bodies and a wide range of specific practices around consent, security and governance.

## 2.8 Summary

Personal information is information that is associated with an identifiable individual. Most businesses hold personal information about employees and customers as part of their day-to-day operations. Personal information can also be used to generate revenue. As a result, personal information can be important intellectual property, especially for consumer or advertising-based businesses.

While many businesses may want to make extensive use of personal information, individuals retain rights over information about themselves and businesses have a range of duties regarding their use and treatment of personal information. In Europe in particular, personal information is subject to substantial regulation. Personal information can also be protected through laws targeted on sensitive pieces of personal information or based on the human rights framework, including the right of privacy. It can also be protected through commercial pressures.

The notion of a private space has been established since Aristotle’s *Politics*. However, it remains a nebulous idea which is subject to diverse views on its scope and importance. We summarise some of the key theoretical ideas about privacy around the following questions:

- What is the scope of privacy?
- What is the role of consent?
- What are the benefits of privacy?
- What harm is caused by breaches of privacy?
- How should privacy be balanced with other interests?
- How can different cultural views be reconciled?
- How can we understand fragmented and inconsistent behaviour?

IT increases the value of personal information, leading to greater business use and commercial exploitation of it. This is also leading to growing contention about the limits of business use of personal information and the ways in which individuals can retain control over it.

**More is known and remembered.** While data protection principles limit the personal information that can be collected and retained, emerging practices and technologies enable businesses to gather increasing amounts of user and location data. Regardless of its ultimate use, the extensive collection and retention of information in itself may cause individuals concern and discomfort. Furthermore, the inability to ‘forget’ personal information may have long-term effects on society as individuals become more conscious of their actions and inhibit their behaviour accordingly or suffer disproportionate consequences.

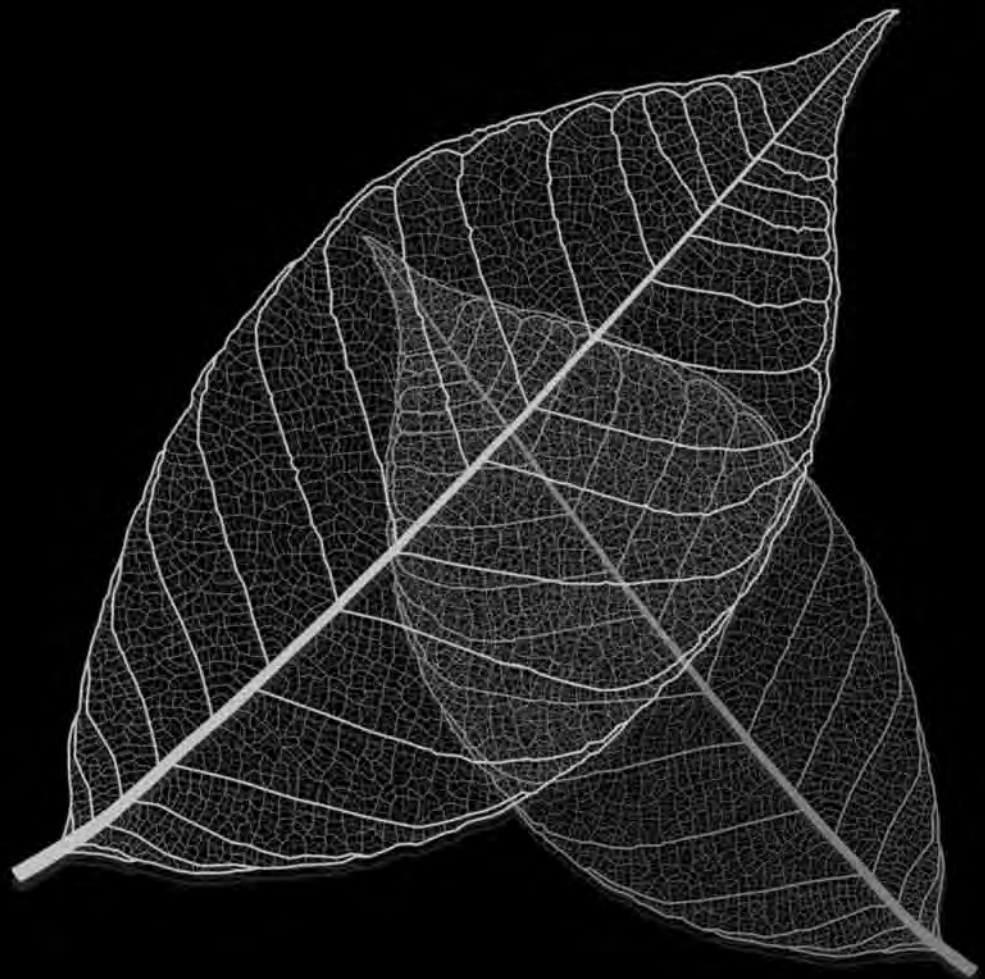
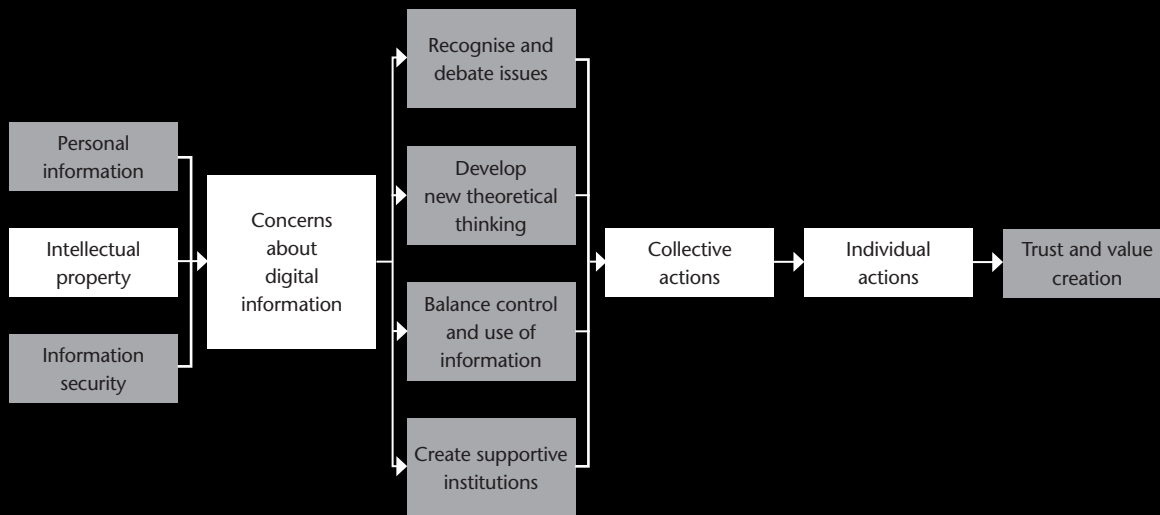
**Businesses are extensively profiling individuals.** While profiling has been a business practice for many years, the sophistication of analytical systems, combined with the vast digital footprint created by most people, is making profiling much more powerful. This can provide benefits by targeting products and services to specific individuals. However, profiling can result in unequal treatment and can offend deeply-held perceptions of fairness. There is often a lack of due process and accountability about decisions. There are also concerns about the long-term impact of filtering information or services to narrow audiences based on this segmentation.

**Governments are connecting information about citizens.** The opportunity to share information more effectively across governments is often essential to increasing the efficiency and quality of public services. However, it raises practical concerns about the quality of information and how it is managed. It also leads to many questions about the degree of governmental power and control gained through centralising personal information.

<sup>45</sup> *The British Computer Society’s Response to the Ministry of Justice on the ‘Data Sharing Review’ by Richard Thomas and Dr Mark Walport*, p2.

# 3. RIGHTS OVER INTELLECTUAL PROPERTY

Rights over intellectual property enable businesses to retain the cash flow benefit from their creative ideas and use of sensitive information. However, innovation and creativity are inherently collaborative and iterative processes. As IT enables ever cheaper sharing of information, how do we balance the need for rights with the opportunities generated by sharing ideas?



# 3. RIGHTS OVER INTELLECTUAL PROPERTY

## 3.1 The business value of intellectual property

To generate revenue, businesses rely on intellectual property and confidential information, which can include inventions, formulae, novel processes, creative content, brand names, designs and customer lists.

Intellectual property is strongly protected in Western legal systems and increasingly demanded of other countries as a pre-condition to participating in international trade. Specific pieces of intellectual property can be legally protected through a variety of means, for example:

- inventions or novel processes can be protected through patents;
- creative content (in the form of literary, artistic, musical and dramatic works, films, broadcasts, communications to the public and software) can be protected as copyright;
- certain databases can be protected in the EU through database rights;
- brand names can be protected as trademarks and designs can be protected as registered designs and design rights; and
- formulae and customer lists can be protected as confidential information, copyright and potentially patentable inventions.

IT raises major challenges for protecting and exploiting intellectual property and commercially sensitive information. However, it also presents significant opportunities for businesses to gain new audiences for creative content, as well as collaborate in innovative and creative activities.

### Economics of information goods

It is well established that the economics of information goods are substantially different to tangible goods. With tangible goods, every item has a cost of production which reflects the physical materials, labour and overhead costs. By contrast, information goods, such as inventions, creative content and customer lists, have a high upfront cost as the information output is created but there is, in theory, no cost attached to copying the pure information once it has been created. Therefore, the cost of the first copy is high but practically zero for subsequent copies.

In practice, the economics of information goods have largely been tempered by physical manifestations, such as paper records, DVDs or books. As a result, there has been a real cost attached to copying information and the economics have been just like any other tangible good.

IT transforms the economics of creative content by turning the dissemination of information into a virtual, rather than a physical, activity. This eliminates many of the cost structures surrounding information goods and indeed brings us closer to the economics of pure information. There are still substantial costs attached to creating the content and running an online infrastructure. However, the marginal cost of copying, storing and disseminating an individual piece of data gets very close to zero.

While this leads to many challenges for business models which have been built on selling individual pieces of content, it also creates new business opportunities. In particular, the changed economics have led to what is termed the 'long tail' effect.<sup>46</sup> By removing the need for physical media such as books or CDs, businesses can maintain a much larger inventory of information goods. This enables a variety of niche content to find a distribution channel, providing consumers with greater choice and leading to further opportunities for innovation.

<sup>46</sup>Chris Anderson, *The Long Tail: Why the Future of Business is Selling Less of More*.

## Reduced costs of information sharing

By massively reducing the costs of sharing information, IT also encourages all kinds of collaboration and joint working between businesses or between businesses and customers. This has particularly been seen along supply chains, as businesses have been able to outsource increasing amounts of work to third party suppliers. It has led to new opportunities to work with partners to create intellectual property. It has also enabled models which bring together employees and customers from all over the world.

Furthermore, IT provides a wide range of opportunities to share creative content with fresh audiences. Encouraging the free flow of information also enables businesses to innovate and create valuable products or services.

## 3.2 Legal considerations

Intellectual property rights aim to secure the cash flow benefits from the exploitation of information resources for the rights-holder. Business will sometimes use intellectual property rights to keep information secret. However, in many cases, intellectual property rights enable a business to sell access to information products and services and keep the related revenue stream.

While intellectual property rights provide exclusive control over information, this control is typically limited in some way, for example rights are not perpetual. Time limits enable the creators and inventors to gain commercial advantage for a particular period and thereby recoup their investment. Thereafter, the content and inventions are opened up for broader use and sharing.

Intellectual property rights can also be limited by the extent to which others can use the information. In some cases, absolutely no use of the information is allowed, whereas in other cases, some use may be tolerated.

### Panel 3.1: UK intellectual property law

Three of the main types of intellectual property rights in the UK are copyright and database right, patents and trademarks.

Copyright protects creative content such as music, movies, books, photographs and software. A database can be protected by copyright if it has been created with originality. Database right is similar to copyright and applies specifically to databases where the creator has invested significant time in its compilation and verification.

In the UK, copyright lasts for the lifetime of the creator plus 70 years. It automatically applies to a wide range of creative content and no registration process is required. Some countries, such as the US, have rules which allow the limited use of copyrighted material without reference to the rights-holder for purposes such as education, criticism, news reporting and research. The UK has more limited exceptions in place.

Patents protect inventions. They provide stronger protection than copyright but are more limited in their application. Periods are shorter, up to 20 years in the UK. Patents also have to be applied for and renewed on an annual basis, making it an expensive process. Once a patent is granted, no-one else can use the invention throughout the period, unless they pay the rights-holder a licence fee. However, the invention has to be published, enabling others to understand what has been done, even if they cannot freely copy it.

Trademarks protect brands or logos which have a commercial value and stop them being imitated or used by other businesses. A counterfeit handbag, which is presented as if it were made by an expensive brand, is an example here. Trademarks also have to be registered in advance and renewed every 10 years. However, there is no prescribed limit to how many times they can be renewed.

The picture is not complete without mentioning confidential information. Trade secrets are based on the protection afforded to confidential information and they are typically defined as confidential information which is secret, substantial and identified.<sup>47</sup>

Trade secrets are important because many pieces of information, such as customer lists, fall into this category. They also provide an alternative approach to patent protection and many small businesses in particular rely on trade secrets rather than investing time and money in registering patents. Furthermore, they enable a business to keep information secret, unlike patent protection. However, they do not provide such strong protection as patents, with recompense for breaches being difficult to achieve in practice.

<sup>47</sup>Michael Risch, 'Why do we have trade secrets?'

## Challenge of enforcing intellectual property rights

It has always been possible to breach intellectual property rights by copying information goods. However, this has been historically limited by the cost and time of the act of physically copying. As a result, while individuals may have engaged in trivial examples of copying for personal use, large-scale breaches, known as piracy, were largely undertaken by criminal gangs for profit.

Changes in technology have fundamentally changed the scale and ease with which individuals can copy material.

- The shift of information from an asset linked to a physical resource to a digital and virtual one has reduced the marginal cost of copying in most cases.
- Improvements in communications technology, such as broadband, have vastly increased the amount of data which can be exchanged and reduced the time it takes.
- New tools and applications have been developed which make the process of copying relatively straightforward.

Large-scale piracy has also been enabled by websites which link people together so that they can share music, video and increasingly books. The explosion of online file sharing, as it is known, can be traced back to the Napster website in the late 1990s.<sup>48</sup> Napster, like subsequent sites such as the Pirate Bay, was ultimately shut down after the courts found it guilty of helping users to infringe copyright rules. However, similar sites continue to exist and many consumers have not been deterred from engaging in illegal file-sharing activities.

## 3.3 Market considerations

The main commercial decision about intellectual property is how it will be turned into cash. In the case of inventions, trade secrets and trademarks, this will be done indirectly through the use of the information in the production and sale of other goods. With creative content, businesses typically look to sell it directly to customers.

### Exploiting creative content

While creative businesses have generally sold their products and services direct to customers, there are a range of business models which use and exploit creative content in different ways.

In an article from 2002, 'Intellectual Property and the Organization of Information Production', Yochai Benkler highlights the wide variety of ways in which information is both an input and an output of a business model. He places businesses models across two different axes.

- **Monetisation strategy:** a business will seek to monetise its content in two broad ways – directly through sales or indirectly through know-how or building reputation. Of course, some organisations or individuals do not intend to monetise their content at all and they develop their content altruistically or purely for pleasure.
- **Production costs:** a business will incur different costs relating to its use of existing content in the production of its information products and services. Where a business owns a large catalogue of creative content, it can reuse it in many ways at no cost. By contrast, a business without any significant catalogue of its own has to pay to access existing content, increasing its production costs.

In moving to the virtual world, many content producers have replicated their business models from the physical world, selling individual pieces of content to consumers. These models are meeting with varying degrees of success, however, and businesses are experimenting with new models which are made possible by the changed economics.

For example, there are growing numbers of business models based on giving away content for free and monetising the value through advertising or other revenue streams. Internet business models tend to rely heavily on advertising to obtain value from content, rather than requiring users to pay for accessing the content. This model is also seen in the music industry, where established artists frequently look to other revenue streams, such as live concerts, merchandising or paid endorsements.

<sup>48</sup>Matthew Green, 'Napster opens Pandora's box: examining how file-sharing services threaten the enforcement of copyright on the internet'.

Some businesses, especially in the music and media industries, are experimenting with subscription models. In these models, content is not bought by a consumer. Instead, an individual consumes content over the network on-demand. Typically, a consumer pays a subscription and has access to limited or unlimited amounts of content for the contracted period.

Alternatively, a business can make most content available free but charge for premium content. Sometimes called a 'freemium' business model, it assumes that consumers will pay for things which they particularly value, even if they will not pay for creative content more broadly.<sup>49</sup> Spotify has built its business model on this basis.

### Panel 3.2: Alternative business models: Spotify

Spotify has been promoted as a new and potentially sustainable way of generating revenue from music content in the digital age.<sup>50</sup> It has been supported by a number of the major music labels in Europe and its business model is markedly different from a traditional music retailer. Instead of selling particular pieces of music, it is based on a user accessing music on-demand through its website.

In order to generate revenue, Spotify allows users to access music in two ways. Firstly, they can access it completely free. However, they have to listen to adverts on a regular basis between their song choices to fund the service. Alternatively, if the user wants to avoid the adverts, they can switch to a subscription model, whereby they pay a fee and have no adverts presented to them.

This is a good example of a freemium model, with a mix of free and premium paid-for options, but whether it generates sustainable value remains to be seen.

## 3.4 Underlying questions about intellectual property

In many cases, intellectual property rights are clear and the business challenges are largely practical in nature. For example, where information is self-evidently important and a business wants to keep it secret, the issues largely concern the effective implementation of information security practices.

However, this clarity can mask deep differences of opinion about the benefits of strong intellectual property rights compared to the benefits that can be obtained from the free flow of information.

The ability to generate new ideas, creative content and culture has been a central feature of human endeavour and development throughout history. There is an inherent tension, though, between the opportunity to build new ideas on what has come before and the desire to control the information which has been created. The limits on intellectual property rights highlighted in this chapter reflect a desire by law-makers to balance these competing interests over information.

As the opportunities to share information for a wide range of social and economic benefits grow, debates touch on some complex underlying questions, including:

- What are the net economic benefits of intellectual property rights?
- What is the moral basis of intellectual property rights?
- What is the impact of changing consumer attitudes to paying for content?
- Are breaches of intellectual property rights morally wrong?

### What are the net economic benefits of intellectual property rights?

Intellectual property has been legally protected in one form or another in Europe since the fifteenth century, and specific rights have evolved to reflect the economic and political needs of the times. The development of the printing press was a major spur to protect books, leading to early copyright protections. In the UK, the growth of manufacturing and trade in the same period led to grants of privilege from the Crown to protect inventions as well as monopolies in trade.

The benefits of strong rights over intellectual property today are largely economic. This reflects the fact that many intellectual property rights are, in practice, held by businesses or commercial intermediaries, such as record companies, rather than the original content creator.

<sup>49</sup>Pascal-Emmanuel Gobry, 'What is the freemium business model?'

<sup>50</sup>Tim Bradshaw, 'Spotify on song with 1m paying subscribers'.

### Panel 3.3: Welfare economics of intellectual property rights

The conventional argument for intellectual property rights centres on the economics of innovation.<sup>51</sup> Information creation, invention and innovation have high upfront costs. An individual or business has to invest substantial time and resources developing the content or idea before any cash can be realised in return. However, the nature of information means that it can easily be copied and therefore appropriated by others.

Intellectual property rights provide protection to information creators and give them confidence that they will be able to reap the financial rewards of their investment. Without these rights, it is argued, competitors could immediately copy the invention or content. Furthermore, as the competitor would not have the investment costs to recoup, it could charge lower prices. As a result, individuals or businesses would be reluctant to make investments in research and development or new creative content. This could lead to an underinvestment in innovation and creativity and intellectual property rights aim to correct this market failure.

Some economists have extended this basic theory to argue for stronger rights over intellectual property. Known as the Property Rights movement, and developed out of the Chicago Business School, this theory argues that the purpose of intellectual property rights is to maximise the economic value of the information good. On this basis, stronger rights should be granted to the creator, which last indefinitely and are not limited by some of the restrictions seen in intellectual property laws today. This approach would make rights more directly comparable to tangible property rights.

Advocates argue that full ownership rights are necessary because, if no-one has exclusive control over a resource, no-one has the incentive to look after it. As a result, the quality of it inevitably degrades over time.

However, the economic benefits of intellectual property rights are not clear cut. Intellectual property rights are fundamentally inefficient in economic terms as they build monopolies over ideas or content. They create a risk of underutilisation of information resources by limiting access to them. Furthermore, since innovation and creativity are inherently iterative, with ideas and content from one person building on ideas from another, strong rights potentially stifle progress and cultural development. Therefore, the long-term benefits of intellectual property can be questioned.<sup>52</sup>

There is limited objective economic evidence about the short and long-term impact of intellectual property rights. The UK Strategic Advisory Board on Intellectual Property Policy (SABIPP)<sup>53</sup> commissioned a detailed survey of economic research in this area in May 2010 and concluded that more research was urgently required.<sup>54</sup> Most economic research to date has concentrated on the short-term losses to rights-holders from intellectual property breaches. However, these losses need to be balanced with any gains to society arising from a greater flow of creative content. It is also important to understand the long-term impact of changing economic incentives and rewards, for example the degree to which information production actually reduces or changes when intellectual property rights are not observed.

### What is the moral basis of intellectual property rights?

Although they have a strong economic basis, there are also moral justifications for intellectual property rights. Creative output can be seen as an extension of an individual's personality, particularly drawing on the ideas of philosopher Immanuel Kant. This leads to claims of natural rights over information which an individual has created, just as an individual has natural rights over personal information about themselves. John Locke argued for natural rights over creative output on the basis that individuals should be able to benefit from the fruit of their labours. If they have invested time and resources in creating ideas and information content, and developed a close identification with it, others should not be able simply to copy it.

However, as with the economic case for intellectual property rights, there are also arguments against the moral case advanced by Locke and Kant.<sup>55</sup> Opponents contend that information

<sup>51</sup> For example, Stanley M. Besen and Leo J. Raskind, 'An introduction to the law and economics of intellectual property'.

<sup>52</sup> For a debate on the property rights theory of intellectual property, see Peter Menell, 'Intellectual property and the Property Rights Movement', and Richard Epstein, 'The Property Rights Movement and intellectual property: a response to Peter Menell'.

<sup>53</sup> This body was merged into the UK Intellectual Property Office in 2010.

<sup>54</sup> Christian Handke, *The Economics of Copyright and Digitisation: A Report on the Literature and the Need for Further Research*.

<sup>55</sup> David Lea, 'From the Wright brothers to Microsoft: issues in the moral grounding of intellectual property'.

and knowledge are public goods and therefore should be shared as widely as possible. Thomas Jefferson is often quoted in this context, in a letter he wrote to Isaac McPherson in 1813:

'That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density in any point, and like the air in which we breathe, move and have our physical being, incapable of confinement or exclusive appropriation. Inventions then cannot, in nature, be a subject of property.'<sup>56</sup>

### What is the impact of changing consumer attitudes to paying for content?

As this chapter has highlighted, moving towards the economics of pure information means that it is substantially cheaper to reproduce information goods. Consequently, the price of information goods becomes more driven by the perceived value of the specific content than the cost of production. However, the extent to which consumers may be prepared to pay for pure content is a question vexing many businesses.

This question is made more complex by the explosion of free content on the internet. This has been provided by amateurs, independent artists and businesses to gain a larger audience for their content. In this environment, it becomes more difficult to charge for information content.

This affects many businesses which rely on creative content to generate revenue and differentiate themselves from others. The newspaper industry is facing particularly severe challenges in competing with free content.

#### Panel 3.4: The newspaper industry and the internet

The newspaper industry has historically relied on a business model which bundles together a range of news, analysis and services based on revenue from advertising and direct sales. The digital world presents two major challenges to this model.

First, it un-bundles these different aspects, which leads to niche competition in each of these areas. Personal adverts, for example, have to compete with a wide range of specialist websites, making it harder to secure readers.

Second, it is competing in a world where news can be gained from multiple sources, many of which give away their content for free. Therefore, the question facing newspapers is: why would consumers pay for news content when they can get the same content elsewhere free?<sup>57</sup>

Instead of charging a subscription, most newspapers have relied on online advertising to generate income in a digital environment. However, this is a challenging revenue model. It is clearly cyclical, with advertising revenue difficult to secure in a recession. The experience of reading an online newspaper is also very different to reading a physical copy. Reading a physical newspaper usually takes place during an individual's leisure time, making it a relatively slow and relaxing experience. By contrast, most viewing of online news takes place during work hours, meaning that it is quick and focused on exactly what the reader wants to know. As a result, online advertising becomes less attractive, as readers are more transitory.

As a result, some newspapers are experimenting with models that either require paid-for subscriptions or mix free and paid-for content. While basic news is ubiquitous, high-quality analysis and comment is not freely available and therefore becomes potentially valuable. On this basis, some newspapers charge for what they deem to be valuable content. This approach appears to have worked for some high-end business publications, which have been able to adopt a range of paid-for models. However, it remains to be seen whether this will apply more broadly, and whether sufficient people will pay to offset the loss of advertising revenue from a smaller readership.

### Are breaches of intellectual property rights morally wrong?

While there are robust debates about the optimum strength of intellectual property rights, few would argue against such rights entirely. As a result, we would expect breaches of intellectual property rights to be seen as morally wrong.

<sup>56</sup>Thomas Jefferson, 'Letter to Isaac McPherson, Monticello, August 13, 1813'.

<sup>57</sup>Knowledge@Wharton, 'Will newspaper readers pay the freight for survival?'

However, it seems that many people, especially the young, do not view activities such as file sharing as wrong. The 2009 report *Copycats? Digital Consumers in the Online Age*, commissioned by SABIPP, confirmed that while there was substantial confusion about what people could do legally and what was illegal, given the amount of legitimate free content on the internet, there could also be a shift in mind-set. In particular, the SABIPP research suggested a strong link between those that engage in illegal downloading and the idea that piracy is a 'victimless crime'.

Content industries argue that when consumers take copies of their content in breach of copyright, this equates to theft. They consider that the amount of material that is copied constitutes lost revenue to them and, given the alleged amount of illegal file sharing that takes place across the world, this potentially amounts to a substantial sum.

In response, it is argued that there is a clear distinction between piracy and physical theft. Downloading a piece of data involves no direct loss for the content company and is quite different to stealing a physical item which had a specific production cost. Furthermore, it can only be equated to a direct loss if the individual would have bought the content but instead chose to access it illegally.

Instead, supporters of this view argue that when consumers find material which they like, however they come by it, they are more likely to purchase it, or similar material, legally. This is supported by research which suggests that those who use online file sharing to access free content are also more likely to purchase content legally.<sup>58</sup>

Hal Varian and Carl Shapiro broaden this point in their book *Information Rules: A Strategic Guide to the Network Economy* (1998), to argue:

'We think the natural tendency is for producers to worry too much about protecting their intellectual property. The important thing is to maximize the value of your intellectual property, not to protect it for the sake of protection. If you lose a little of your property when you sell it or rent it, that's just a cost of doing business, along with depreciation, inventory losses, and obsolescence.'<sup>59</sup>

However, this is a complex area because it is important to recognise that, with digital technology, information is shared by virtue of making a copy of it. This contrasts with the physical world, where it is possible to share books or records with friends or family on a temporary basis. No-one suggested that this was depriving rights-holders of revenue. Indeed, public libraries are based on the idea of many people viewing a single copy of content and sharing content has been seen to enhance our cultural and intellectual world.

Digital technology is different because it does leave the viewer potentially with a permanent copy of the material. However, this does mean that intellectual property rights may operate to a degree that was not originally intended to prevent any kind of sharing.<sup>60</sup>

### Limits of the current framework for intellectual property

In sections 3.5–3.8, we build on the underlying questions asked in this chapter to address some of the most controversial aspect of intellectual property today. At the heart of these is the appropriate balance between exercising strong controls over information and letting it flow freely.

We consider three areas of particular debate which stem from the changes brought by digital technology.

- We need to balance strengthening intellectual property rights with encouraging open approaches and recognise that **there are alternatives to strong rights**.
- The push for transparency means that **there is greater openness in the public and private sectors**.
- Co-creation of intellectual property is happening because **businesses are interacting more with each other and their customers**.

<sup>58</sup>See some of the arguments by Alexandros Stavrakas in 'When piracy isn't theft'.

<sup>59</sup>Hal Varian and Carl Shapiro, *Information Rules: A Strategic Guide to the Network Economy*, p97.

<sup>60</sup>Lawrence Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy*.

## 3.5 Strengthening intellectual property rights

Intellectual property rights have been substantially strengthened in recent years to enable businesses to generate more revenue from their creative content or inventions. However, there are alternative approaches, outlined in section 3.6, which put a greater emphasis on information sharing. Supporters of these approaches argue that businesses should develop business models which embrace the new technological opportunities and the openness that these enable, rather than retain models which are no longer effective in the digital environment.

### Stronger legal rights and enforcement

It is commonly acknowledged that intellectual property laws of all types have grown massively in the past 50 years. The amount of copyright legislation, the length of copyright protection, the number of patents and the breadth of items given trademark or patent protection are all evidence of the growing strength of intellectual property rights.<sup>61</sup> This is generally attributed to the mounting influence of the content-producing industries, such as entertainment, pharmaceuticals and bio-technology. These industries are likely to benefit from stronger protection of rights and have the economic power to push for changes. In addition, the Property Rights movement described earlier has become influential in the US courts and supported a move towards strong intellectual property rights.

This growing strength is reflected in moves to standardise and harmonise intellectual property rights across the world. As with privacy, intellectual property rights spring from a Western legal tradition based on ideas of liberty and the pre-eminence of the individual. However, the adoption and enforcement of intellectual property rights is increasingly becoming a pre-condition to participate fully in world trade, with developing nations required to sign up to a range of intellectual property measures. For example, in order to join the World Trade Organisation, a state also needs to ratify the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). This includes a number of provisions concerning copyright and patent protection.

Furthermore, content providers have emphasised strong enforcement of existing laws. This can be seen in a number of areas, for example:

- actions against individual consumers who have been involved in illegal file-sharing activities; and
- pressure on countries hosting pirate sites to prosecute operators, such as action by Sweden against the Pirate Bay website.

New laws in this area increasingly focus on the role of Internet Service Providers (ISPs) and move some responsibility on to them to detect and report individuals who repeatedly commit copyright breaches.

#### Panel 3.5: The role of the Internet Service Provider

The UK's Digital Economy Act 2010 potentially requires the largest Internet Service Providers (ISPs) to terminate the broadband connections of persistent file sharers after a series of written warnings. This is similar to laws in France, where offenders will be sent warning letters and then made to appear before a judge if they persist in offending.

ISPs are broadly resistant to the idea of greater responsibility as they do not view themselves as policing how individuals use their broadband connections. Postal services have traditionally been recognised as 'common carriers', meaning that they have no responsibility for the content of the post that they collect and distribute. While ISPs can claim to be similarly neutral, there are some differences. In particular, it is possible to spot activities such as file sharing without opening the file. As a result, ISPs can identify possible transgressions more easily and in a less invasive manner than postal service providers.

However, critics argue that there are longer-term implications for using ISPs in this way without having appropriate controls over what information is being checked and how it is being used. Currently, demands for ISP monitoring come from many sources and there would be risks to privacy in particular if monitoring were to become commonplace.<sup>62</sup>

<sup>61</sup>William Landes and Richard Posner, *The Political Economy of Intellectual Property Law*.

<sup>62</sup>Geoff Huston, 'The ISP: the uncommon carrier'.

There is also significant opposition to such strong enforcement measures from consumer groups. They contend that disconnecting broadband connections is wholly disproportionate to the offence committed and may cause unreasonable harm. Many people may use the broadband connection in any single household. Depriving the entire household from having broadband punishes all members by excluding them from many legitimate internet products and services.

There are further practical difficulties. What happens, for example, when an individual downloads content illegally using the wireless connection of a neighbour which is not properly secured? Opponents suggest that it may also stop businesses providing free wireless to customers, in case they use the facilities for illegal file-sharing activities. As a result, opponents argue that laws directed at ISPs could adversely impact on all kinds of innovative activity in the technology sector and beyond.

### 3.6 Encouraging open approaches

An alternative to strengthening property rights is to focus on the benefits of information sharing in terms of creativity, innovation and culture. These ideas are represented in various movements which fall under the broad banner of 'openness' and which are underpinned by a belief that things can be done better when information is shared and made freely available to others. Open movements typically promote alternative licensing schemes which protect content, but in a less restrictive way than traditional copyright licensing.

Indeed, the notion of 'open' is at the heart of the internet, both in terms of its technology platform and its culture, and these movements have largely grown around the internet. This section will consider three distinct 'open' ideas:

- open source software;
- open access; and
- open innovation.

#### Alternative intellectual property regimes

Open movements do not ignore intellectual property rights. Indeed, a great insight of Richard Stallman, the pioneer of the open source software movement, was to use intellectual property rights to ensure that future uses of the software remained free and open. As a result, open movements typically promote alternative licensing schemes which protect content, but in a less restrictive way than traditional copyright licensing. These alternative regimes have been adopted largely by not-for-profit organisations, academics or individual creators, although open source software has gained some traction in a business context.

These alternative regimes are sometimes called 'copyleft' and they have been developed in response to the opportunities presented by digital technology. The use of digital technology makes it easier to share information, update it or mix together different pieces of existing content. However, mainstream copyright protections heavily limit the use of content in this way, making it difficult to maximise the opportunities presented by the technology.

Proponents of more open licensing also cite the enormous growth in copyright protection in recent years. Whereas copyright rules for many years applied in practice to only a small amount of creative outputs, changes in the law have meant that copyright restrictions apply to the vast majority of content posted on the internet. While few would argue against the right of content creators to sell their content, critics argue that the degree of control exercised over content today goes far beyond what was ever originally intended.

Therefore, alternative licencing schemes aim to redress the balance and a well-known example is the Creative Commons.

#### Panel 3.6: The Creative Commons

The Creative Commons is a not-for-profit organisation that develops and promotes licences over creative works which are more open than traditional copyright licences. Within this, there are a range of options for a creator to choose.

- 'Attribution' licences enable others to copy, perform or display the content provided they attribute it to the creator.
- 'Attribution no derivatives' licences enable others to copy, perform or display the work but they cannot change it in anyway.

### Panel 3.6: The Creative Commons (continued)

- 'Attribution non-commercial share alike' licences enable others to copy, perform or display works for non-commercial purposes only. They can also build upon the creation and create something new, although they will have to licence it in the same way as the original work.

Therefore, while they retain some degree of control for a rights-holder, such licences aim to encourage collaboration and innovation. In a summary of the Creative Commons philosophy written in 2005, co-founder Lawrence Lessig, argues:

'We believe that many who make their work available on the Internet are happy to share. Or happy to share for some purposes, if not for others. Or eager that their work be spread broadly, regardless of the underlying rules of copyright. And these people, we thought, could use a simple way to say what their preferences were.... And thus the motivation for CC licenses: A simple way for authors and artists to express the freedoms they want their creativity to carry.'<sup>63</sup>

There are many examples of Creative Commons licences, including Wikipedia. There are also other organisations which have developed alternative copyright systems, such as the GNU General Public Licence for open source software.

### Open source software

The most advanced form of open thinking can be seen in the software world. The idea of open source software dates back to the 1950s although the term was only adopted in the 1990s. Open source software relies on a licensing regime which freely shares the software code among developers. This strongly contrasts with proprietary software where the code is kept secret by the software company.

The open source approach allows others to freely access, test and develop the code but usually requires that any developments are also licensed on an open source basis. Therefore, a developer must license any amendments they make on the same terms as the original code was licensed. This principle of hereditary licensing is central to the rules of the General Public Licence (GPL). Open source software is often developed by programmers on a voluntary basis and available free of charge.

While there are some philosophical arguments concerning freedom of information among open source advocates, they are largely driven by practical considerations. They argue that open source software is better than proprietary software because of the way that it is created. By having many people examine the software, find and correct bugs and add on new pieces of functionality, it should be better and more robust than software which is developed by just a small number of people. There are examples of open source software which have been widely adopted, such as the Firefox web browser and the Linux operating system.

While the notion of open source may seem to go against the interests of commercial bodies, the economics of software can make open source an attractive model for software businesses. Software exhibits the economic feature of network effects, so that it becomes more valuable as more people adopt it. Therefore, in the early stages of software, a business will want to drive adoption, potentially at the expense of earning profits and open source presents a good model for driving widespread adoption. A business can then look for ways to make money from additional functionality or services which they can offer around the basic software. Many commercial businesses may also plug pieces of open source software into their products, thereby avoiding licence fees.

### Open access

Another example of the open ethos is open access, which involves making content freely available to read. Open content goes further and enables others to edit content, for example wiki technology.

Open access has been seen prominently in academic publishing, where academics open up their research for widespread distribution and access. This moves away from the established model of publishing in paid-for journals. Open access journals are usually funded by institutional subsidies or by publication fees, which are paid by the author's institution.

<sup>63</sup>Lawrence Lessig, 'CC in Review: Lawrence Lessig on How it All Began'.

Such an approach makes sense for many academics as they do not sell their research directly. They are rewarded for their research indirectly through universities and other sources of funding. Therefore, they are not financially impacted by the potential reduction in revenue which results from open access. Indeed, sharing the results of their research enables wider distribution, potentially increasing the impact of the research and meeting broader goals relating to the public good and the sharing of knowledge.

Opening up content can be done either by authors publishing their research in an open repository themselves, termed self-archiving, or publishing in an open access journal. In a study by the EC-funded Study of Open Access Publishing in 2010, approximately 10-15% of peer reviewed journals were found to be open access, largely scientific and medical journals.<sup>64</sup>

There has been some academic research on the extent to which open access increases the impact of research. Studies usually look at the number of citations for an article as a proxy for the impact of research and the number of downloads as an indicator of readership. However, the research findings are contradictory. Gunther Eysenbach, for example, found that open access articles were cited more frequently than closed access ones, particularly those published in open access journals.<sup>65</sup> In contrast, Philip Davis et al, in their 2008 article 'Open access publishing, article downloads, and citations: randomised controlled trial', found that while open access articles were downloaded more, there was no increase in citations the first year after publication. They argue that any apparent increase in citations is likely to be caused by other factors, such as article quality.

## Open innovation

In *Open Innovation: The New Imperative for Creating and Profiting from Technology* (2003), Henry Chesbrough defines open innovation as:

'...a paradigm that assumes that firms can and should use external ideas as well as internal ideas, and internal and external paths to market, as the firms look to advance their technology.'<sup>66</sup>

Therefore, the essence of open innovation is sharing ideas and working with partners to create new types of value or new ways of delivering value. This contrasts with a traditional model of research and development based on an internal research function which is protected by high degrees of secrecy.

There has been a long tradition of universities and industry working together to develop new technology, drugs or other inventions. University research and development in areas such as science and technology have underpinned many pharmaceutical and technical advances.

However, it has been driven in recent years by two interrelated factors, according to Bronwyn Hall.<sup>67</sup> Firstly, there is a realisation among even large firms that they cannot produce all the parts of a product or service that a customer needs. Secondly, their products have to work with others in the marketplace and they need to work with other businesses to ensure this.

Strong intellectual property rights may seem to go against the notion of open innovation. However, Hall argues that businesses which have adopted open innovation ideas have also increased the number of patents they have registered.

At the heart of open innovation is the question of how to appropriate value. Claiming rights over intellectual property is clearly a way of doing this. Indeed, clear allocations of intellectual property can be helpful when defining and enforcing contracts. However, there are other ways that businesses can gain value from innovation without using intellectual property rights. For example, products can be bundled together, some of which are protected and some of which are not. A business may also want to share inventions and ideas that they do not plan to develop further themselves. Instead, they may think that others can do more with them, from which they can then benefit.

The complexity of patent strategy is illustrated through litigation activity around mobile phone technology. Many technology companies hold patents over different elements of a smartphone. Therefore, in order to produce a functioning phone, it may be necessary to agree licences with a number of different businesses. Where two businesses have relevant patents, cross-licensing agreements may be made. However, where a business has made extensive use of open source,

<sup>64</sup>SOAP, 'Open Access journals are 10% of journals: findings from the Study of Open Access Publishing (SOAP)'.

<sup>65</sup>Gunther Eysenbach, 'Citation advantage of open access articles'.

<sup>66</sup>Henry Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology*, pxxiv.

<sup>67</sup>Bronwyn Hall, 'Open innovation and intellectual property rights - the two-edged sword'.

it may have few bargaining chips in such a negotiation. This has led to businesses acquiring companies for the purpose of building patent portfolios to fend off litigation and reduce the costs of cross-licensing.<sup>68</sup>

### 3.7 The push for transparency

The push for greater transparency is seen most prominently in the public sector, where the Open Data movement is pushing for the widespread release of government data to drive a variety of economic and social benefits. As technology has improved, pressures have also grown in corporate reporting for more comparable and timely data from businesses. However, while there are great benefits to transparency, it also potentially creates new risks, especially when changes in incentives change the behaviour of individuals.

#### Government information

Most pressures for transparency to date have been felt by the public sector. The Open Data movement encourages the voluntary release of a wide range of data by governments.

#### Panel 3.7: The Open Data movement

The Open Data movement has grown in recent years based on arguments of transparency, accountability and democracy. It aims to get governments to release as much information as possible. This includes all kinds of transactional information, such as budgets, contracts, salaries and services delivered, as well as things like maps, crime locations and transport information. It also wants the data to be released in formats that allow it to be easily reused by others and turned into meaningful information.

Many of the arguments in favour of releasing information are based on principles of democracy and accountability. Supporters go back to Louis Brandeis's well known remark from his 1913 article, 'What publicity can do', to push the notion of transparency – 'sunlight is...the best of disinfectants'.<sup>69</sup> This is a principle that resonates throughout many areas of regulation and is based on the belief that transparency will drive good behaviour and hold people to account in the event of failures.

There are also economic drivers to opening up government data. The reason that supporters want data in a reusable format is to encourage the development of applications that use, aggregate and analyse data. This might lead to new business opportunities and economic growth, as well as engaging ways to present information to individuals to support accountability.

A UK government white paper on the topic, published in August 2011, summarised the benefits in the following way:

'Open Data may be the most powerful lever of 21st century public policy: it can make accountability real for citizens; it can improve outcomes and productivity in key services through informed comparison; it can transform social relationships – empowering individuals and communities; and it can drive dynamic economic growth.'<sup>70</sup>

Few people in democratic countries argue against the virtues of transparency. However, there are some practical concerns about the use of open data. In many cases, the data is raw, raising risks around its accuracy and integrity. There may not be clear data standards or definitions, making it difficult to compare data from different sources. In response to these concerns, supporters of the Open Data movement often point to the notion of crowdsourcing as a way of correcting errors and inconsistencies. As with open source software, they argue that as more people see the data, more errors will be spotted and the data quality will improve.

Another area of concern is the surrounding context of data and its overall meaning. Where data is taken in isolation, it may have little real meaning or its meaning could be misinterpreted. For example, it is likely to be easy to find data about the costs of projects and much harder to find useful data about the benefits that have been realised. However, without both types of data, it is impossible to say whether value has been created.

<sup>68</sup>The Economist, 'Inventive warfare' and 'Patently different'.

<sup>69</sup>Louis Brandeis, 'What publicity can do'.

<sup>70</sup>HM Government, *Making Open Data Real: A Public Consultation*, p10.

### Panel 3.7: The Open Data movement (continued)

There may also be unexpected consequences and behavioural changes from the release of information. While it may be expected that transparency will lead to more responsible behaviour from government officials, they may react in other ways if they know that their actions will be made public. Although a strong advocate for the notion of openness, Lawrence Lessig argues for caution in the rush to release data:

‘We are not thinking critically enough about where and when transparency works, and where and when it may lead to confusion, or to worse. And I fear that the inevitable success of this movement – if pursued alone, without any sensitivity to the full complexity of the idea of perfect openness – will inspire not reform, but disgust. The “naked transparency movement”...is not going to inspire change. It will simply push any faith in our political systems over the cliff’.<sup>71</sup>

While it is markedly different to open data, which is concerned with the lawful release of information by government bodies, the publication by Wikileaks of confidential government information also raises interesting questions. For example, there have been deep differences of opinion on the fundamental morality of publishing such information. Some view it as a major force for information democratisation, enabling individuals to understand the activities, good or bad, of governments. Others view it as irresponsible and highly damaging.

The Wikileaks case also demonstrates the difficulty of defining the limits of information to be published and where a notion of organisational privacy starts. While information published by Wikileaks was unlawfully obtained, and therefore very different to the type of data release advocated by the Open Data movement, it does highlight the degree of political judgement involved in deciding where the line should be drawn and where the benefits of government secrecy outweigh the benefits of transparency and information sharing.

### Business reporting

While open data has largely been a public sector issue to date, there are some broader implications for businesses.

Many companies transact heavily with governments and the push to make contracts more transparent will have effects on these businesses. Indeed, the scope of open data is typically seen to extend to any service funded by public money, whether it is run in the public, private or not-for-profit sector. As a result, information about the size or nature of public sector contracts, which a business may view as highly sensitive, is likely to become public. Businesses working extensively with the public sector may therefore have to consider the implications of such scrutiny.

There are also links to other trends in business reporting towards transparency. Shareholders have always had rights to information through the financial reporting system and the publication of annual reports. The development of XBRL as a technology to tag financial data provides opportunities to get this information to the market quicker and in a more comparable format. The SEC in particular has been a major advocate of XBRL as a means of achieving greater transparency and enabling retail investors in particular to make better decisions about their investments.

To date, digital reporting technologies have been used largely to replicate existing financial reporting, simply changing the technical format in which it is done. However, as the technology continues to improve, and the costs of releasing information reduce, there may be pressures to go further. Level 3 digital reporting, as described in the ICAEW report *Developments in Digital Reporting* (2005), describes the tagging of elements at the transactional level, not simply the consolidated reported figures. While businesses may want to keep such information confidential, it is possible that pressure will grow on businesses to release a wider range of information.

While such information is likely to be of interest to the markets, the greatest pressure may come from governments and regulators. Tax authorities, for example, have been enthusiastic adopters of XBRL, as it gives them data in a more useable format, improves the efficiency of their processes and enables more sophisticated analysis. Such bodies may look to get access to increasing amounts of data, which may again put pressures on the notion of confidential company information.

<sup>71</sup> Lawrence Lessig, ‘Against transparency: the perils of openness in government’, p1.

### 3.8 Co-creation of intellectual property

Businesses are interacting more with each other and their customers. This is resulting in co-creation of intellectual property across supply chains and with customers. While businesses may want to maximise their rights over intellectual property, there may also be new questions about how the benefits of this collaboration are shared and growing perceptions of unfairness where businesses exploit the creativity of others.

#### User-generated content

A major development of Web 2.0 social media technologies has been the growth in content which is generated and posted online by consumers, rather than professional content providers. This includes blogs, photos and videos.

Many of the intellectual property issues to date concerning user-generated content have concerned breaches of copyright by the content creators. By including any clips or extracts of copyright-protected material in the newly-created content, users are likely to be breaching copyright rules. They need to obtain the permission of the rights-holder to use the extract, and this is not always done correctly, opening up the user to legal action for breach of copyright. Some argue that such complex rules, designed to be used by professional content creators, are inappropriate in this new, amateur world. However, rights-holders often enforce their rights strictly and require permission to be granted in every case.

User-generated content also raises new questions concerning who has the right to exploit content which is created and shared in this environment. What kind of rights should the content creator have over it compared to the business which is providing the platform for posting and sharing it? In practice, the rights to exploit the content typically fall to the business providing the platform. While users may retain formal ownership rights, the business is given open-ended rights to use it. Therefore, the business benefits from advertising revenue which may be earned from that particular web page, although of course other commercial arrangements are also possible.

#### Panel 3.8: YouTube copyright requirements

YouTube is one of the largest websites which provides a platform for uploading and sharing videos. It sets out intellectual property rights as follows:<sup>72</sup>

- The user retains ownership. However, he or she must grant YouTube and other service users licenses.
- YouTube is given 'a worldwide, non-exclusive, royalty-free, transferable licence (with right to sub-licence) to use, reproduce, distribute, prepare derivative works of, display, and perform that Content in connection with the provision of the Service...'
- Services users are given 'a worldwide, non-exclusive, royalty-free licence to access your Content through the Service, and to use, reproduce, distribute, prepare derivative works of, display and perform such Content'.

Content providers also have to mark their work with a Creative Commons licence, which enables others to reuse the content provided that they attribute it to the original creator.

#### Co-creating value

The traditional idea of a value chain is based around a business creating a valuable product or service for a customer, which a customer then buys and uses. This creates a clear separation between 'producer' and 'user'.

While the distinction has never been absolute, new technology increases the opportunities to work together and collaborate in the creation of value. In their article 'Co-creating unique value with customers' (2004), C.K. Prahalad and Venkat Ramaswamy describe value co-creation with customers in the following way:

'It begins by recognising that the role of the consumer has changed from isolated to connected, from unaware to informed, from passive to active.'<sup>73</sup>

<sup>72</sup>See [www.youtube.com/t/terms](http://www.youtube.com/t/terms).

<sup>73</sup>C.K. Prahalad and Venkat Ranaswamy, 'Co-creating unique value with customers', p4.

As a result, co-creation creates an experience which is personalised and based on the specific needs of a customer. Building this more personal relationship with the customer potentially leads to a greater degree of customer loyalty and a higher-value relationship. By passing activities to the customer, a business may also be able to see reductions in its own costs.

There are many different ways that the idea of co-creation can be realised in practice. At its simplest, a business can set up communities of customers to elicit suggestions and feedback around products and services or help each other with common queries. Customers can also be used in marketing activities. This has been seen in the growth in 'viral' marketing, whereby buzz is created by individuals circulating material promoting a product or service without the business being directly involved. Although risky, it can garner great publicity and potentially be more effective than traditional business-led marketing.

However, ideas of co-creation go beyond feedback and marketing, as shown by the Crushpad example.

### Panel 3.9: Crushpad business model

This Californian-based business specialises in wine production. However, its value proposition is totally personalised for each customer and the degree to which they want to be involved in the production of a barrel of their own wine.

Customers develop a plan for their wine based on the grapes of their choice in consultation with Crushpad experts. The grapes are then grown with the customer able to stay in touch via occasional videos and online updates. Once the grapes are ready, the customer can become involved in the physical process of winemaking, for example sorting and crushing the grapes. As the wine ages, customers can taste it and decide about the blends. Samples can be sent if needed. Finally, the customer can design a label for their bottles.

As a result, the customer and business interact throughout the process, making it a unique experience for the individual.

This kind of interaction demonstrates some of the possibilities of blurring the lines between businesses and customers.

While presenting new opportunities, these changes potentially raise questions around the appropriation of benefits between parties. Where a customer has been involved in the co-creation of content or new products and services, there may be growing questions about who has the right to appropriate its profits. Customers may increasingly demand mechanisms for sharing any benefits which are derived from their endeavours.

## 3.9 Summary

To generate revenue, businesses rely on intellectual property and confidential information which can include inventions, formulae, novel processes, creative content, brand names, designs and customer lists.

Intellectual property rights aim to secure the cash flow benefits from the exploitation of information resources for the rights-holder. Business will sometimes use intellectual property rights to keep information secret. However, in many cases, intellectual property rights enable a business to sell access to information products and services and keep the related revenue stream.

In many cases, intellectual property rights are clear and the related business challenges are largely practical in nature. However, this clarity can mask deep differences of opinion about the benefits of strong intellectual property rights compared to the benefits that can be obtained from the free flow of information.

As the opportunities to share information for a wide range of social and economic benefits grow, debates touch on complex underlying questions, including:

- What are the net economic benefits of intellectual property rights?
- What is the moral basis of intellectual property rights?
- What is the impact of changing consumer attitudes to paying for content?
- Are breaches of intellectual property rights morally wrong?

We consider three areas of particular debate which stem from the changes brought by digital technology.

**There are alternatives to strong rights.** Intellectual property rights have been substantially strengthened in recent years to enable businesses to generate more revenue from their information content or inventions. However, there are alternative approaches which put a greater emphasis on information sharing. Supporters of these approaches argue that businesses should develop business models which embrace the new technological opportunities and the openness that these enable, rather than retain models which are no longer effective in the digital environment.

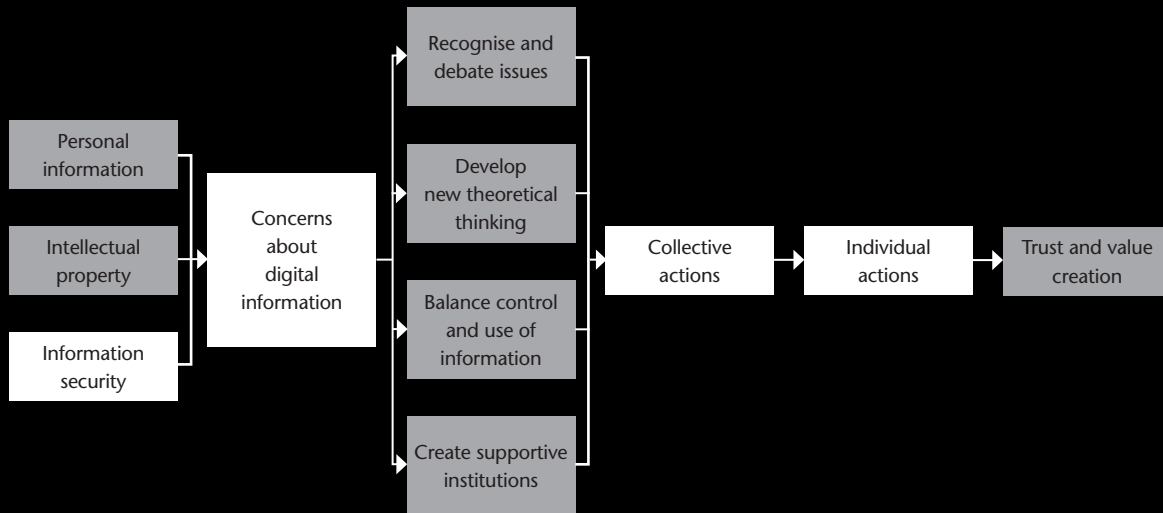
**There is greater openness in the public and private sectors.** The push for transparency is seen most prominently in the public sector, where the Open Data movement is pushing for the widespread release of government data to drive a variety of economic and social benefits. As technology has improved, pressures have also grown in corporate reporting for more comparable and timely data from businesses. However, while there are great benefits to transparency, it also potentially creates new risks, especially when changes in incentives change the behaviour of individuals.

**Businesses are interacting more with each other and their customers.** This is resulting in co-creation of intellectual property across supply chains and with customers. While businesses may want to maximise their rights over intellectual property, there also may be new questions about how the benefits of this collaboration are shared and growing perceptions of unfairness where businesses exploit the creativity of others.



# 4. INFORMATION SECURITY PRACTICES

Good practices, especially in information security, are needed to underpin trust and value creation from digital information for individual businesses. How do new trends in IT change the risks facing businesses? And how can individual businesses improve their implementation of practices?



# 4. INFORMATION SECURITY PRACTICES

## 4.1 Principles of information security

In many cases, information rights are well established and clear. Therefore, the business imperative is to secure those rights effectively.<sup>74</sup> The field of information security deals with the protection of valuable and/or sensitive information and is built around three key principles:

- confidentiality;
- integrity; and
- availability.

The principle of confidentiality protects information from data breaches which occur when information is accessed by, or disseminated to, unauthorised parties. Breaches occur for example when criminals hack into systems or access them using the stolen details of individuals. Many data breaches are also caused by employees. This could be through malicious activities, where employees sell confidential information to competitors or criminals. Alternatively, it could be caused by careless activities or omissions by employees, where they lose sensitive information, for example misplacing a laptop which contains customer information.

The second principle is integrity. Information is often relied upon in decision making and needs to be accurate and complete. Consequently, it may need to be protected from interference or damage. Financial information is particularly important for a business and there needs to be sufficient security in place so that stakeholders have confidence in the accuracy of that information.

Finally, the principle of availability ensures that users have access to information when they need it. Therefore, it protects information from permanent or temporary loss. This could result from, for example, natural disaster, technical or human error or sabotage.

These principles are well established and information security practices have been present throughout history. Codes, for example, date back to Roman times, if not earlier, and protect the confidentiality of information by limiting access to those who know the appropriate code.

### Identity and authentication

Confidentiality, integrity and availability are underpinned by notions of identity. Authentication techniques validate whether people are who they say they are.

#### Panel 4.1: Types of authentication

There are three established ways of authenticating a person's identity:

- through something they possess, such as a bank card, access token or formal document like a passport;
- through something they know, for example mother's maiden name; and
- through a personal characteristic, which is primarily a biometric factor such as a finger print or iris identification.

Passwords are the most common form of identity authentication for IT systems. These are simple to use and administer. However, they are not a strong form of authentication and can usually be broken quite easily through sheer brute force of trial and error character combinations. Passwords may also be guessed with a little knowledge of the individual user, where they have used family or pet names, for example, or common words such as 'password'.

<sup>74</sup>Relevant ICAEW publications include *Glossary of IT Security Terms 2011*, *Dealing with Internet Security Threats and Information Security Myths and Realities Revisited 2011*.

#### Panel 4.1: Types of authentication (continued)

Passwords can be strengthened by lengthening them or including more complicated combinations of numbers, letters or other characters. Users can also be required to change them on a regular basis to reduce the impact if a password is compromised.

However, creating stronger passwords can lead to different problems. As users typically find it difficult to remember long, complicated passwords, they often write them down. This creates a new risk of the password being seen and used by someone else.

Another way of strengthening authentication is combine two or more factors, known as two or three-factor authentication. For example, to access funds in a bank account, an individual needs to have a bank card (something they possess) and use a PIN (something they know). Many businesses use access tokens as well as passwords when employees log into systems.

New developments in this area investigate the use of pictures and longer passphrases, which individuals may find easier to remember, as well as greater use of biometrics as alternative forms of authentication.

## 4.2 Established information security practices

The principles of information security are reflected in a wide range of established information security practices. Business processes and management techniques are a central part of any information security strategy. Given the dominance of IT, technical computer security is also a very important component of information security. While regulation has not historically featured heavily in this area, regulatory pressures are growing as the profile of information security failures increases.

### Management practices and processes

A variety of measures are needed to deliver effective and efficient information security.

Risk management processes are central to management thinking on information security. A business will have to prioritise between different security measures, based on the resources available to it and its specific risks. Therefore, risk management underpins a successful and proportionate security regime and is also the foundation of the more specific management practices and methodologies outlined in this section.

Information security good practices are reflected most comprehensively in the management system standard ISO 27001.<sup>75</sup> This is an international standard that was originally developed in the UK by the British Standards Institute, based on a Code of Practice from the Department of Trade and Industry. While adoption remains voluntary, public bodies and large businesses are increasingly demanding that their suppliers adhere to the standard.

#### Panel 4.2: Security standards: ISO 27001/2 key provisions

ISO 27001 is a management system standard which provides a specification for implementing an information security management system within an organisation. This is complemented by ISO 27002, which provides a comprehensive list of possible security controls and is reflected in Annex A of ISO 27001.

In order to comply with the standard, management needs to follow a set of procedures which will ensure that proper management of information security, as appropriate to the organisation, is taking place. There is a requirement to identify important information assets within a defined scope, including their importance from the differing perspectives of confidentiality, integrity and availability. A risk assessment must be undertaken, although the methodology is not prescribed, and management has to demonstrate how it is managing the identified risks. Finally, management has to confirm that the controls detailed in Annex A have been considered for their applicability, together with any additional controls specific to the organisation. An on-going set of processes for management review, audit, documentation, training awareness and incident management is also required.

<sup>75</sup>ICAEW, *Information Security – An Essential Today, a Guide to ISO/IEC 27001 and ISO/IEC 27002 for Business Managers*.

## Panel 4.2: Security standards: ISO 27001/2 key provisions (continued)

The controls in Annex A are grouped into 11 areas:

- security policy;
- organisation of information security;
- asset management;
- human resources security;
- physical and environmental security;
- communications and operations management;
- access control;
- information systems acquisition, development and maintenance;
- information security incident management;
- business continuity management; and
- compliance.

The provisions of ISO 27001/2 are incorporated into the IT Infrastructure Library (ITIL), which is a set of good practices regarding the management of IT operations and services.

There is also a body of work that has grown up in the context of financial statement audit and assurance. The reliability of financial information is extremely important to the users of that information. As the storage and processing of financial information moved from physical ledgers to computer systems, questions grew about the controls in place to ensure the integrity, confidentiality and availability of information in this new environment.

As a result, the accounting profession was instrumental in developing new thinking and practices concerning IT risks. The controls and processes which were developed are now reflected in Control Objectives for Information and related Technology (COBIT), which was first published in 1996 by the Information Systems Audit and Control Association (ISACA) and COBIT is widely used in IT audit activities. COBIT contains a wide range of measures, processes and controls over the management of IT systems and the creation of value through IT. Although overlapping with ISO 27001/2, it is a broader set of measures, with information security just one component part.

Information security practices are also likely to be supported by an information security policy. Such a policy should outline business decisions and the rules and practices to be followed in a specific area. Information security policies commonly include matters such as:

- responsibility and accountability for security matters;
- employee use of the internet or computing resources for personal purposes; and
- the creation, management and deletion of user IDs to allow access to systems.

### Computer and IT security measures

Computer and IT security is also an important part of information security today. The early computers, developed in the Second World War, were built as standalone machines, with no connections to other machines. This isolation helped to maintain security and specific measures addressed physical and environment threats such as theft, espionage or fire.

These original risks still remain and physical and environmental security continues to have an important role to play. In addition, computers have moved into the business and consumer domain, making the environment ever more open. As a result, the risk of security failures has grown and IT security has constantly evolved to respond to new threats. This has led to a patchwork of measures in devices and hardware, operating systems, networks and individual applications, including:

- technology to monitor systems and identify where and when breaches occur;
- technologies such as virus protection and firewalls to keep malign influences out of systems;
- technology to protect the integrity and authenticity of communications, such as encryption and network security; and
- technology to verify identity such as passwords, tokens and biometric information.

Security is an important aspect of how IT systems are built and businesses should include security considerations in the early stages of commissioning systems to make them secure by design, as far as possible. A business may also want to manage its risks broadly and minimise the impact of security breaches. For example, data can be stored across a number of different systems so that unauthorised access into a single system has less impact. It can implement processes which regularly monitor systems for intrusion attempts and breaches.

Furthermore, the impact of technical security measures is often to restrict what a user can do. Indeed, users may bypass controls which they perceive to be unjustified and a hindrance to their job. Therefore, any security strategy needs to balance security with functionality.

However, there will always be a degree of risk through using networked IT systems. A computer security expert may argue that the only way to be truly secure is to unplug a computer from the internet and shut down all network connections. In order to do business, though, this is not realistic in most cases. A business can restrict what individual users can do on the internet through a range of technical controls and management policies. However, a business becomes subject to some security risks in return for connecting computers to a wider network and gaining access to the potential benefits that this offers.

As with other areas of risk management, a business can choose to mitigate risks, through adopting appropriate security measures, or simply accept them. It can also outsource security measures to specialist suppliers, although it will not be able to transfer the risks fully.

## The role of regulation

To date, information security has been left primarily to the discretion of individual businesses and approached as an internal risk management decision rather than as the subject of regulation.

Nevertheless, there is some targeted legislation in place regarding information security. For example, data protection laws in Europe include legal duties to prevent the unauthorised access of personal information. These duties are more stringent and rights more extensive in the case of 'sensitive personal data', such as religious beliefs, race and sexual orientation. Data subjects also have the right to correct information which is held about them. Fines can be levied where these duties are breached.

The US Sarbanes-Oxley Act of 2002, which applies to all businesses registered on a US stock exchange, requires senior management to confirm that appropriate controls are in place regarding financial information, including IT controls. For companies that have to comply with these requirements, anecdotal evidence suggests that there has been an improvement to the IT controls and security in place, although that has been at a significant cost to businesses.<sup>76</sup>

A growing area of regulation is data breach notification laws. These started in California in 2003 and have subsequently been replicated in many US states. The EU also adopted a directive in 2009 applying a data breach notification law to telecommunications companies<sup>77</sup> and a revision of the data protection rules in Europe may incorporate a broader breach notification requirement.

### Panel 4.3: Breach notification laws

Breach notification laws require the disclosure of information security breaches to nominated public bodies and / or subjects whose information has been compromised. They apply primarily in the context of personal information.

There are various objectives for these laws. By forcing a business to disclose breaches to customers whose information has been accessed by unauthorised parties, breach notification laws enable affected individuals to take extra care, for example checking statements about financial affairs more closely.

Notification may also improve information security at a macro level through openly sharing accurate information on what is happening with regard to security threats and breaches. Currently, there is little objective evidence around the incidence of security breaches. Most of it emanates from the IT security industry itself and greater transparency of data breaches could help research on security.

<sup>76</sup> Compare the views in these articles – Jeremy Grant, 'Financial chiefs hit out at Sarbox costs' and Thomas J. Healey, 'Sarbox was the right medicine'.

<sup>77</sup> EU Directive on Privacy and Electronic Commerce 2002/58/EC, amended in 2009.

### Panel 4.3: Breach notification laws (continued)

It is also argued that such laws encourage businesses to adopt good security practices and discourage poor practices. Because data breaches are publicised, businesses may be more committed to implementing good security measures and avoiding bad publicity as far as possible.

Data breach notification laws are not without controversy. It is not necessarily clear what should be disclosed, when it should be disclosed and what really constitutes a data breach. Furthermore, businesses are reluctant to share potentially damaging information where they believe it will be made public. However, such behaviour undermines the broader goals of the legislation. Therefore, regulators need to balance the desire to deter poor practice through widespread publicity of failures, with the desire for businesses to share information about threats and breaches, thereby improving understanding of the wider environment.

The evidence regarding the success of breach notification laws has been mixed. However, the pressure for such laws is likely to increase as the profile and impact of breaches grows.

There are also examples of industry standards which have been widely adopted. PCI DSS, for example, has to be complied with by any business which holds payment card data.

### Panel 4.4: Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an information security standard that must be followed by any business that stores, processes or transmits payment card data.<sup>78</sup> This is a single standard that applies across all of the major card providers and replaces a variety of standards that individual card providers previously had in place.

The standard contains 12 requirements regarding information and IT security, including maintaining a secure network, encrypting data when it is transmitted over public networks and restricting access to card data.

Compliance must be verified annually through a combination of independent audit, third party vulnerability scanning or self-assessment, depending upon how the organisation is classified. Organisations either pass or fail the validation process. There is a regime of financial penalties in the event of non-compliance which can result in multi-million pound fines.

## Management challenges

Despite the existence of a wide range of good practices, many businesses struggle to implement effective information security. One reason for continuing security failures is that it is often difficult to connect security measures to business priorities and thereby gain sufficient management and employee attention.<sup>79</sup>

Information security practices and policies are likely to be most effective when they are clearly aligned with business objectives and have strong executive support. In these circumstances:

- practices are more likely get employee focus and attention;
- management are likely to make better decisions about security and focus resources on the areas of greatest need; and
- it is more likely that a business will move past a 'tick box' mentality and apply specific practices more meaningfully.

In sections 4.3 to 4.6, we identify four particular management challenges which relate to understanding the business risks around security failures and enhancing the security capabilities of an organisation:

- making decisions about security measures;
- building skills and organisational structures for security;
- embedding good practices throughout the business; and
- securing information beyond business boundaries.

<sup>78</sup>For an overview of PCI DSS requirements, see Dick Price, 'What is PCI DSS and who needs to know?'

<sup>79</sup>Gurpreet Dhillon and Gholamreza Torkzadeh consider some of the objectives for information security in their article 'Value-focused assessment of information system security in organizations'.

## 4.3 Making decisions about security measures

It can be difficult to make good decisions about information security investments. Good practice suggests that management should assess the risks surrounding information and balance the costs of security measures against the possible impact of security failures. However, the difficulty of quantifying these matters limits the effectiveness of structured decision-making processes in practice.

### Traditional decision models

Management frequently find it difficult to make good decisions about information security investments and spending. Indeed, traditional decision models have often been based on 'FUD', or fear, uncertainty and doubt.<sup>80</sup> Alternatively, security functions may be given a fixed amount to spend however they see fit, with little other financial discipline or oversight. In these cases, benchmarking figures such as the percentage of IT budget which is spent on IT security become important prompts for decision making.

Without a structured approach to decisions, businesses could be under or overspending on security measures. Furthermore, even if the overall security budget is in line with industry averages, this provides no guidance on whether resources are being spent wisely or prioritised appropriately. As the risks to information security grow and businesses are subject to an increasing number of attacks, the impact of poor decisions in this area will also increase.

### Quantifying security risks and benefits

There are economic models that a business can adopt to support decision making in this area. These models focus on a cost / benefit approach and aim to compare the benefits of implementing security measures with their costs. This is similar to standard investment techniques such as Return on Investment, which is translated into Return on Security Investment (ROSI). The basic calculation is shown below.

$$\text{ROSI} = \frac{(\text{Risk Exposure} \times \% \text{ Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}$$

However, ROSI is more challenging than standard investment techniques to apply because of the uncertainty of the variables. For example, it is difficult to accurately predict the likelihood of breaches occurring. Although understanding of breaches has improved in recent years, the range of threats and vulnerabilities around information makes it particularly difficult to predict breaches.

The potential loss is also highly variable depending on the exact nature of the breach and the information compromised. Losses could include:

- direct loss from the theft of intellectual property or the levying of fines regarding the loss of personal data;
- time and resources to investigate the breach and fix failures;
- time and resources to inform customers or other authorities of data breaches and manage any immediate reputational damage; and
- long-term damage to reputation and brand because of the incident.

Research by Lawrence Gordon and Martin Loeb further highlights the difficulty of security investment.<sup>81</sup> This research suggests that there is an optimal amount of investment on information security. Therefore, even where individual measures appear to be justified, they may make no overall difference to a business. As a result, quantifying the costs and benefits of information security measures is likely to remain challenging.

### Valuing digital assets

To support a more structured approach to security investment decisions, businesses can focus their security resources on the areas of greatest need. This involves building an inventory of digital information assets and then establishing which are the most sensitive and valuable pieces of information.

<sup>80</sup>Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan, 'A model for evaluating IT security investments'.

<sup>81</sup>Lawrence A. Gordon and Martin P. Loeb, 'Return on information security investments: myths vs. reality'.

Like ROSI calculations, this is difficult to do in practice. Many businesses may have only a limited understanding of all the information that they possess and may have to undertake significant work to firm this up. Valuing information is also likely to be quite arbitrary. Indeed, information that appears to be fairly worthless when gathered can gain great sensitivity or value when used in a different context. However, a business is likely to be able to improve its decisions about security where it can build up deeper understanding of its information assets and their relative importance.

## 4.4 Building skills and organisational structures for security

While many information security measures are technical, a business is also likely to benefit from techniques which integrate security skills and knowledge across technical and business functions.

It is commonly acknowledged that IT projects generate higher returns when they effectively combine the technical skills of the IT department with the business knowledge and experience of other parts of the organisation. This helps to deliver technical solutions which meet real business needs. It enables accountability to be shared across the organisation and sit where it is most appropriate. It also builds common understanding around the goals of IT projects, thereby increasing alignment and commitment.

Following on from this, information security also benefits from techniques which integrate skills and knowledge across technical and business functions. These techniques can support good practices. They may also support the spread of accountability throughout the business for a range of security measures, many of which are rooted in business processes rather than being technical IT measures.

### Governance techniques

Information security has historically been seen as a specialist area which has attracted little attention from wider business functions. This specialisation has been emphasised by the fact that responsibility for information security has often sat in IT departments. However, the perception of security as a technical topic increases the challenge of linking security practices and policies with business objectives.

Information governance is a set of management practices which aims to protect the quality and control of information throughout the organisation and integrate accountability accordingly. It is often associated with the notion of stewardship and typically allocates responsibility or ownership of data to particular individuals. This potentially helps a business to increase accountability for the use and management of information.

There are a variety of different flavours of governance in this context. The term 'data governance' is strongly associated with the implementation and exploitation of large Enterprise Resource Planning (ERP) systems. It focuses on the quality, security and definition of data. 'Information governance', in contrast, has been developed particularly in the context of medical records and focuses on the effective, secure and legal use of sensitive health information. 'Information security governance' is another specialist term.

#### Panel 4.5: Information security governance

The IT Governance Institute, which is the research arm of ISACA, outlines one approach to sharing major responsibilities over security at a senior level, including the board, senior executives, a security steering committee and the chief information security officer. Their publication *Information Security Governance: Guidance for Boards of Directors and Executive Managers* (2006) highlights responsibility over six areas:

- the strategic alignment between the business and information security;
- risk management;
- value delivery and the efficient implementation of information security;
- performance measurement;
- resource management and sharing information security knowledge across the business; and
- integration across functions to ensure security policies and measures are understood and applied.

## Skills of information security leaders

Identifying a leader of information security is often seen as central to integrating security across a business. Many businesses may place this responsibility on IT managers but the new role of Chief Information Security Officer (CISO) is of growing importance, especially in larger businesses.

It might be expected that such a role would have an increasing focus on business knowledge and stakeholder management in order to improve communication and build common understanding of security goals and measures. This would parallel a more general move in IT leaders, where deep technical skills are often seen as of lesser importance and IT leaders increasingly focus on understanding the business and communicating with senior management.

A 2010 survey by Marilu Goodyear et al, *Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers*, reports that CISOs believed their most important skills were communication skills, policy development and political skills. While the role is still in its early stages and evolving, it would therefore appear that it is a more business-orientated role. This is supported by the fact that CISOs may not report to the IT function and may not even come from an IT background.

## 4.5 Embedding good practices throughout the business

Historically, information security was primarily concerned with physical controls. Information was held on paper and security was designed to protect physical media. Even in the early days of computers, security measures focused on physical access to the computer room and fire detection and prevention. However, while remaining stored in increasingly large databases housed in mainframe computers, information has also become increasingly available to users on desktops and laptops and is easily transferable to mobile devices. These changes fundamentally increase the risks of information security failures.

For example, large amounts of information can be held on small devices and transferred on the basis of an email and a few key strokes. As a result, data breaches can involve very large numbers of data records. Furthermore, breaches do not necessarily require malice to occur. Behaviour that is just a little careless can also lead to significant damage.

Responsibility for information security is now dispersed far beyond a few technical specialists into the wider organisation. IT has enabled information to be more dispersed, putting greater emphasis on individual behaviour and making it more important to embed good security practices. Many data breaches are caused, in practice, by individuals losing or abusing sensitive information they have on computers and mobile devices. This calls for a different mind-set, with every individual taking more responsibility for behaving securely and following basic procedures.

As a result, finding ways to encourage and embed good security behaviour throughout an organisation is increasingly important. Furthermore, as employees increasingly use consumer devices, and frequently their own personal devices, to store or access corporate data, embedding good behaviour will become even more important.

### Panel 4.6: The consumerisation of IT

The 'consumerisation of IT' refers to employees' growing familiarity with technology and the impact that this has on a traditional corporate IT department. As individuals increasingly use computers and mobile devices in their personal lives, they are demanding similar freedoms and flexibility in their work-related technology. Indeed, in many cases, employees use their own smartphones, tablets or laptops for work using a variety of communications technologies. They may make extensive use of web-based or mobile applications, as well as social media sites.

In these cases, an IT department is likely to face significant resistance to tight controls over what employees can do with their equipment. As a result, there is like to be even greater reliance on employees' understanding of the risks and their ability and willingness to take the appropriate steps to protect corporate data and communications.

## Raising employee awareness

Training can help raise employee awareness of security policies and processes.

Most businesses have basic security policies and processes in place which facilitate consistent good practice. These could include the processes and authorisations required to set up new user identities (IDs), change profiles or delete IDs once staff have left. They could also include broader staff policies, such as the use of the internet for personal use, prohibitions on downloading non-official software, using memory sticks, maintaining clean desks and using confidential bins for sensitive wastepaper. Businesses may also look to develop policies around the use of social media or smartphones and tablets.

In order to bring these policies to life, businesses need to train employees in information security. Security policies are included in many induction programmes for new employees.

Measures are also often included in individual performance agreements requiring adherence to standards and performance requirements. Internal audits can be a useful way of identifying whether processes and procedures are being followed. And ultimately, holding individuals to account in the event of serious failures sends an important message to the business.

## Culture and leadership

Culture and senior-level commitment are also important factors and where security can be aligned with the objectives and brand of the business, it is more likely to become central to business activities.

By contrast, the impact of failures in leadership is highlighted by the case of the HMRC data loss, where insufficient management focus led to good practices not being followed by staff.

### Panel 4.7: HMRC data loss

A particularly high-profile data breach took place in the UK government agency Her Majesty's Revenue and Customs (HMRC) in 2007. In the course of audit activities, the National Audit Office requested HMRC to send it records relating to 25 million state benefit recipients. Junior staff put a copy of a range of all the data, including identity and bank details, onto two CDs. They proceeded to send them through the internal mail, with no record, and then via a courier. The disks did not arrive and were not subsequently found.

A report on the incident and the wider issues of data handling in HMRC found that the incident itself was caused by a series of errors and poor communication, such as the failure to redact personal information and to get authorisation for transferring such a large amount of data offsite.

However, it concluded that the failure could ultimately be traced back to the broader policies and culture of the organisation, stating that 'information security simply wasn't a management priority as it should have been.'<sup>82</sup>

A wide range of institutional factors which had led to the incident were cited to justify this conclusion, for example:

- information security policy was not well communicated;
- there was insufficient training and awareness of policies and procedures; and
- there was a lack of accountability regarding information.

## 4.6 Securing information beyond business boundaries

A growing security challenge concerns the explosion in outsourcing and collaboration across supply chains. As a result, information rarely sits in one organisation as a static resource but instead is the subject of continual flows between different parties. This may lead to a shift in security thinking, away from establishing a secure perimeter around the organisation to a more dynamic model which emphasises security across a supply chain.

For example, information is likely to be held by a range of suppliers, not simply within the business itself. This complicates the information security process because the business is now dependent on multiple parties to protect information. A business can outsource the

<sup>82</sup>Kieran Poynter, *Review of Information Security at HM Revenue and Customs: Final Report*, p3.

implementation of information security policies and procedures but it cannot outsource responsibility for information security. Indeed, in the event of breaches, the business will continue to be held responsible for failures, rather than the outsourcing service provider. As service models evolve, businesses need to retain an active interest in the security practices of their suppliers.

Things are likely to get more complex as IT itself gets increasingly outsourced and managed through shared infrastructure services such as the 'cloud'.

#### **Panel 4.8: Cloud computing**

Cloud computing is a delivery model by which businesses access their systems over the internet, enabling access wherever and whenever they want. They share the infrastructure with other customers and may also share applications, depending on the model adopted. Therefore, instead of a business owning its own hardware and software, it accesses IT systems as if they were a service, typically paying on the basis of use.<sup>83</sup>

The cloud model is one that generates great interest and excitement from the technology sector. By enabling substantial economies of scale, it should reduce the cost of IT services significantly and provide scalability as well as flexibility for customers.

However, it takes data far beyond the boundaries of an individual business and indeed, it may not be at all clear where the data is physically or who is the supplier at the end of the chain. This clearly raises new issues around the security of information and how customers can gain sufficient comfort from cloud suppliers around their security processes and procedures. Suppliers often argue that the security within a cloud environment can be substantially better than in an individual business, especially a small business which may lack specialist skills. However, security concerns remain a significant barrier to the adoption of cloud delivery models in the short term.

### **Information security by contract**

One important element of good practice is for businesses to specify requirements regarding information security in their contracts with third parties. A business could require compliance with a standard such as ISO 27001, so as to have confidence that the supplier follows standard information security management processes. This approach is becoming increasingly common with government and large business contracts and is the biggest reason for such standards being adopted in practice.<sup>84</sup>

This trend has led some commentators to contend that, while underlying technical principles, standards and processes will continue to be specified by contracts, information security for many businesses is increasingly going to become a legal as well as a technical topic.

Typically, it is hard for small businesses to specify security standards or conditions in contracts and they are likely to have to rely on standard terms and conditions in supplier contracts. This creates new risks related to reliance on suppliers.

### **Assurance standards**

Supporting contractual requirements is the ability of a business to gain comfort through audit and assurance processes that their data is being protected adequately.

#### **Panel 4.9: Gaining comfort over service providers**

There are a number of standards that can be followed to gain comfort over the information security practices of a supplier.

The American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No.16, Reporting on Controls at a Service Organisation (SSAE 16) was released in 2011. This replaced the AICPA's Statement on Auditing Standards No. 70 (SAS 70) which was a widely recognised standard to gain assurance over the internal controls of service providers. The update to the standard reflects the changing environment for service providers, including factors such as the globalisation of businesses and a more complex regulatory environment.

<sup>83</sup>ICAEW, *Cloud Computing: A Guide for Business Managers*.

<sup>84</sup>InfoSecurity Europe and PwC, *Information Security Breaches Survey 2010*.

#### Panel 4.9: Gaining comfort over service providers (continued)

ICAEW also has technical guidance in this area.<sup>85</sup> AAF 01/06 and ITF 01/07 suggest a series of control objectives to be addressed when carrying out an assurance engagement on IT outsourcing suppliers.

The International Auditing and Assurance Standards Board's International Standard on Assurance Engagements 3402, Assurance Reports on Controls at a Service Organisation (ISAE 3402) contains substantially the same provisions for application on an international basis.

As with contractual requirements generally, small businesses may find it difficult to demand assurance rights in practice. This potentially increases the risks to them of using third parties. As a result, suppliers may need to publish independent assurance reports on a voluntary basis or find alternative mechanisms to win the trust of potential customers.

## 4.7 Personal information practices

Information security practices are vital to ensuring the confidentiality, integrity and availability of personal information. There are also some practices that a business could adopt which may help it to manage the specific issues associated with personal information.

This section highlights six such practices:

- organisation structures;
- privacy by design;
- privacy notices;
- responses to privacy failures;
- privacy audit and assurance techniques; and
- privacy-enhancing technologies.

### Organisation structures

It can be difficult to establish a coherent organisational structure around personal information because a number of different functions are involved and responsibility cannot be easily contained in one area.

The IT function, for example, needs to be aware of privacy requirements when designing systems and managing information security. A system can be highly secure while not respecting privacy, for example if it retains or reuses information without the consent of individuals. However, it is also possible to design systems in such a way as to protect privacy, for example by obscuring certain pieces of data and making it difficult to aggregate data together.

Legal functions are likely to have a central role in determining and implementing privacy policies, especially where a business operates in highly regulated environment. The complexity of legal requirements is likely to require specialist skill and knowledge.

Marketing functions need to be highly aware of privacy issues, as they are likely to be reusing personal data in customer analysis and communication and looking to maximise the value of the information they have.

In the US, responsibility for privacy matters has often been a high-profile role, with the recent development of the Chief Privacy Officer role in many large US businesses. This reflects a stronger commercial focus in the US on privacy. By contrast in Europe, privacy has often been seen as a compliance-based and administrative role, applying the requirements of data protection legislation rather than providing strategic value. However, as the importance of personal information to business models grows, so too do the risks attached to it. Therefore, senior level involvement may become more common.<sup>86</sup>

<sup>85</sup> See Technical Release AAF 01/06, *Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties* and Technical Release ITF 01/07, *Assurance Reports on the Outsourced Provision of Information Services and Information Processing Services*.

<sup>86</sup> International Association of Privacy Professionals, *A Call for Agility: The Next Generation Privacy Professional*.

## Privacy by design

Privacy by design is an approach to designing systems, processes and new products whereby privacy implications are considered as early as possible.<sup>87</sup> Developed as a concept in the 1990s by Ann Cavoukian, the Privacy Commissioner of Ontario, it is built on the observation that in many cases, businesses only consider privacy requirements at the end of a project, when they are looking at compliance issues.

Failures to take account of privacy early in a project could be due to lack of management attention or interest in the issue. There is also an inherent tension between innovation and compliance functions, and finding ways to support new ideas while considering privacy constraints can be difficult in practice. Building a dialogue around privacy requirements across the organisation is therefore an important step and privacy impact assessments are a way of doing this.

### Panel 4.10: Privacy impact assessments

A privacy impact assessment (PIA) is carried out in the early stages of any project which may make use of personal information and potentially threaten privacy rights. Such assessments are similar in concept to environmental impact assessments and are not usually mandated.

A PIA aims to help a business identify all the privacy risks related to system, process or product changes and thereby design systems which are sensitive to privacy considerations. The UK ICO describes the benefits of PIAs as follows:<sup>88</sup>

- 'To identify privacy risks to individuals.
- To identify privacy and DP compliance liabilities for your organisation.
- To protect your reputation.
- To instil public trust and confidence in your project/product.
- To avoid expensive, inadequate 'bolt-on' solutions.
- To inform your communications strategy.
- Enlightened self-interest.'

There are number of templates and checklists which can be used to help in this process, including a handbook from the ICO. These emphasise the need for assessments to take place early in the process and go beyond a mechanical tick-box exercise. Rather, they should link to the wider risk management processes of the business.

Most PIAs to date have taken place in the public sector, rather than the private sector. However, regulators encourage them as useful tools in implementing a privacy by design approach.

## Privacy notices

Privacy notices are an important part of communicating privacy practices to individual consumers. They lay out the privacy policies and practices of a business and enable a consumer to consent to the use of their personal information in the ways specified. As a result, in consumers' eyes, they support:

- Transparency – having visibility of the personal information held by a business and how it is used; and
- Control – having the ability to opt in or out of particular uses and maintain some control over what personal information is shared.

However, privacy notices are often written in legal jargon and can therefore be difficult to understand. As a result, individuals frequently ignore privacy policies in practice.

It is suggested that a business develop a range of notices for different audience needs, based on some simple standard templates. Where such notices are clear and easy to compare, this approach potentially builds higher levels of trust with consumers and is popular with regulators. A multi-level privacy notice will typically consist of three layers<sup>89</sup>:

<sup>87</sup>ICO, *Privacy by Design*.

<sup>88</sup>ICO, *Privacy Impact Assessment – An Overview*.

<sup>89</sup>See, for example, the 2006 guidance from the OECD, *Making Privacy Notices Simple: An OECD Report And Recommendations*.

- a very basic notice, with contact details and how the information will be used;
- a condensed notice, including clear sections such as scope of the policy, personal information collected, use of information, choices and contact details; and
- a full notice, with all the information that a consumer could need.

However, there is a balance to be struck as high levels of transparency and control are not necessarily easy to understand and exercise. Where a business seeks to give users very granular control over how their personal information is used and shared, this may result in complex and unusable settings, as evidenced by the social networking site Facebook's difficulties in this area.

#### Panel 4.11: Facebook's privacy settings and controls

Through 2009 and 2010, Facebook took substantial criticism for sharing users' personal information with other businesses and putting it in the public domain. One of the issues at the heart of this debate was control and clarity over what Facebook was doing.<sup>90</sup>

Facebook argued that they took a granular approach, giving users a very specific set of controls over how their information was shared. However, this control was accompanied by default privacy settings which shared information very publicly. Therefore, while users could continue to keep their personal information private within their network, the onus was on them to manage their privacy settings proactively. Of course, in many cases, users did not act proactively and allowed the default settings to operate.

Furthermore, the granularity meant that the privacy settings became extremely complex to manage for the average user. As was noted by the New York Times, the Facebook privacy policy, at 5,830 words, was longer than the US constitution. There were 50 settings and 170 options.

In an article in the Washington Post, Mark Zuckerberg acknowledged the errors made by Facebook.<sup>91</sup> While he defended the broad position of the business, arguing for the merits of more open data, he accepted that the controls were too complex and users did not feel in control of their information:

'The biggest message we have heard recently is that people want easier control over their information. Simply put, many of you thought our controls were too complex. Our intention was to give you lots of granular controls; but that may not have been what many of you wanted. We just missed the mark... We have heard the feedback. There needs to be a simpler way to control your information.'

Therefore, finding the balance so as to make users feel genuinely empowered is an important lesson for businesses.

### Responses to privacy failures

In spite of good practices, privacy failures can still happen and lead to substantial reputational damage. Therefore, managing the consequences of breaches is an area of growing importance.

Businesses are likely to take an approach similar to other types of disaster management activity where reputation could be damaged. The aim is to respond quickly and effectively to customer concerns and actions could include:

- withdrawal or amendment of the changes which raised concerns;
- direct communication with the affected customers;
- working with regulators to take on board their concerns; and
- longer term public relations activity to rebuild reputation.

Google's experience with Buzz is a good example of such actions.

<sup>90</sup> *New York Times*, 'Facebook privacy: a bewildering tangle of options' and Nick Bilton, 'Price of Facebook Privacy? Start Clicking'.

<sup>91</sup> Mark Zuckerberg, 'From Facebook, answering privacy concerns with new settings'.

#### Panel 4.12: The controversial launch of Google Buzz

Google is at the leading edge of using personal information. However, Google has experienced problems in the development of new products and the launch of the Buzz product was one such example.

Buzz is a social networking tool linked with Google's email service. Upon launch, users logged onto their email accounts to find that they were automatically part of a new network, based on the contacts that they had on email. Furthermore, other users could see their network and therefore their closest contacts. Given that no consent had been given for sharing this information with others, this not only offended many users but also breached privacy laws in some countries.<sup>92</sup>

Google responded to criticism in a number of ways. First, they amended the product to take account of the feedback. Google's own blog stated:

'We've heard your feedback loud and clear, and since we've launched Google Buzz four days ago, we have been working round the clock to address the concerns you've raised....'<sup>93</sup>

Google also issued an apology and explained that, although they had tested the system internally, this had been insufficient.

While this response succeeded in stemming some of the criticism, many claimed that it did not go far enough and a group of regulators continued to examine whether it breached privacy laws. Indeed, the Canadian Privacy Commissioner, backed by regulators in nine other countries, wrote an open letter to Google in April 2010. In it, she argued that although Google did respond quickly and apologise, it showed a disregard for privacy in its development of new products and services:

'While your company addressed the most privacy-intrusive aspects of Google Buzz ... we remain extremely concerned about how a product with such significant privacy issues was launched in the first place....It is unacceptable to roll out a product that unilaterally renders personal information public, with the intention of repairing problems later as they arise. Privacy cannot be sidelined in the rush to introduce new technologies to online audiences around the world.'

This response demonstrates the care that a business needs to take when developing new products for customers which also satisfies regulator and customer concerns.

#### Privacy audit and assurance techniques

To gain confidence that their privacy practices are appropriate and effective, and to demonstrate this confidence to others, a business can build on established audit and assurance techniques.

#### Panel 4.13: Privacy audits

A privacy audit aims to gain comfort that a business is complying with relevant laws and regulations and is managing privacy risks in this area appropriately. As the risks and profile of privacy issues grow, so too do the demands for privacy audits. They are becoming a particularly popular mechanism for regulators to employ.

As highlighted in panel 2.6, the FTC imposed an obligation on Google to have independent privacy audits every 2 years for the next 20 years following the Buzz product launch. Similar requirements were made by the Canadian Privacy Commissioner.

The UK ICO has also increased its privacy audit activities. Audits on private sector companies are carried out with the consent of the business, although consent is not needed in the public sector. An executive summary of privacy audits is published on the ICO's website and organisations audited by the ICO include Google, the Metropolitan Police, Nationwide Building Society and the Law Society. However, only 19% of businesses which were offered a privacy audit by the ICO accepted it.<sup>94</sup>

<sup>92</sup>Nicholas Carlson, 'Warning: Google Buzz has a huge privacy flaw'.

<sup>93</sup>Todd Jackson, 'A new Buzz experience based on your feedback'.

<sup>94</sup>Cameron Craig, 'Data privacy: When will watchdog ICO get its teeth into private sector audits?'

#### Panel 4.13: Privacy audits (continued)

In response to the growing demand for audits, the AICPA and the Canadian Institute of Chartered Accountants (CICA) have issued a set of *Generally Accepted Privacy Principles*. These can be used by businesses or audit firms to support a range of activities, including internal and external privacy audits.

A business can also look to third party privacy seals to provide assurance to stakeholders on its privacy practices, such as CICA's WebTrust seals or those provided by the company TRUSTe. These schemes are usually based around the Fair Information Principles and provide mechanisms for regular audits. Privacy seals have become very popular, especially in the US, where many established websites display them. However, critics of such schemes point out that a business usually pays to be accredited, raising questions around the independence of assessments.

### Privacy-enhancing technologies

The notion of privacy-enhancing technologies (PETs) was first outlined by David Chaum in 1981.<sup>95</sup> Since that time, a wide range of PETs have been developed which are designed to help individuals protect and manage their personal information. Consequently, they can be employed to mitigate or manage many of the problems outlined in Chapter 2.

PETs can broadly be divided into two types. There are tools which help an individual manage their personal information and which are therefore focused on transparency and control. And there are technologies which aim to prevent others from gathering personal information, including:

- anonymising or pseudo-anonymising products which strip the identity of the individual from the rest of the data;
- encryption tools which stop unauthorised parties from accessing information;
- filters and blockers which stop third parties from reaching individuals; and
- track and evidence erasers.

Anonymity techniques are particularly popular. For example, the Open Data movement is looking to these techniques to enable the release of personal information without compromising privacy rights. While they may be attractive, anonymity techniques are challenging in practice. Unless they are carried out very well, it can be possible to re-identify individuals by combining bits of data.

#### Panel 4.14: The problems of anonymity: the Netflix data prize

Netflix is a US-based business which rents movies to its customers. As part of the service, customers are invited to post reviews and ratings of the films they watch to provide feedback to other customers. This information is then used to recommend films to other users.

In 2007, Netflix established a prize, worth \$1 million, to improve their recommendation algorithm. This was based on publicly releasing a data set containing 100 million movie ratings by 500,000 users. These ratings were anonymised by stripping any identification from the data set.

However, two researchers from the University of Texas, Arvind Narayanan and Vitaly Shmatikov, were able to re-identify specific individuals by matching data from the Netflix data set with publicly available data from another movie review site, IMBD, which did have personally identifiable information.<sup>96</sup> By using just 50 profiles from the IMBD site, they were able to re-identify two individuals with statistical near certainty. Netflix subsequently abandoned plans for a second prize.

Therefore, while anonymising techniques potentially have an important role in protecting individual privacy, there are significant difficulties in achieving true anonymity in the digital environment. These difficulties underlie the challenge of defining personal information when individuals can be identified through combinations of non-sensitive data.

Governments also have concerns about the use of strong PETs, where they limit a government's ability to track communication between crime and terror suspects.

<sup>95</sup>Enterprise Privacy Group, *Privacy by Design: An Overview of Privacy-Enhancing Technologies*.

<sup>96</sup>Arvind Narayanan and Vitaly Shmatikov, 'Robust de-anonymization of large sparse datasets (How to break anonymity of Netflix prize dataset)'.

Furthermore, PETs have not been heavily adopted in the marketplace by users. There are a number of possible reasons for this. The business case for adoption by businesses or the technology industry may not be clear. Instead, it is largely left to individual users to adopt them. When combined with a low ease of use for many of the tools, PETs to date have met with limited success in practice.

## 4.8 Intellectual property practices

Specific practices to protect intellectual property fall into two broad areas.

- There is intellectual property or sensitive commercial information that a business wants to keep secret. In these cases, the key risks come from failures in security, for example where intellectual property is appropriated by hackers or sold by employees. As a result, practices are largely based on information security principles.
- There is also information content that a business wants to exploit but share widely. Here, the risks concern access to content without paying for it. In these cases, businesses are concerned with the enforcement of intellectual property rights.

### Implementing effective information security practices

There are many anecdotes concerning organised criminal and state-sponsored gangs hacking businesses in order to gain access to valuable intellectual property which they can sell to rival businesses or governments. As a result, technical security measures are likely to be increasingly important to businesses as they attempt to keep their sensitive information confidential.

Business employees can perpetrate intellectual property theft by selling information to competitors. As a result, controls around information access for employees may be particularly important and there are many good practices which can stop unauthorised access or track suspicious activity, such as system ID management and audit trails. Staff morale can also be an important influence on whether employees may engage in such activities.

The increase in information sharing across businesses is also an area of growing risk. To a large extent, risks here can be mitigated through contractual arrangements between parties and effective security measures to protect intellectual property from unauthorised access by suppliers. However, a business may need to consider how to structure relationships between different parties across the supply chain and what intellectual property it is prepared to share.

### Digital rights management systems

Technology and content companies have experimented with systems to protect intellectual property rights for many years with varying degrees of success. Now termed digital rights management (DRM) systems, they stop the user from copying content. However, they have attracted significant controversy.<sup>97</sup> As a result, while DRM systems are used, they are not universally implemented by content producers.

Critics accuse DRM technologies of being disproportionate. While they can stop casual copying, DRM systems can never, in practice, stop determined individuals from circumventing protections and illegally copying material. However, they can have a disruptive and detrimental impact on other users.

DRM systems are generally not compatible with one another and there are no clear standards in place. Instead, they are closely linked with the device or service which is being used and therefore they can be inflexible and inconvenient, locking users into specific pieces of technology. This has made the idea of DRM very unpopular with users who can end up paying more than once for the same piece of content on different platforms. It also has long term implications for the sustainability of content. If content is tied in with particular pieces of software or hardware which are not compatible with other systems, it could result in content becoming inaccessible in the long-term.

Another criticism of DRM is that it can provide controls that go beyond the intellectual property rights currently provided for in law. Indeed, sceptics of DRM refer to 'Digital Restrictions Management' as a more accurate description of what it does. For example, in some cases, DRM may prevent any kind of copying, which goes beyond what many countries allow through the fair use doctrine. It is also possible for the content provider to have access to see how the content has been used, giving them insight into the individual consumer. Many opponents see this as inappropriate and an invasion of privacy.

<sup>97</sup> See the opposition by the Electronic Frontier Foundations at [www.eff.org/issues/drm](http://www.eff.org/issues/drm).

As a result of these arguments, most music today is downloaded without DRM software. However, other content, such as movies and video games, is still protected in most cases by DRM software and its use continues to provoke strong debate.

It should be noted that DRM systems are also suggested as a way of protecting personal information and enabling an individual to have control over how their personal information is accessed, used and shared.

## 4.9 The growing regulatory agenda

As security failures increasingly impact on individual consumers and citizens, there is a developing regulatory agenda, particularly around the security of personal information. As a result, a business may need to shift its thinking from internal risk management to meeting external demands.

### Economics of information security

An important influence on the development of information security legislation has been the thinking of economists in the growing field of information security economics. Researchers have observed that software in many instances continues to be quite insecure, despite opportunities to improve security. In looking for reasons for this failure, it is argued that the issues are not purely technical. Rather, the economic incentives around security are not fully aligned and the parties with the greatest power to improve security are not encouraged or rewarded to do so.<sup>98</sup>

In practice, the burden of securing data typically falls on individual businesses or consumers. However, those with the technical or financial power to make a significant difference to information security in practice are players in the technology industry and financial institutions. The economic analysis of this area is growing and is likely to provide new perspectives.

#### Panel 4.15: Information security regulation and the House of Lords report

In 2007, the UK House of Lords Science and Technology Committee undertook a review of internet security relating to individual consumers. Influenced by the economic approach, they made a number of recommendations to align incentives more effectively and increase transparency around the actions of different market participants. For example, it recommended:

- exploring the possibility of greater vendor liability in the event of security failures which could be attributed to the negligence of the supplier;
- that banks be held responsible for losses caused by financial fraud;
- that internet service providers develop stronger industry security standards in the provision of internet connections to consumers; and
- the enactment of a data breach notification law.

All of these measures were intended to shift the responsibility from the consumer onto the industries which can make a real difference to information security in practice. However, despite wide-ranging consultations on the report, the UK government did not implement the recommendations.

There is also growing research into the economic incentives around privacy protection, such as with PETs. While the costs to implement such technologies may be clear, the benefits of being proactive remain uncertain. There has been a range of studies into the potential business case of good privacy practices and PETs.<sup>99</sup> However, business behaviour in practice is typically still driven by the threat of financial penalties in the event of non-compliance, rather than the positive benefits of good privacy practices.

## 4.10 Summary

In many cases, information rights are well established and clear. Therefore, the business imperative is to secure those rights effectively. The field of information security deals with the protection of valuable and/or sensitive information and is built around three key principles, namely confidentiality, integrity and availability.

<sup>98</sup>This is explored in more detail in Ross Anderson, 'Why information security is so difficult - an economic perspective'.

<sup>99</sup>See, for example, London Economics, *Study on the Economic Benefits of Privacy-Enhancing Technologies: Final Report to The European Commission DG Justice, Freedom and Security* and the ICO, *The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection*.

The principles of information security are reflected in a wide range of established information security practices. Business processes and management techniques are a central part of any information security strategy. Given the dominance of IT, technical computer security is also a very important component of information security.

Despite the existence of a wide range of good practices, many businesses struggle to implement effective information security. One reason for continuing security failures is that it is often difficult to connect security measures to business priorities and thereby gain sufficient management and employee attention.

It can be difficult to make good decisions about information security investments. Good practice suggests that management should assess the risks surrounding information and balance the costs of security measures against the possible impact of security failures. However, the difficulty of quantifying these matters limits the effectiveness of structured decision-making processes in practice.

While many information security measures are technical, a business is also likely to benefit from techniques which integrate security skills and knowledge across technical and business functions. Information governance is a set of management practices which aims to protect the quality and control of information throughout the organisation and integrate accountability accordingly

IT has enabled information to be more dispersed, putting greater emphasis on individual behaviour and making it more important to embed good security practices. As employees increasingly use consumer devices, and frequently their own personal devices, to store or access corporate data, embedding good behaviour will become ever more important. Training can help raise employee awareness of security policies and processes. Culture and senior-level commitment are also important factors and, where security can be aligned with the objectives and brand of the business, it is more likely to become central to business activities.

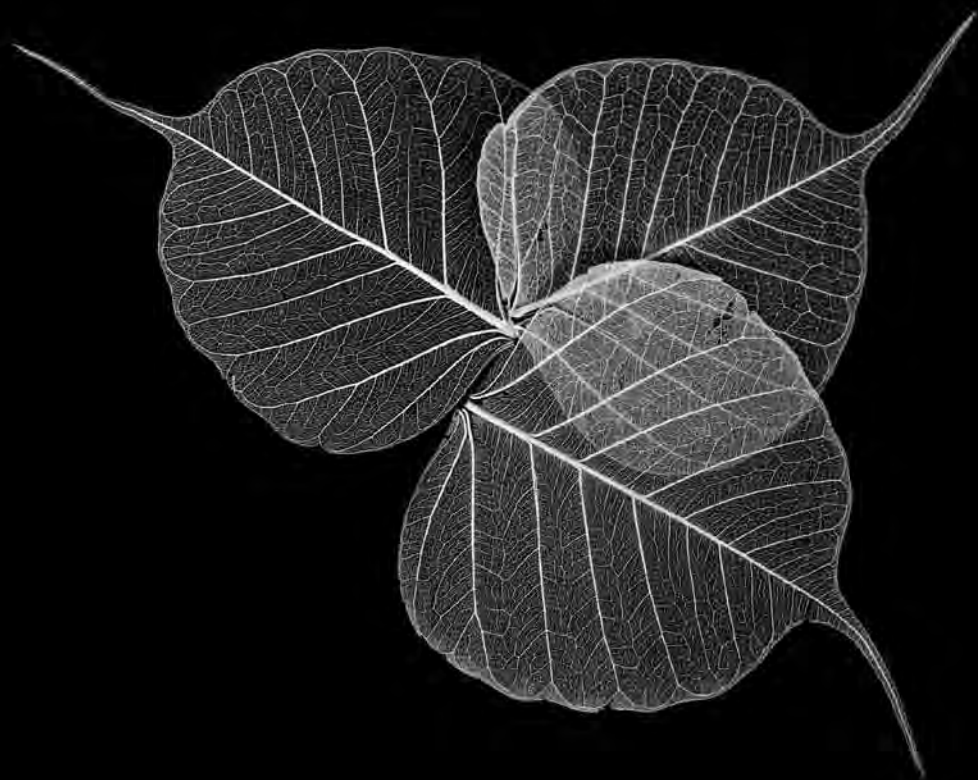
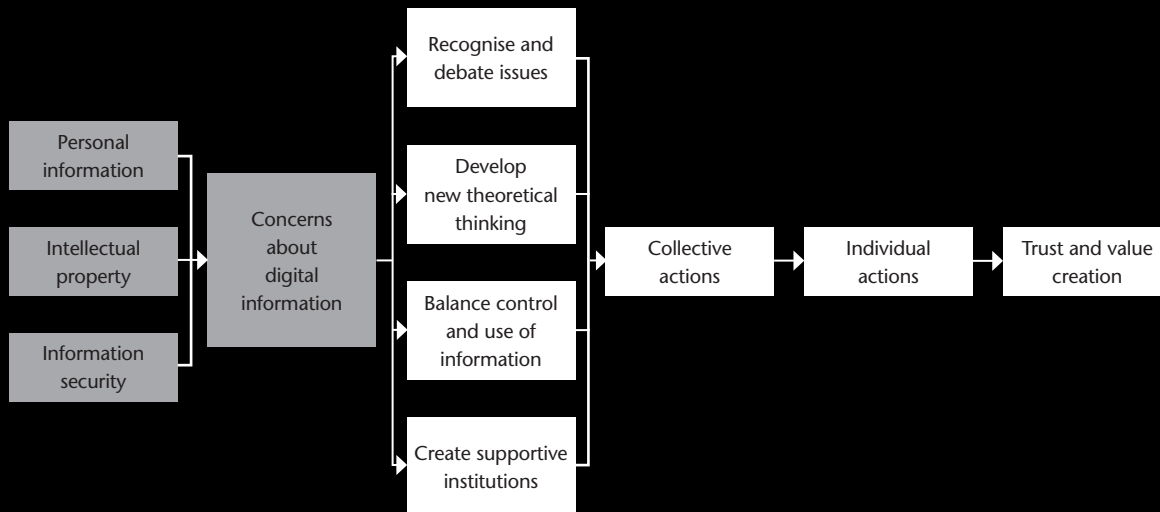
A growing security challenge concerns the explosion in outsourcing and collaboration across supply chains. As a result, information rarely sits in one organisation as a static resource but instead is the subject of continual flows between different parties. This may lead to a shift in security thinking, away from establishing a secure perimeter around the organisation to a more dynamic model which emphasises security across a supply chain.

Finally, as security failures increasingly impact on individual consumers and citizens, there is a developing regulatory agenda, particularly around the security of personal information. As a result, a business may need to shift its thinking from internal risk management to meeting external demands.



# 5. BUILDING TRUST

Individual good practices are not sufficient. There needs to be widespread engagement and action at all levels across society to address the issues raised in this report. How do we promote informed debate? And what are the elements of a social and legal framework fit for a digital economy?



# 5. BUILDING TRUST

## 5.1 Impact of new technology

Chapters 2, 3 and 4 outlined many good practices in the fields of personal information, intellectual property and information security, as well as the broad legal and social environment within which businesses are operating.

They also highlighted some areas which are testing the limits of current thinking.

- With the rapid increase in the collection of personal information, there are new questions around who should be able to retain, use, share and benefit from this information.
- The changed economics of information goods encourages the free and open exchange of creative content and challenges the scope and application of intellectual property rights.
- The growing frequency and impact of information security failures on businesses and individuals is leading to pressure for new regulation.
- The international operation of many businesses challenges the national and regional basis for established regulation in these areas.

These challenges are not surprising, given the radical impact that new technology can have on economies and wider social structures.

### Creative destruction

New technology is a central part of economic development and economists have long recognised the revolutionary impact of new technology on the way that we do things and the way that businesses and governments are organised. The Austrian economist, Joseph Schumpeter, for example, argued in the 1940s that technology was the key driver of economic growth and innovation, triggering a process of ‘creative destruction’, whereby established processes and businesses were destroyed by fresh methods built on new technology.<sup>100</sup>

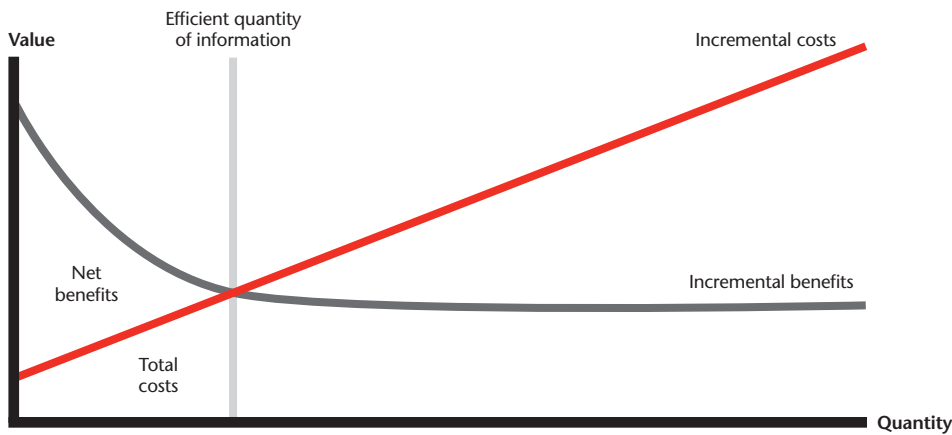
IT is a particularly disruptive technology because it radically changes the economics of information. It shifts the supply curve of information by reducing the costs of information. It also shifts the demand curve of information by increasing the benefits that can be gained through it. This creates a vast new space of economically efficient information, making many new activities viable and profoundly changing the way that a business can create and deliver value to customers. This is illustrated in Figures 5.1 and 5.2.<sup>101</sup>

Figure 5.1 shows the supply and demand curves that can, in principle, be drawn for each and every type of information to represent the incremental cost of providing more of that information and the incremental benefit of using such information. The area under the supply curve represents total costs, the area under the demand curve represents total benefits and the area between the curves represents net benefits.

<sup>100</sup> Joseph Schumpeter, *Capitalism, Socialism and Democracy*.

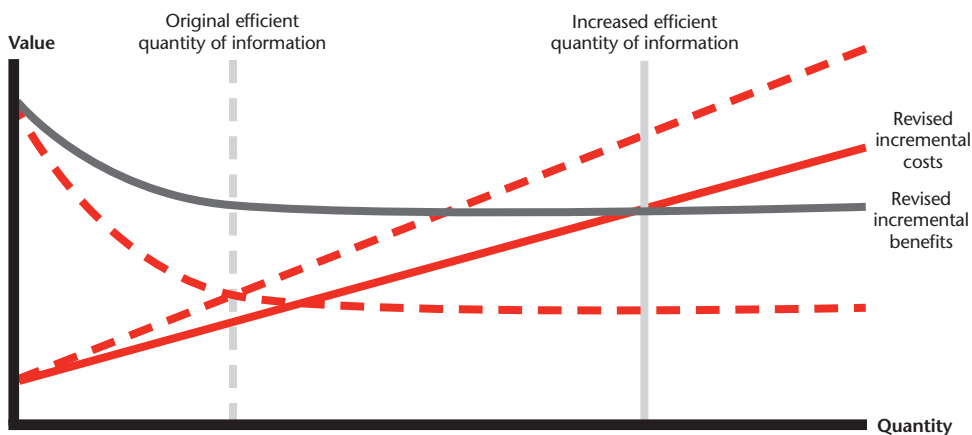
<sup>101</sup> This section incorporates parts of ICAEW's earlier report, *Measuring IT Returns*.

**Figure 5.1: Information supply and demand curves**



Through the combination of different technologies, IT changes the supply and demand curves. It does this in two ways, frequently at the same time. It reduces the costs of information-handling and communication activities and it enables businesses to get more benefits from the use of information. By shifting both the supply and demand curves, IT potentially increases the amount of information that it is economically viable to produce and the net benefits of that information. These shifts are shown in Figure 5.2.

**Figure 5.2: Impact of IT on information quantity**



### Social implications

However, transformation in economic possibilities through new technology often creates social tensions and new questions in parallel. It can lead to many situations that have not been previously considered or which push against the established boundaries of rights and duties. It can heighten existing tensions between different interests.

IT does all of these things. Furthermore, by enabling powerful aggregation and analytical techniques, IT increases the value of all kinds of information that may have been previously thought of as useless or valueless data, leading to new competition over how it should be used and exploited.

Alongside the development of new technology, we often see new norms develop which will build confidence in it and support widespread adoption, for example:

- laws governing how technologies are used, potentially labelling particular uses as not socially acceptable;
- laws covering the social consequences of technological development, such as the workers' rights developed in the wake of factory technology;
- laws which replace or update laws that have become easy to evade or avoid as a result of new technology; and
- social norms to define acceptable individual behaviour in the light of new technology.

The debate between the opportunities presented by new technology and the actions needed to build social acceptability is currently seen most prominently in the area of medical technology. Medical ethics and law are well established areas of theory and practice which reflect the dilemmas faced in this area and provide a framework for doctors and lawyers to take all relevant interests into account when making decisions. Debates in these areas frequently focus on how to encourage new areas of research and maximise the potential benefits they bring, such as stem cell research, while also finding limits or checks which make developments socially, morally and legally acceptable.

Therefore, unless we recognise and address the social challenges related to digital information, there is a risk that opportunities to use it are missed.

## 5.2 Trust in business

Trust is an important feature which underpins the use and value of new technologies and therefore can support the development of a digital economy. While the term 'trust' has many specific applications in this context, such as cyber trust,<sup>102</sup> we use it broadly to refer to the relationship between an organisation and its different stakeholders.

### The notion of trust

All businesses exist by creating value for a number of different parties, which include:

- customers;
- shareholders;
- employees; and
- suppliers.

For any of these relationships to be sustainable, there also needs to be a degree of trust between the parties. If one party does not trust the other to deliver their side of the exchange and to adhere to certain expected standards of behaviour, the relationship is unlikely to survive long. Therefore, any successful business relies on building trusting relationships with a variety of different parties.

#### Panel 5.1: Building business trust

Trust is exhibited where one party expects another party not to act in a harmful way, despite the opportunity to do so. Therefore, the trusting party is vulnerable to the actions of the trusted party but chooses to act anyway, believing that the other party will do them no harm.

Although apparently similar, trust is not the same as prediction. It is a way of simplifying decisions and acts as an alternative to a rational calculation of risk and reward:

'...trust reduces complexity far more quickly, economically and thoroughly than does prediction. Trust allows social interactions to proceed on a simple and confident basis where, in the absence of trust, the monstrous complexity posed by contingent futures would again return to paralyze action.'<sup>103</sup>

In economic terms, trust reduces transaction costs substantially and most economic and social interactions require a degree of trust in practice.

Trust is a complex notion and can be seen to operate at two levels.

- Narrow scope trust concerns the trust attached to an individual business, based on its particular behaviour, brand and reputation. Therefore, the activities outlined in Chapter 4 can help a business to build up this kind of trust.
- Broad scope trust concerns the wider legal and institutional environment. Where laws are in place to compel particular business behaviour, and there are clear sanctions in the event of non-compliance, there is likely to be a higher level of trust in all businesses. By contrast, where there is a low level of broad scope trust, individual businesses will have to work harder to build trust with individual customers or others.

The interaction between these two levels of trust is hotly debated.<sup>104</sup> However, it is broadly recognised that both levels of trust play a role in encouraging market transactions.

<sup>102</sup> For a collection of materials on cyber trust and other aspects of cyber security, see Brian Collins and Robin Mansell, *Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews* and the associated papers.

<sup>103</sup> J. David Lewis and Andrew Weigert, 'Trust as a social reality', p969.

<sup>104</sup> Kent Grayson, Devon Johnson and Der-Fa Robert Chen, 'Is firm trust essential in a trusted environment? How trust in the business context influences customers'.

## Elements of building trust in a business

Businesses can build trust at an individual level by implementing good practices. However, good practices need to be underpinned by clear legal obligations and social expectations. We identify four essential elements to building broader trust around digital information.

**Recognise and debate issues.** Regulators, law makers and the technology industry have a major role to play. However, all businesses are affected by some of the issues raised in this report, as are all individual consumers and citizens. Therefore, debates need to engage broadly across all sections of society in order to take account of different interests and perspectives.

**Develop new theoretical thinking.** While technology is the direct cause of the difficulties outlined in the report, it is radical changes to the economics of information which are at the heart of the social tensions. Therefore, we need to encourage a variety of new thinking which is rooted in the economics of digital information.

**Balance control and use of information.** There needs to be clear rights over information to enable parties to form expectations about its use and protection. However, this control needs to be balanced with the ability of different parties to use and share information for a wide range of benefits.

**Create supportive institutions.** A variety of institutions are needed which can address this broad range of issues and develop robust and flexible solutions. Institutions need to include many participants, including regulators, businesses, individual consumers and the technology industry and promote common approaches, as far as is possible.

Although each of these elements is essential, they are also fraught with difficulty which may limit realistic progress. Academic research can play an important role in developing deeper understanding of the challenges of the digital environment and supporting each of these elements. By providing objective evidence on the risks and benefits attached to digital information, as well as different policy options, research can help policy-makers, management and individuals make better decisions. The appendix outlines the role and challenges of academic research and goes on to highlight a variety of possible research topics.

## 5.3 Recognise and debate issues

The starting point for building greater trust is widespread engagement across society to debate issues. This includes representatives from business and government, as well as individual consumers and citizens.

Indeed, individual consumers and citizens have a particularly important role in these debates:

- they are the subjects of personal information which is being used by businesses to generate profits;
- they are creators of all kinds of new intellectual property which is being shared across social media platforms; and
- they are the consumers of services and creative content which build on their personal information and intellectual property.

Therefore, they have a direct stake in the outcome of these debates. However, many of the debates highlighted in this report have been dominated in practice by regulators, the industries which have been most affected by the technology changes and pressure groups. How do we get broader engagement in defining new social norms and expectations which underpin more formal policy solutions?

## Build awareness and recognition

Central to building widespread engagement is raising awareness of the issues outlined in this report and gaining recognition of their importance. There are a number of barriers to achieving this.

For many businesses, the issues outlined in this report primarily appear to affect those at the forefront of personal information use or specific industries which develop and exploit creative content. In other cases, there continues to be a strong emphasis on the development of good practices as a way of solving concerns and issues of trust.

The impact of failures on individual businesses is not necessarily clear or easily quantified, and businesses may be more focused on extracting the maximum benefits that they can from digital information. Furthermore, the possible impact on society of failing to address these concerns

is not generally regarded as catastrophic, as is potentially the case with issues such as climate change or securing safe energy supplies, for example. As a result, it can be difficult to gain sufficient attention and priority from senior decision makers.

While individuals may voice concerns about the security and use of their information, they also benefit from widespread use and sharing of their personal information and intellectual property. This again makes it difficult to gain sufficient attention and action from individuals. Furthermore, there are substantial economic interests in maximising the use of personal information and tightening controls over intellectual property, which may overwhelm the concerns of individuals.

However, we suggest that a failure to address many of the issues outlined in this report will have significant effects on the economy and wider society.

While good practices can solve many of the problems for individual businesses, they are not sufficient. Good practices are grounded in wider legal rights and social expectations, which help a business to link specific policies to business objectives. Trust for individual businesses is likely to be higher when there is broad trust in the wider institutional environment. Furthermore, as technology continues to improve, leading edge issues will impact on a greater range of businesses. The use of smart meters by energy companies, for example, raises new questions concerning the analysis of detailed energy usage records and extends privacy debates into fresh areas.

Opportunities to use digital technologies will be lost if businesses fail to invest in new services or creative content, or individuals lack sufficient trust to use them. This potentially has a major economic impact and may reduce the social benefits that individual consumers gain from new services.

Furthermore, pervasive use and sharing of digital information could result in a wide range of profound and irreversible social changes, for example, individuals losing the ability to remain anonymous or shake off information about their past. As a result, they merit serious consideration by all.

## Encourage debate

If it can be recognised that there are serious issues to be debated about the use and sharing of digital information, we move onto the questions to be addressed. Panel 5.2 outlines some of the questions which need to be considered and debated by individual consumers and citizens, as well as regulators and the technology industry.

### Panel 5.2: Contentious questions

- To what extent is the commercial exploitation of personal information a matter of concern?
- How should various uses of personal information be balanced against different benefits, for example, security matters, medical and social research and personalised services?
- To what extent should public and location data, as well as search data, be gathered and used by businesses?
- To what extent should businesses be able to use extensive personal profiling?
- How should voluntary sharing of personal information over the internet be viewed: a matter of personal choice and risk or something for greater regulation?
- To what extent is copying content (when in breach of copyright) morally wrong?
- To what extent do consumers want to pay for creative content?
- How should the benefits from co-created intellectual property be shared?

## 5.4 Develop new theoretical thinking

By shifting the economics of information, IT radically changes the ways that information can be collected, used and shared. However, much of the thinking outlined in this report is based on the economics of the physical world, rather than the virtual world enabled by digital technology.

Our thinking can often be limited by our imaginations and an inability to understand the full implications of new technology. Consider, for example, the early days of motor vehicles in the UK, when cars had to be driven behind someone walking with a red flag to warn the public of the potential danger of a motor vehicle.<sup>105</sup> While this may now appear to be a strange response

<sup>105</sup> The Locomotive Act 1865, also known as the Red Flag Act.

to an exciting new technology, it was rooted in an inability to understand the potential benefits of motor vehicles and radically different ways of managing their risks, such as road safety codes, traffic lights and other such methods. It was also rooted in vested interests that were resistant to change.

Therefore, as part of the informed debate around digital information, we need to encourage more challenging and radical thinking which is rooted in the new economic opportunities.

We highlight three areas in which established thinking may need to be recast:

- the growing importance of information ethics;
- the move from tangible to intangible property; and
- the convergence between information regimes.

### Growing importance of information ethics

Ethics is concerned with determining right and wrong behaviour, based on moral principles. Normative ethics looks at behaviour at a general level and develops principles for determining right and wrong actions. Applied ethics looks at specific ethical dilemmas to determine the right course of action in particular circumstances.

Information ethics is concerned with right and wrong behaviour surrounding information and has been a small field to date.<sup>106</sup>

#### Panel 5.3: Information ethics

Notions of information ethics, and the expected behaviour around information according to moral principles, can be traced back to ancient Greece. However, it moved into the modern world following the writings of Norbert Wiener. His books *Cybernetics* (1948) and *The Human Use of Human Beings* (1950) foretold many of the computing developments that were to come and developed a series of principles by which ethical dilemmas about information could be resolved. Where dilemmas could not be resolved through the extension of existing principles, he suggested that they should be resolved based on ideas of freedom, equality and benevolence.

Weiner was ahead of his time and his work was ignored for many years. The discipline of information ethics started to take hold in the 1980s, following the explosion of computer use in government and businesses. While it remains a developing field, it covers thinking and research in a wide range of areas, including:

- privacy and intellectual property;
- the digital divide (which refers to the impact of technology on those who do not have access to it);
- computers in the workplace; and
- the responsibilities of information and IT professionals.

There is clear scope for greatly expanding this field and developing stronger moral positions on the use and sharing of information to respond to some of the challenges presented in this report. The fact that a business or individual has the ability to use or share pieces of sensitive information about others does not necessarily mean that they should do so. The impact of sharing that information may be profoundly or disproportionately damaging and therefore, even if it is legal, some degree of self-restraint may be helpful.

Information ethics can apply to individual behaviour. It can also be integrated into business ethics more broadly.

#### Panel 5.4: The cases of TJX and ChoicePoint

TJX is a large cut-price retailer, owning brands such as TK Maxx. ChoicePoint provides a range of personal profiling services, such as background screening and authentication. Both of these US-based businesses suffered serious data breaches where a substantial amount of personal information was accessed. In TJX's case, it was the credit card details of 45 million customers. ChoicePoint had 145,000 customer files accessed for the purposes of identity theft.

<sup>106</sup> Luciano Floridi, 'The information society and its philosophy: introduction to the special issue on "the philosophy of information, its nature and future developments"'.  
The Information Society and its Philosophy: Introduction to the Special Issue on "The Philosophy of Information, its Nature and Future Developments"

#### Panel 5.4: The cases of TJX and ChoicePoint (continued)

In an article entitled 'How ethics can enhance organizational privacy', Mary Culnan and Cynthia Williams outline how the businesses could have integrated ethical principles into their compliance obligations and thereby strengthened their internal processes. Observing that individuals are in a vulnerable position where businesses hold personal information about them, Culnan and Williams argue that a business should adhere to the ethical principle of 'doing no harm'. As such, by failing to stop criminals from accessing personal information, both TJX and ChoicePoint also failed in their ethical duties. They argue:

'No organization can guarantee that it will not suffer a privacy harm in the future. However, the stronger the sense of moral responsibility, as evidenced by the organization's leadership and infused throughout the corporate culture, the more likely the organization will be to have implemented sound technical, structural, and procedural improvements.'<sup>107</sup>

#### Move from tangible to intangible property

Information has shifted from being a resource which is attached to physical media, such as paper records, books and CDs, to being a virtual resource with no physical manifestation.

This shift creates new theoretical challenges because of the differences between the nature of information and tangible assets such as land or other material possessions.<sup>108</sup> These differences have an impact on the way that property rights over information have developed and temper the degree of control that any business or individual has over information about them or which they have created.

#### Panel 5.5: Differences between tangible and intangible property

Private property rights over tangible goods are underpinned to a significant extent by the idea of a limited resource. It is this dimension of scarcity that drives the need for clear boundaries over use and exclusion. However, information in itself is not scarce. While the creation and dissemination of information may involve the use of scarce resources, information itself is what is termed a non-rival good. In other words, it can be enjoyed to an equal degree by multiple people at the same time. Sharing a piece of information with others does not usually degrade the quality of the information or deny the originator of the information the ability to use it at the same time. This is very different to a physical product, where the use of it by another party directly impinges on the owner's enjoyment of the good. As a result, the underlying justification for private property rights is weakened.

One of the key elements of property rights is the right to exclude others from accessing or using the resource. However, another characteristic of information is that it is often non-excludable in practice. Information can sometimes be excluded on the basis of the law, for example, it may be forbidden to share certain types of information with others. However, once it is released, it is difficult to exclude others from gaining access to it in practice. As a result, full property rights over information are challenging to enforce.

Many different people may also be involved in the capture, aggregation and dissemination of information with a variety of motives and potential gains from it. Where a business has invested resources to capture information about the location or public activities of an individual, both the business and the individual may have a legitimate interest in how the information is used. Therefore, rights may need to be shared among a number of different parties.

As a result, the best way of looking at information in legal terms is that in and of itself it is relatively inert and information cannot be 'owned' or 'stolen'. However, a number of the bundle of intellectual property rights, as well as statutorily created duties and rights, arise in relation to information.

It is also the case that the theoretical difficulties attached to owning information have had minimal impact in practice, as information has largely been attached to physical goods and has therefore been viewed as a tangible good for all intents and purposes. However, in the digital world, this is not the case at all. As a result, further thinking is needed on the implications of these differences and whether our understanding of the nature of digital information needs to evolve as a result.

<sup>107</sup> Mary Culnan and Cynthia Williams, 'How ethics can enhance organizational privacy: lessons from the Choicepoint and TJX data breaches', p685.

<sup>108</sup> Danny Quah, *Digital Goods and the New Economy*.

## Convergence between information regimes

Another challenge for the current rights framework is the growing overlap between personal information and intellectual property. This overlap affects businesses, as they typically have a wide spectrum of information that is sensitive or valuable and which comes from a variety of sources. Some of this information may constitute personal information. Some of it may constitute intellectual property. As a result, businesses need a coherent and consistent approach to information risks, based on the sensitivity and value of the information, regardless of its formal classification.

However, a feature of the regime of information rights today is that it contains two very distinct and separate areas of legal analysis and philosophical debate: rights over personal information and rights over intellectual property.

There are good historical reasons why these debates have been conducted largely in isolation from each other. Privacy was originally based on notions of physically protecting the home or person. It only became focused on information in the second half of the 20th century. Intellectual property, by contrast, focused on creative content such as books, or inventions. These two disciplines, therefore, appear to protect things that look and feel very different.

They also have different philosophical groundings. Privacy debates have often centred on philosophical or political arguments and privacy rights are an important part of the human rights framework. Intellectual property rights, though, are largely economic in nature and therefore the subject of very different debates.

However, as all pieces of information become digitised into bits and bytes, an address, a photograph and a music file all start to look very similar. The overlap is clearly seen in the development of creative content on the internet by individuals. The content of a blog is an example of creative content, which could fall within intellectual property notions. However, it may also contain substantial personal information that the writer wishes to share. Social networking profiles also contain a wide mix of personal information, such as activities and location, and intellectual property, such as photographs.

Furthermore, as businesses capture increasing amounts of information about customers or service users, personal information is becoming an increasingly important asset of any business. In many cases, it may be their most valuable piece of intellectual property and the key revenue driver.

This overlap has implications for debate and public policy options. For example, there is growing tension between the protection of personal information and intellectual property. As copyright infringements have become increasingly perpetrated by individual consumers in their home, pressure has grown to identify this type of activity by interrogating the records of internet service providers. However, the records of individual customers are potentially personal information and accessing them to report individuals to rights-holders could breach privacy rights. Priority has to be given to the protection of one type of information ahead of the other.

As a result, we need to consider the tensions between these different areas and increasingly look to develop more integrated thinking and policy solutions. This is echoed by Ian Hargreaves in his report on UK intellectual property laws, saying, 'questions of IP, privacy, and security are converging in ways that will, over time, present sharp challenges to the current legal framework.'<sup>109</sup>

## 5.5 Balance control and use of information

The third element for building business trust concerns the nature of the solutions which are developed. The social and legal environment around digital information needs to balance two key considerations:

- effective control over access to, and use, of digital information; and
- opportunities to generate value through its widespread use and dissemination.

How we resolve trade-offs between these elements in a variety of specific circumstances will have a significant influence on future business innovation through IT. Indeed, the different ways that this balance has been struck in the US and UK are sometimes cited as underlying factors which support the success of Silicon Valley and discourage similar innovation in the UK.

<sup>109</sup> Ian Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth*, p19.

### Panel 5.6: Encouraging innovation with IT

There are many factors which have enabled Silicon Valley to become the technology and software hub of the world. Many of these factors relate to access to capital, skills and a culture of risk-taking, coupled with high rewards for success. However, it is sometimes suggested that the more open legal environment regarding information rights plays a role in encouraging innovation in digital information.

Chapter 2 outlined the US approach to personal information, which is broadly market-based and libertarian. This compares with a European approach which is strongly regulated. The intellectual property regime of the US is also less restrictive than in the UK. In particular, the doctrine of fair use, which has not been adopted in the UK, enables limited reuse of material which is otherwise protected by copyright.

These differences raise the possibility that businesses which start up in the US have a significant advantage in how they can use a variety of digital information to build a successful business model.

In his report in 2011 on UK copyright laws which was commissioned by the government, Ian Hargreaves acknowledged that copyright law in the UK had been overtaken by technological change and was not enabling business and research communities to maximise their use of these technologies. While he rejected the adoption of the US fair use doctrine, he recommended implementing a number of specific exceptions to copyright laws to support greater use and commercial exploitation of information in some situations.

The need to balance control over information with the reasonable use and sharing of information reflects a long-standing debate in property rights theory more broadly.

### The theory of property rights

Rights to control access to resources, namely property rights, underpin a functioning market economy.

### Panel 5.7: Private property rights

Private property rights are usually described as a bundle of three core powers: to use the item, to exclude others from using it and to transfer it to a third party.<sup>110</sup>

There are strong economic justifications for property rights and there is little debate today that property rights underpin the functioning of a market economy. Although this was recognised by Adam Smith in the 18th century, the Property Rights school of economics started properly in the 1960s with economists such as Ronald Coase, Armen Alchian and Harold Demsetz.<sup>111</sup>

In economic terms, property rights provide clear boundaries over the exclusive use of resources. They enable individuals to form reasonable expectations about the behaviour of others regarding resources. As a result, property rights reduce the costs of transactions and thereby encourage markets to grow.

Property rights have also been justified by philosophers from the ancient Greeks, through the Enlightenment and on to the present day. The notion of private property is particularly connected with ideals of freedom and the ability of an individual to control his or her own destiny. Indeed, the American Revolution is often seen to be a revolution about the ownership of land, with the prime role of the government being to protect and preserve property.<sup>112</sup>

There are significant legal differences between land ('real estate' or 'real, heritable or immovable property') and movable property such as goods and chattels, to say nothing of intangible property such as intellectual property. Land titles are the strongest.

Property rights need to strike a happy medium which provides the degree of predictability and security that individuals and markets need to operate while also enabling the reasonable use and sharing of resources.

Where resources are subject to too little control, they risk being overused. This is known as the tragedy of the commons.

<sup>110</sup> Anthony Honoré, 'Ownership'.

<sup>111</sup> See for example Harold Demsetz, 'Towards a theory of property rights'.

<sup>112</sup> Paul Johnson, 'Freeholds and freedom: the importance of private property in promoting and securing liberty'; O. Lee Reed and E. Clayton Hipp, 'A "Commonest" manifesto: property and the general welfare'.

### Panel 5.8: The tragedy of the commons

A commons is property which is held for the benefit of everyone and where there are no restrictions on how individuals can use the resource, for example a field where any individual can allow their cattle to graze freely. While no longer a typical way to allocate property rights, commons do still exist in places such as Forest of Dean in the UK.

In his article 'The tragedy of the commons' (1968), Garret Hardin highlights the dangers of such a system of property rights, especially where the resource is limited. Using the example of a field with no limits on grazing, he argues that every individual will want to maximise the value of the commons to him or her and therefore will benefit from adding more cattle into the field to graze. The field, though, is ultimately a limited resource and will quickly become over-grazed and ruined. However, while each individual gets the full benefit of adding an extra animal on to the land, the impact of the failure is shared among all of the community.

As a result, no individual is encouraged or rewarded to look after the field or voluntarily limit his or her use of it for the good of everyone in the long term. As Hardin describes:

'Each man is locked into a system that compels him to increase his herd without limit – in a world which is limited... Freedom in a commons brings ruin to all.'<sup>113</sup>

However, property rights can go too far. As property rights are a bundle of rights, rather than a single right, it is possible to separate different aspects of this bundle and sell them to different people. We see this most obviously in renting agreements, where the owner of the resource sells their right to use it and exclude others from using it for a period of time.

Where property rights are so extensive and fragmented between many different individuals, it can lead to deadlock and a failure to use the resource at all. This is known as the tragedy of the anti-commons.

### Panel 5.9: The tragedy of the anti-commons

In his article, 'The tragedy of the anti-commons: property in the transition from Marx to markets' (1998), Michael Heller describes how the number of organisations with rights over shop properties in Russia led to gridlock, leaving shops empty and leading to the widespread use of informal street kiosks in their place.

He noticed that, while the market economy was growing and more goods were becoming available to purchase, this was not translating into successful shops. Indeed, many of Moscow's shop-fronts remained empty. Instead, kiosks sprung up on the pavement directly in front of the empty shop-fronts to be used as trading posts. His explanation for this development was based on the way that authorities were allocating new private property rights over the shops.

Heller highlights an inverse correlation in the way that property rights had transitioned from a socialist environment to a market one. Where property had been highly protected under the socialist system, and therefore transitioned with extensive rights over its use, it had not performed well in the market economy. By contrast, property that had fewer rights around its use, such as residential property, was being traded successfully.

As a result, there were many individuals or government bodies with a right to veto the use of property for a particular purpose, but no-one had a sufficient set of rights which enabled them actually to use the shop property. He identified up to six rights that could be held by multiple rights-holders over a piece of property, including rights to sell, lease, receive revenue from the sale or lease, determine use and occupy. Unless all the parties could agree, the property remained unused.

In the context of digital information, there are risks similar to both the commons and anti-commons:

- where information is over-used or shared without limits, the value of intellectual property may be diminished and individuals may become increasingly reluctant to share their personal information with others; and
- where there are very tight controls over access to information, it may become impossible to innovate through its use, losing out on a wide range of possible benefits

<sup>113</sup>Garret Hardin, 'The tragedy of the commons', p1244.

As a result, we need to understand the trade-offs between these two extremes and build solutions which balance them in the best possible way.

## 5.6 Create supportive institutions

The fourth element of building trust is creating institutions which can foster understanding of different perspectives, encourage debate and develop a variety of practical solutions.

### Build understanding of different perspectives

One of the features of debates about information rights is that they can involve deeply opposing interests and philosophical beliefs. As a result, we need to create institutions that involve the spectrum of interests and beliefs and can foster understanding between different groups.

This includes a wide range of participants, including:

- the technology industry;
- businesses which are using and exploiting IT and digital information;
- governments, in their capacity as information users and IT buyers;
- regulators and legislators;
- individuals such as consumers, service users, citizens and shareholders;
- think tanks and pressure groups; and
- academics.

While all participants have the same ultimate goal of maximising the economic and social benefits of technology, they may have very different visions of what this looks like and the elements which are needed to build trust. As a result, institutions, such as the Internet Governance Forum, can play an important role in bringing stakeholders together and building dialogue.

#### Panel 5.10: The Internet Governance Forum

The Internet Governance Forum is a forum where a wide range of stakeholders come together and debate issues surrounding the internet. Participants include governments, businesses, academics and non-governmental organisations working in this area. It is convened under the auspices of the United Nations and holds an annual meeting.

The 2011 meeting was held in Nairobi, Kenya and sessions were arranged around themes including:

- managing critical internet resources;
- access and diversity;
- security, openness and privacy; and
- internet governance for development.

The forum's broad membership goes well beyond traditional, state-dominated institutions. It has encouraged the development of local or regional forums, which have been particularly effective in promoting the internet in developing countries. It has also enabled open discussions on a wide range of topics and built understanding of different perspectives.

### The need for international cooperation

One of the major economic consequences of IT is that it enables extensive globalisation and international communication. Many businesses now operate with customers, employees and suppliers from many countries. As a result, they may be managing a highly complex compliance environment. A business also needs to understand and manage multiple expectations and behaviours, which may display cultural differences.

Furthermore, cyber criminals work across national boundaries, with many organised gangs outsourcing activities to specialist coders around the world. The use of infected computers and botnets means that computers can be used from anywhere in the world to launch attacks on businesses or individuals. This international dimension makes it increasingly difficult for local law enforcement agencies to identify criminals and prosecute them effectively. While there is some

international cooperation and intelligence sharing, such activities tend to be inconsistent. Indeed, with suspicions of state sponsorship around some cybercrime activities, cross-jurisdictional action is difficult to achieve in many cases.

As a result, institutions need to operate at a number of different levels.

- There will always be a need for national institutions which reflect the priorities and will of individual states, as well as local cultures.
- Regional institutions, for example at the EU level, can play an important role in bringing groups of countries together and building regional cooperation.

There is also a growing need to build institutions and find approaches, such as common principles, which can operate across national and regional boundaries. As well as the Internet Governance Forum, there are also international institutions to support formal policy frameworks, such as the Trade Related Aspects of Intellectual Property Rights (TRIPS) part of the World Trade Organisation. However, further thinking is required on how institutions can support global cooperation more effectively.

Institutions also need to include three types of participants in particular:

- legislators and regulators;
- the technology industry; and
- individual consumers and citizens.

In the remainder of this chapter, we consider the role of each of these participants. However, they are likely to have very different perspectives, interests and priorities. As a result, finding agreement remains difficult in many cases and a variety of practical solutions are likely to be required.

### The role of legislators and regulators

The legal and regulatory frameworks around information rights provide predictability and confidence in the actions of businesses and individuals around information. Consequently, laws and regulation underpin the business and social environment and are hugely important to building trust in business behaviour.

However, regulators and lawmakers face significant challenges in developing good solutions around digital information because of the nature of good regulation.

#### Panel 5.11: Requirements for good regulation

ICAEW has developed a framework for good regulatory practice based on robust evidence, which outlines the key steps which should be taken in developing new regulation:<sup>114</sup>

- making the case for change;
- options development;
- evaluation of options;
- planning implementation;
- mitigating remaining problems;
- implementation; and
- evaluation of results.

All of these steps need to be supported by consultation and engagement with those who will be affected by the regulation. Good regulation, therefore, by its very nature, takes time to develop.

Given the pace of technological and business change, this is likely to mean that regulation is rarely at the leading edge of business practice and will usually be well behind the curve of innovation.

In response to these challenges, law makers and regulators need to develop proposals which are, as far as possible:

- platform-neutral and not tied to specific technologies; and
- flexible and applicable to a wide range of businesses models.

<sup>114</sup> ICAEW, *Measurement in Financial Reporting*.

However, regulators are unlikely to be best placed to understand fully the new possibilities offered by IT. Many of the issues highlighted in this report are nuanced and may not be well served by heavy or blunt regulation. As a result, it is unrealistic to look at the law and formal regulation to provide definitive solutions to many of the challenges we raise. They need to be supplemented by a range of other, less formal measures.

## The role of the technology industry

Industry standards can be a good supplement to formal legal obligations. Such measures can be more flexible and responsive to the needs and dynamics of specific industries.

There are some relatively successful areas of industry standards in IT security, such as PCI-DSS. However, the success of such schemes in practice is mixed. Informal approaches to regulation have often been seen as self-serving, providing few practical benefits to consumers in practice. The approach to privacy in the US, for example, is coming under increasing pressure by lawmakers given the perceived lack of consumer protection that it embodies. However, the maturity and complexity of the technology industry can make it difficult to develop effective alternatives to formal regulation.

### Panel 5.12: Standards and informal regulation in the technology industry

Effective standards and informal regulation are driven by the common interests of the participants. Frequently, businesses may be keen to avoid costly formal regulation. They may develop standards to build trust and confidence in an industry as a whole to discourage cowboy behaviour and support industry growth.

However, the complexity and fragmentation of the IT industry makes this difficult to achieve in the context of privacy and intellectual property. There are many different players in the value chain who have diverse interests. For example, technology companies looking to build business models around the sharing of information content are likely to have very different interests to content providers. Implementing technical solutions to promote individual privacy may have limited value to a business which wants to use personal information to generate revenue.

Furthermore, the sector is relatively young. The markets are extremely competitive and heavily driven by network effects, both in terms of technology standards and content. In many of these sectors, there is substantial first-mover advantage, with businesses often driven by the need to gain users as quickly as possible. All of these factors are likely to deter businesses from cooperating with one another to develop industry-based solutions.

## The role of individual consumers and citizens

Social norms and expectations play a central role in building greater predictability for businesses. They also underpin market pressures on businesses to behave properly to one another as well as to their customers and employees. Where businesses fail to observe social norms or expectations, they may be punished in the marketplace, even if their actions are legal.

### Panel 5.13: Building effective market pressures

Market pressures are based on customer choice. Where customers can go elsewhere, businesses are encouraged to behave well so as to keep their loyalty and custom. In the US, substantial reliance is placed on the market to drive business behaviour around the use of personal information. In Europe, market pressures have supported the more formal regulatory regime, especially in the UK. Market pressures, and the behaviour of consumers, can also drive intellectual property policies and help a business to determine what intellectual property they should charge for and what they should freely release.

Market pressures are supported by a variety of factors. There needs to be real choice in the provision of services and therefore creating competitive markets is a key step. There needs to be transparency so that customers can make informed choices about different businesses. There also needs to be a degree of consensus between customers around expected business behaviour and standards so that there is a critical mass that will impact businesses.

However, there are limits to the effectiveness of market pressures. In many cases, consumers may place a low priority on information security and privacy compared to cost and service quality. As a result, even where businesses exhibit poor behaviour around information, customers may be willing to overlook it in favour of other factors. Also, diversity of opinions can make market pressures quite fragmented in practice.

There is significant scope for policy-makers to use information to enhance market pressures in the context of privacy and information security. For example, there is often little public visibility of business processes in these areas and transparency can potentially be increased through regulation or voluntary initiatives in corporate reporting.

However, there is also a broad spread of consumer attitudes and expectations around how businesses should behave around IT and digital information, which inevitably weakens market pressures. Consequently, public debate can help to build more consistent and effective market pressures on businesses.

## 5.7 Summary

New technology is a central part of economic development. However, transformation in economic possibilities through new technology often creates social tensions and new questions in parallel. Unless we recognise and address the social challenges related to digital information, there is a risk that opportunities to use it are missed.

Trust is an important feature which underpins the use and value of new technologies and therefore can support the development of a digital economy. Businesses can build trust at an individual level by implementing good practices. However, good practices need to be underpinned by clear social expectations and legal obligations. We identify four essential elements to building broader trust around digital information.

**Recognise and debate issues.** Regulators, law makers and the technology industry have a major role to play. However, all businesses are affected by some of the issues raised in this report, as are all individual consumers and citizens. Therefore, debates need to engage broadly across all sections of society in order to take account of different interests and perspectives.

**Develop new theoretical thinking.** While technology is the direct cause of the difficulties outlined in the report, it is radical changes to the economics of information which are at the heart of the social tensions. Therefore, we need to encourage a variety of new thinking which is rooted in the economics of digital information.

**Balance control and use of information.** There needs to be clear rights over information to enable parties to form expectations about its use and protection. However, this control needs to be balanced with the ability of different parties to use and share information for a wide range of benefits.

**Create supportive institutions.** A variety of institutions are needed which can address this broad range of issues and develop robust and flexible solutions. Institutions need to include many participants, including regulators, businesses, individual consumers and the technology industry and promote common approaches, as far as is possible.

Although each of these elements is essential, they are also fraught with difficulty which may limit realistic progress. Academic research can play an important role in developing deeper understanding of the challenges of the digital environment and supporting each of these elements.



# APPENDIX – AREAS FOR RESEARCH

## A.1 The role of academic research

This report maps out a wide range of business practices, as well as the established social and legal environment around information. However, more needs to be done to build trust around digital information and academic research has a crucial role to play.

In order to improve security measures in practice, businesses may benefit from sharing their experiences around information practices through networks of peers or other informal mechanisms. However, businesses may also be reluctant to share information about security failures or vulnerabilities openly. As a result, there is a clear role for academic research in improving understanding of how businesses seek to implement security measures in practice and how successful or otherwise they are in doing so. Research can preserve individual anonymity while enabling greater sharing of knowledge and experience.

Objective evidence is also central to building an approved social and legal framework around digital information. Without robust evidence to support decision making, there is a significant risk of hasty or ill-thought through actions which do not achieve their ultimate objectives. Although this report has highlighted a wide range of research, there continues to be limited robust evidence on many of the topics discussed. In some cases, there is little or no research at all.

## A.2 Sharing business experience and knowledge

There are two distinct approaches that can be taken to academic research on business practices.

Quantitative analysis interrogates statistical data with the aim of finding correlations between different data elements. Such correlations can then provide evidence to support or challenge specific propositions. In the context of business practices, quantitative research could consider the preconditions for good business performance or the consequences of particular actions, for example the decrease in share price when a business discloses a major security breach.

By contrast, case studies aim to develop deep understanding of organisational practices, structures or capabilities. By looking at a single organisation, or small group of organisations, they typically examine a particular event or series of events in detail, identify reasons for success or failure and suggest lessons which may be relevant for others. As such, they can provide valuable insights on the implementation of practices and the factors that may influence success. Case studies are therefore likely to be of more practical use to individual businesses.

### Possible research topics

There has been limited research undertaken into information security practices in businesses and consequently there is substantial scope for more research, especially through case studies.<sup>115</sup> This could include building detailed understanding of organisational practices and influences, developing frameworks for business thinking about security requirements and identifying key skills and capabilities that a business may need.

Linked to research on information security practices is research on corporate policies around information, and how businesses can effectively align practices with policies and business objectives. Given the likely importance of gaining organisational commitment to security aims and practices, this is an area in which further research would be welcome.

There is also very little research on specific practices relating to personal information and intellectual property. As a result, there is scope for developing a better understanding of organisational processes and the formation of specific policies in these areas.

<sup>115</sup> For an overview of the different approaches to information security research, see Gurpreet Dhillon and James Backhouse, 'Current directions in IS security research: towards socio-economic perspectives'.

## Panel A.1: Suggested research topics on information practices

### Information security practices

- How do businesses define their security priorities?
- What tools do management use to justify security investments? How can these tools be refined?
- How do businesses identify data assets and compare their importance and sensitivity?
- How do businesses encourage communication of security objectives and priorities?
- How are information risks integrated into the wider business risk framework?
- What influences the development of a security-conscious culture?
- What skills and capabilities are needed to implement security measures effectively?
- How can businesses understand and manage third party supplier information risks?
- What techniques do businesses use to manage and authenticate identities?
- What is the role of audit and assurance activities in information security?

### Corporate information policies

- How do businesses align information policies with business objectives? How can businesses improve their ability to do this?
- What are the key drivers to developing corporate information policies? And how do businesses balance different drivers?
- What organisational structures support the effective formation of policies?
- How do businesses integrate thinking about the benefits and risks of information and IT?
- At what stage are information policies considered in the development of new systems or processes within a business?

### Privacy practices

- To what extent is privacy becoming a value-enhancing component of a brand?
- How do businesses manage the international complexities of privacy regulation and attitudes?
- What organisational structures support the effective management of privacy issues?
- What are the benefits of adopting a 'privacy by design' approach?
- How have privacy impact assessments been used effectively?
- How do businesses manage communication with consumers on the treatment of their personal information?
- What is the role of privacy audit and assurance activities in building trust?
- What is the business case of privacy-enhancing technologies?
- How do businesses manage customer concerns about privacy failures?
- How do businesses collect and manage consent to handle personal information?
- How do businesses innovate in an environment of changing and conflicting customer demands?
- How do individuals obtain redress for breaches or misuse of personal information?

### Intellectual property practices

- How do businesses develop policies around what information to charge for and what to give away free?
- What alternative business models are developing to support the exploitation of information content?
- How do businesses build a culture which discourages employees from stealing intellectual property?
- How effective are digital rights management systems in protecting intellectual property?

## A.3 Supporting collective actions

We also suggest some themes for further research to support the development of a social and legal environment to meet the challenges of digital information. These are based on the four elements of building business trust.

### Theme 1: Recognise and debate issues

Researchers can help to build recognition and debate by defining the nature and scope of issues. They can also increase knowledge around the size and magnitude of problems to help to focus attention on areas of greatest need.

There are important issues, for example, around the scope of protection for personal information. These include questions such as:

- What information should be classified as personal information which needs to be protected? This is especially important given the growing power of aggregation techniques and the collection of vast amounts of public and location data.
- What is the role and nature of consent in the online environment in particular? To what extent is consent an adequate response to extensive data gathering and use by businesses and governments? Furthermore, what constitutes 'informed consent' in this environment?
- How do we make sense of conflicting attitudes and inconsistent behaviour regarding individuals' personal information? How do we take account of the potential generational differences in this area?

Regarding intellectual property, there are many outstanding questions on the nature of the economic harm being caused by breaches of intellectual property rights. As with personal information, there are also questions around changing attitudes, especially among younger generations.

Finally, we need to improve our understanding of the magnitude of security breaches and the impact on businesses, individuals and the economy as a whole. There is also a need to understand better the drivers towards individual and business behaviour around protecting their valuable information in order to build policies which change behaviour and improve security in practice. How can we get individuals to care more about the protection of their information? And how can we best drive business behaviour in this regard?

### Theme 2: Develop new theoretical thinking

New theoretical thinking on information rights is needed to support the growing digital economy. In particular, researchers and policy-makers may need to consider the impact on privacy and intellectual property rights of an abundance of information which is low cost but valuable.

There is scope to expand the field of information ethics and examine whether new ethical norms will help to develop greater trust. This could support both individuals and business decisions about the use and sharing of digital information, and includes a range of questions on underlying moral considerations concerning our treatment of the sensitive or valuable information of others, for example:

- the ethics of sharing information about other individuals on social networking sites;
- ethical considerations for employees in activities such as using customer personal information and accessing the intellectual property of the business; and
- the role of ethics in promoting good practices in individual businesses.

New thinking is also needed on the nature of intangible property and how it can be owned and controlled.

Finally, more integrated thinking is needed between information security, personal information and intellectual property. While there will always be some types of information which remain clearly personal information or intellectual property, we see a growing 'grey area' of information that is both personal data and intellectual property

As a result, we suggest that more integrated thinking is required which, for example:

- identifies and considers conflicts or contradictions between policies in each area; and
- considers the long-term implications of the convergence of information types.

### Theme 3: Balance control and use of information

Researchers can build a stronger evidence base to help policy-makers balance the control and use of information and understand both the short and long-term impact of strengthening or weakening information rights

Information rights today are based on a complex balance between the benefits of sharing information and the benefits of controlling access to it. We have highlighted the competing claims of, for example, transparency, surveillance and privacy interests or the interests of information producers and information consumers. As the opportunities to generate value from information continue to expand at a tremendous pace, these decisions will become increasingly complex and contentious.

Business and public policy decisions need to be based on robust evidence around the benefits and risks of using information in particular ways. However, there continues to be a lack of evidence to inform decision makers on many of these difficult decisions. In many cases, there is little or no objective evidence.

Consequently, there is substantial scope for research in many areas to support policy decisions, such as the long-term risks attached to the use of personal information and the economics of strengthening or loosening intellectual property rights. Research could build knowledge and understanding in a variety of areas.

- What are the specific benefits of controlling personal information and intellectual property, and what are the risks attached to failures to protect information adequately?
- What are the specific benefits of enabling widespread use and sharing of personal information and intellectual property, and what opportunities would be lost by preventing such access?
- What are the frameworks that can be used to balance these different interests? While economics can be used to compare the costs and benefits of different scenarios, there are also a wide range of social interests involved. Therefore, theories of justice and human rights, among others, can play an important role in weighing up different interests.
- How do decision makers compare the various benefits and risks in specific situations?

All of these research areas are made more complex by the variety of different stakeholder interests involved. The benefits and risks for individual consumers and citizens, for example, are likely to be very different to those for businesses. How do we decide which interests prevail in any given situation? And when does the wider public interest trump the interests of individual stakeholders?

### Theme 4: Create supportive institutions

Finally, researchers also need to develop ideas about the creation of relevant institutions. Regulation can only be one element of a wider social and legal framework and greater understanding is needed of potential industry initiatives as well as consumer pressures and social norms.

We suggest, for example, that researchers could contribute new thinking about institutions and frameworks which would be effective at an international level. This thinking could cover:

- how international frameworks and institutions would operate and relate to national ones;
- how to understand and take account of cultural differences; and
- how to recognise the different economic needs of developed and developing economies.

Researchers can also assess the implications of change for different options. This includes developing a detailed understanding of the current environment, how it operates and the problems that the new actions are aiming to address. Researchers could build deeper understanding of, for example:

- the operation of regulation such as data protection laws and breach notification laws;
- the mechanics, drivers and benefits of industry cooperation in different areas; and
- actions that would better inform customer choices.

## A.4 Research challenges

While there is substantial scope for more research, we also need to recognise that researchers face a series of challenges in developing evidence around information security and rights.

### Research disciplines

Questions on the legal and social environment cover a broad range of academic disciplines. As a result, we have drawn on research from many different fields in developing this report.

There is substantial research into technical solutions across all three areas of security, privacy and intellectual property. For example, the IT research community, drawn largely from computing and engineering schools, focuses on software development techniques to develop new insights in areas such as cryptography or privacy-enhancing technologies.

The second major research discipline is information systems (IS), which intersects IT issues with broader management, social and economic research. For example, there is growing research in the IS field on the notion of online trust, the behavioural economics of personal information and the implementation of security practices in businesses.

The accountancy discipline has a research community which is particularly interested in information controls and security, and the impact of IT on wider business risk management.

We have drawn on philosophical, political and economic theory to understand the basis for rights over information and the underlying debates about the appropriate strength of information rights. There is also a small but growing field of information ethics which considers the moral aspects of information use and the impact of IT.

Finally, law schools have deep expertise in the areas of privacy and intellectual property. By focusing on legal rights and obligations in these areas, legal researchers provide rich analysis around the objectives and scope of laws, as well as problems in enforcing them.

The range of disciplines involved makes it difficult to integrate ideas and establish what research really tells us. While we recognise the institutional barriers that need to be overcome, further multi-disciplinary research would be helpful.

### Data challenges

It is also difficult to find good quality data to support research projects. Good research is based on robust and clean data, and in many cases, there is a dearth of publicly available information which can be used in research. Data about security practices or failures is not generally published and therefore researchers may have to look for proxies or create their own data sets through questionnaires.

The success of case studies depends on substantial organisational access which may be difficult for researchers to agree, especially in sensitive areas such as security. Case studies are often criticised for being subjective and subject to the bias of the subjects and researchers. Given the specific context of each case study, it can also be difficult to develop general learning points from them.

New regulations such as breach notification laws can help to make some information about security failures public and therefore can support research in these areas. However, in order to improve understanding of business practices, businesses need to make more data available for research. Greater cooperation between industry and academia is therefore needed to support relevant research projects.

# ACKNOWLEDGEMENTS

ICAEW is grateful to the following commentators for sharing their knowledge and experience of the topics with us, providing helpful reactions in a personal capacity to the development of the ideas in this report or commenting on drafts of it.

Martin Abrams  
Richard Anning  
Nina Barakzai  
Jennifer Barrett  
Caspar Bowden  
David Boyes  
Louis Branz  
Ian Brown  
John Court  
Mary Culnan  
Gurpreet Dhillon  
Gus Hosein  
Anthony House  
Richard Kemp  
Dapo Ladimeji  
Mike Linksvayer  
Alastair MacWillson  
Siani Pearson  
Rufus Pollock  
Chris Potter  
Dick Price  
John Soma  
Paul Steinbart  
Toby Stevens  
Steve Sutton  
Scott Taylor  
Richard Thomas  
Bridget Treacy  
Kevin Trilli  
Henry Wallis

None of the commentators should be assumed to agree with the views expressed in this report, and they are not responsible for any errors or omissions.

The report's principal authors are Kirstin Gillon and Robert Hodgkinson.

# BIBLIOGRAPHY

- Acquisti, Alessandro, Friedman, Allan and Telang, Rahul, 'Is there a cost to privacy breaches? An event study', *Proceedings of the International Conference on Information Systems*, 2006.
- Acquisti, Alessandro and Grossklags, Jens. 'What can behavioral economics teach us about privacy?' in Acquisti, Alessandro, De Capitani di Vimercati, Sabrina, Gritzalis, Stefanos and Lambrinouidakis, Costas (eds.), *Digital Privacy: Theory, Technologies and Practices*, Boca Raton, Florida: Auerbach Publications, 2007, pp363-377.
- Anderson, Chris, *The Long Tail: Why the Future of Business is Selling Less of More*, New York: Hyperion, 2006.
- Anderson, Ross, 'Why information security is hard – an economic perspective', *Proceedings of the 17th Annual Computer Security Applications Conference*, 2001, pp358-365.
- Andrews, Amanda, 'iPad to boost 2011 IT spend to \$3.6 trillion', *The Telegraph*, 30 March 2011.
- Angwin, Julia, 'The web's new gold mine: your secrets', *Wall Street Journal*, 30 July 2010.
- Aristotle, *Politics*, translated by Lord, Carnes, Chicago: University of Chicago Press, 1984.
- Ball, Kirstie and Wood, David Murakami (eds.), *A Report on the Surveillance Society for the Information Commissioner*, Wilmslow, Cheshire: ICO, 2006.
- Bassi, Alessandro, Hitachi Europe and Horn, Geir, *Internet of Things in 2010: Roadmap for the Future*, Brussels: European Commission Information Society and Media/ EPoS5, 2008.
- BBC News, 'The cyber raiders hitting Estonia', 17 May 2007.
- BBC News, 'UK's families put on fraud alert', 20 November 2007
- BBC News, 'Twitter user in bid to break super-injunctions', 9 May 2011.
- Benkler, Yochai, 'Intellectual property and the organization of information production', *International Review of Law and Economics*, vol 22, 2002, pp81-107.
- Besen, Stanley M. and Raskind, Leo J., 'An introduction to the law and economics of intellectual property', *Journal of Economic Perspectives*, vol 5, no 1, 1991, pp 3-27.
- Bilton, Nick, 'Price of Facebook privacy? Start clicking', *New York Times*, 12 May 2010.
- Bolster, Paul, Pantalone, Coleen H. and Trahan, Emery A., 'Security breaches and firm value', *Journal of Business Valuation and Economic Loss Analysis*, vol 5, issue 1, 2010, article 1.
- Bradshaw, Tim, 'Spotify on song with 1m paying subscribers', *Financial Times*, 8 March 2011.
- Brandeis, Louis, 'What publicity can do', *Harpers Weekly*, 20 December 1913.
- British Computer Society, *The British Computer Society's Response to the Ministry of Justice on the 'Data Sharing Review' by Richard Thomas and Dr Mark Walport*, 2008.
- Brynjolfsson, Erik and Hitt, Loren, 'Computing productivity: firm level evidence', *The Review of Economics and Statistics*, vol 85, no 4, 2003, pp793-808.
- Carlson, Nicholas, 'Warning: Google Buzz has a huge privacy flaw', *Business Insider*, 10 February 2010.
- Cavoukian, Ann, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation*, Ontario: Information and Privacy Commissioner/Ontario, 1999.
- Cavusoglu, Huseyin, Mishra, Birendra and Raghunathan, Srinivasan, 'A model for evaluating IT security investments', *Communications of the ACM*, vol 47, no 7, 2004, pp87-92.
- Cavusoglu, Huseyin, Mishra, Birendra and Raghunathan, Srinivasan, 'The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers', *International Journal of Electronic Commerce*, vol 9, no 1, 2004, pp69-104.

- Chesbrough, Henry, *Open Innovation: The New Imperative for Creating and Profiting from Technology*, Boston: Harvard Business School Publishing, 2003.
- CIBER, *Copycats: Digital Consumers in the Online Age, a CIBER Report for the Strategic Advisory Board for Intellectual Property Policy*, London: CIBER, 2009.
- Collins, Brian and Mansell, Robin, *Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews*, commissioned by the UK Office of Science and Technology as part of a Foresight project, 2004.
- Connors, Emma, 'Up close and too personal', *The Weekend Australian Financial Review*, 3-4 September 2011, pp52-53.
- Craig, Cameron, 'Data privacy: when will watchdog ICO get its teeth into private sector audits?' *silicon.com*, 28 Jul 2011.
- Culnan, Mary J., 'Protecting privacy online: is self-regulation working?' *Journal of Public Policy & Marketing*, vol 19, no 1, 2000, pp20-26.
- Culnan, Mary J. and Williams, Cynthia Clark, 'How ethics can enhance organizational privacy: lessons from the Choicepoint and TJX data breaches', *MIS Quarterly*, vol 33, no 4, 2009, pp673-687.
- Davis, Philip M., Lewenstein, Bruce V., Simon, Daniel H., Booth, James G. and Connolly, Matthew J.L., 'Open access publishing, article downloads, and citations: randomised controlled trial', *British Medical Journal*, vol 337, 2008, article 568.
- Demsetz, Harold, 'Towards a theory of property rights', *American Economic Review*, vol 57, no 2, 1967, pp347-359.
- Detica, *The Cost of Cyber Crime: a Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office*, Guildford: Detica Ltd, 2011.
- Dhillon, Gurpreet and Backhouse, James, 'Current directions in IS security research: towards socio-economic perspectives', *Information Systems Journal*, vol 11, 2001, pp127-153.
- Dhillon, Gurpreet and Torkzadeh, Gholamreza, 'Value-focused assessment of information system security in organizations', *Information Systems Journal*, vol 16, 2006, pp293-314.
- Enterprise Privacy Group, *Privacy by Design: an Overview of Privacy-Enhancing Technologies*, 2008.
- Epstein, Richard A., 'The Property Rights Movement and intellectual property: a response to Peter Menell', *Regulation*, Winter 2008, pp58-63.
- European Commission Justice Directorate-General, 'European Commission sets out strategy to strengthen EU data protection rules', press release, 4 November 2010.
- Eysenbach, Gunther, 'Citation advantage of open access articles', *PLoS Biology*, vol 4, no 5, 2006, pp692-698.
- Federal Trade Commission, 'FTC charges deceptive privacy practices in Google's rollout of its Buzz social network', press release, 30 March 2011.
- Floridi, Luciano, 'The information society and its philosophy: introduction to the special issue on "The philosophy of information, its nature and future developments"', *The Information Society*, vol 25, no 3, 2009, pp153-158.
- Fussell, Jim, 'Group classification on national ID cards as a factor in genocide and ethnic cleansing', *Seminar Series of the Yale University Genocide Studies Program*, 15 November 2001.
- Gobry, Pascal-Emmanuel, 'What is the freemium business model?' *Business Insider*, 8 April 2011.
- Goodyear, Marilu, Goerdel, Holly T., Portillo, Shannon, and Williams, Linda, *Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers*, Washington DC: IBM Center for the Business of Government, 2010.
- Gordon, Lawrence A. and Loeb, Martin P., 'Return on information security investments: myths vs. realities', *Strategic Finance*, November 2002, pp26-31.
- Grant, Jeremy, 'Financial chiefs hit out at Sarbox costs', *Financial Times*, 7 June 2007.
- Grayson, Kent, Johnson, Devon and Chen, Der-Fa Robert, 'Is firm trust essential in a trusted environment? How trust in the business context influences customers', *Journal of Marketing Research*, vol XLV, April 2008, pp241-256.
- Green, Matthew, 'Napster opens Pandora's box: examining how file-sharing services threaten the enforcement of copyright on the internet', *Ohio State Law Journal*, vol 63, 2002, pp799-819.

Hall, Bronwyn H., 'Open innovation and intellectual property rights – the two-edged sword', *Japan Spotlight*, Jan/Feb issue, 2010, pp18-19.

Handke, Christian, *The Economics of Copyright and Digitisation: A Report on the Literature and the Need for Further Research*, London: Strategic Advisory Board for Intellectual Property Policy, 2010.

Hardin, Garrett, 'The tragedy of the commons', *Science*, vol 162, 13 December 1968, pp1243-1248.

Hargreaves, Ian, *Digital Opportunity: A Review of Intellectual Property and Growth*, 2011.

Healey, Thomas J., 'Sarbox was the right medicine', *Wall Street Journal*, August 9 2007.

Heller, Michael, 'The tragedy of the anti-commons: property in the transition from Marx to markets', *Harvard Law Review*, vol 111, no 3, 1998, pp621-688.

HM Government, *Making Open Data Real: A Public Consultation*, 2011.

Honoré, Anthony M., 'Ownership' in Guest, A.G. (ed.), *Oxford Essays in Jurisprudence*, Oxford: Oxford University Press, 1961.

House of Lords Science and Technology Committee, *Personal internet Security, 5th Report of Session 2006–07*, London: The Stationery Office Limited, 2007.

HP, *HP Global Master Privacy Policy*, available online at the HP Global Citizenship Center.

Hunton & Williams Centre for Information Policy Leadership, *Data Protection Accountability: The Essential Elements*, London/New York: Hunton and Williams CIPL, 2009.

Hunton & Williams Centre for Information Policy Leadership, *Demonstrating and Measuring Accountability, a Discussion Document – Accountability Phase II, the Paris Project*, London/New York: Hunton and Williams CIPL, 2010.

Huston, Geoff, 'The ISP: the uncommon carrier', *The Internet Protocol Journal*, vol 5, no 3, September 2002, pp23-27.

ICAEW, *Digital Reporting: A Progress Report*, London: ICAEW, 2005.

ICAEW, *Assurance Reports on Internal Controls of Service Organisations Made Available to Third Parties*, Technical Release AAF 01/06, London: ICAEW, 2006.

ICAEW, *Measurement in Financial Reporting*, London: ICAEW, 2006.

ICAEW, *Assurance Reports on the Outsourced Provision of Information Services and Information Processing Services*, Technical Release ITF 01/07, London: ICAEW, 2007.

ICAEW, *Measuring IT Returns*, London: ICAEW, 2008.

ICAEW response to the EC consultation *Early Challenges Regarding the "Internet of Things"*, 27 November 2008.

ICAEW, *Information Security – An Essential Today, a guide to ISO/IEC 27001 and ISO/IEC 27002 for Business Managers*, London: ICAEW, 2009.

ICAEW, *Cloud Computing: A Guide for Business Managers*, London: ICAEW, 2010.

ICAEW, *Glossary of IT Security Terms*, London: ICAEW, 2011.

ICAEW, *Dealing with Internet Security Threats*, London: ICAEW, 2011.

ICAEW, *Information Security Myths and Realities Revisited 2011*, London: ICAEW, 2011.

Information and Privacy Commissioner/Ontario and Deloitte & Touche, *The Security-Privacy Paradox: Issues, Misconceptions and Strategies*, 2003.

Information Commissioner's Office, *Privacy Impact Assessment – An Overview*, online resource.

Information Commissioner's Office, *What Price Privacy? The Unlawful Trade in Confidential Personal Information*, Wilmslow, Cheshire: ICO, 2006.

Information Commissioner's Office and the Enterprise Privacy Group, *Privacy by Design*, Wilmslow, Cheshire: ICO, 2008.

Information Commissioner's Office, *Data Protection – Protecting People, A Data Protection Strategy for the Information Commissioner's Office*, Wilmslow, Cheshire: ICO, 2009.

Information Commissioner's Office, *The Privacy Dividend: The Business Case for Investing in Proactive Privacy Protection*, Wilmslow, Cheshire: ICO, 2010.

Information Commissioner's Office, *Data Sharing Code of Practice*, Wilmslow, Cheshire: ICO, 2011.

- Information Commissioner's Office , 'UK businesses must 'wake up' to new EU law on cookies, Information Commissioner warns', press release, 8 March 2011.
- International Association of Privacy Professionals, *A Call for Agility: The Next-Generation Privacy Professional*, York, ME: IAPP, 2010.
- Internet Advertising Bureau, *Your Online Choices, a Guide to Online Behavioural Advertising*, available online.
- Jackson, Todd, 'A new Buzz experience based on your feedback', *The Official Gmail Blog*, 13 February 2010.
- Jefferson, Thomas, 'Letter to Isaac McPherson, Monticello, August 13, 1813' in Lipscomb, A. (ed.), *The Writings of Thomas Jefferson XIII*, 1904.
- Johnson, Bobbie, 'Privacy no longer a social norm', *The Guardian*, 11 January 2010.
- Johnson, Paul, 'Freeholds and freedom: the importance of private property in promoting and securing liberty', *Economic Affairs*, vol 28, no 4, December 2008, pp32-35.
- Jorgenson, Dale W. and Vu, Khuong, 'Information technology and the world economy', *Scandinavian Journal of Economics*, vol 107, no 4, 2005, pp631-650.
- Knight, Sam, 'All-seeing Google Street View prompts privacy fears', *Times Online*, 1 June 2007.
- Knowledge@Wharton, 'Will Newspaper Readers Pay the Freight for Survival?' 19 May 2010.
- Kumaraguru, Ponnurangam and Cranor, Lorrie Faith, *Privacy Indexes: A Survey of Westin's Studies*, Pittsburgh, PA: Institute for Software Research International, School of Computer Science, Carnegie Mellon University, 2005.
- Landes, William and Posner, Richard, *The Political Economy of Intellectual Property Law*, Washington DC: AEI-Brookings Joint Center for Regulatory Studies, 2004.
- Larson, Erik, 'Phone-hacking shows jail needed for data theft, U.K. privacy chief says', *Bloomberg*, 29 July 2011.
- Lea, David, 'From the Wright brothers to Microsoft: issues in the moral grounding of intellectual property rights', *Business Ethics Quarterly*, vol 16, no 4, 2006, pp579-598.
- Lessig, Lawrence, 'CC in Review: Lawrence Lessig on How it All Began', *Creative Commons News*, 12 October 2005.
- Lessig, Lawrence, *Remix: Making Art and Commerce Thrive in the Hybrid Economy*, London: Penguin Books Ltd, 2008.
- Lessig, Lawrence, 'Against transparency: The perils of openness in government', *New Republic*, 9 October 2009.
- Lewis, J. David and Weigert, Andrew, 'Trust as a social reality', *Social Forces*, vol 63, no 4, June 1985, pp967-985.
- London Economics, *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs): Final Report to the European Commission DG Justice, Freedom and Security*, July 2010.
- Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age*, New York: Princeton University Press, 2009.
- McKinsey, *Consumers Driving the Digital Uptake: The Economic Value of Online Advertising-based Services for Consumers*, McKinsey/IAB Europe, 2010.
- McMillan, Robert, 'Is it time for RSA to open up about Securid hack?' *InfoWorld*, 13 June 2011.
- Menell, Peter S., 'Intellectual property and the Property Rights Movement', *Regulation*, Fall 2007, pp36-42.
- Narayanan, Arvind and Shmatikov, Vitaly, 'Robust de-anonymization of large sparse datasets (How to break anonymity of Netflix prize dataset)', *Proceedings of the 29th IEEE Symposium on Security and Privacy*, May 2008, pp111-125.
- New York Times, 'Facebook privacy: a bewildering tangle of options', 12 May 2010.
- Nissenbaum, Helen, 'Protecting privacy in an information age: the problem of privacy in public', *Law and Philosophy*, vol 17, 1998, pp559-596.
- Odlyzko, Andrew, 'Privacy, economics, and price discrimination on the internet', *ICEC Proceedings of the 5th International Conference on Electronic Commerce*, 2003, pp355-366.

OECD Working Party on Information Security and Privacy, *Making Privacy Notices Simple: An OECD Report And Recommendations*, DSTI/ICCP/REG(2006)5/FINAL/ANN, 2006.

Office of the Privacy Commissioner of Canada, 'Letter to Google Inc. Chief Executive Officer', press release, 19 April 2010.

Orwell, George, 1984, London: Martin Secker & Warburg Ltd, 1949.

Poynter, Kieran, *Review of Information Security at HM Revenue and Customs: Final report*, 2008.

Prahalad, C.K. and Ramaswamy, Venkat, 'Co-creating unique value with customers', *Strategy and Leadership*, vol 32, no 3, 2004, pp4-9.

Price, Dick, 'What is PCI DSS and who needs to know?' *Chartech*, February 2010, pp12-14.

Prins, Corien, 'When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?', *SCRIPTed*, vol 3, no 4, 2006, p270.

Privacy by Design, *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices*, Information and Privacy Commissioner of Ontario / The Centre for Information Policy Leadership at Hunton & Williams LLP/Hewlett-Packard (Canada), 2009.

InfoSecurity Europe and PwC, *Information Security Breaches Survey 2010*, 2010.

Quah, Danny, *Digital Goods and the New Economy*, LSE Centre for Economic Performance, Discussion Paper No 563, 2003.

Rawls, John, *A Theory of Justice*, Bellknap: Boston, 1971.

Reed, O. Lee and Hipp, E. Clayton, 'A "Commonest" manifesto: property and the general welfare', *American Business Law Journal*, vol 46, issue 1, 2009, pp103-137.

Risch, Michael, 'Why do we have trade secrets?' *Marquette Intellectual Property Law Review*, vol 11, no 1, 2007, pp3-76.

Robinson, Neil, Graux, Hans, Botterman, Maarten, Valeri, Lorenzo, *Review of the European Data Protection Directive*, Rand Europe/Information Commissioner's Office, 2009.

Schumpeter, Joseph, *Capitalism, Socialism and Democracy*, London: G. Allen & Unwin, 1943.

Seltzer, William and Anderson, Margo, 'The dark side of numbers: the role of population data systems in human rights abuses', *Social Research*, vol 68, no 2, Summer 2001, pp481-513.

Sherman, Michelle, 'Social Media research + employment decisions: may be a recipe for litigation', *Social Media Law Update blog*, 18 January 2011.

SOAP, 'Findings from the Study of Open Access Publishing (SOAP)', 4 April 2011.

Social and Market Strategic Research, *Report on the Findings of the Information Commissioner's Office Annual Track 2010*, Hull: SMSR, 2010.

Solove, Daniel J., "'I've got nothing to hide" and other misunderstandings of privacy', *San Diego Law Review*, vol 44, 2007, pp745- 772.

Solove, Daniel J, 'A taxonomy of privacy', *University of Pennsylvania Law Review*, vol 154, no 3, 2006, pp477-560.

Soma, John T., Courson, J. Zachary, Cadkin, John, 'Corporate privacy trend: The 'value' of personally identifiable information ('PII') equals the 'value' of financial assets', *Richmond Journal of Law and Technology*, vol XV, issue 4, 2009, article 11.

Stanford Encyclopaedia of Philosophy, 'Privacy', first published online 14 May 2002.

Stavrakas, Alexandros, 'When piracy isn't theft', *The Guardian*, 24 November 2009.

Thomas, Richard and Walport, Mark, *Data Sharing Review*, 2008.

The Economist, 'Inventive warfare', 20 August 2011, pp53-54.

The Economist, 'Patently different', 20 August 2011, p54.

Varian, Hal R. and Shapiro, Carl, *Information Rules: A Strategic Guide to the Network Economy*, Boston: Harvard Business Press, 1998.

Vijayan, Jaikumar, 'TJX data breach: at 45.6M card numbers, it's the biggest ever', *Computerworld*, 29 March 2007.

Warren, Samuel and Brandeis, Louis, 'The right to privacy', *Harvard Law Review*, vol 4, 1890, pp193-220.

Weitzner, Daniel J., Abelson, Harold, Berners-Lee, Tim, Feigenbaum, Joan, Hendler, James and Sussman, Gerald Jay, 'Information accountability', *Communications of the ACM*, vol 51, no 6, June 2008, pp82-87.

Westin, Alan F., *Privacy and Freedom*, New York: Atheneum, 1967.

Westin, Alan F., 'Social and political dimensions of privacy', *Journal of Social Issues*, vol 59, no 2, 2003, pp431-453.

Whitman, James Q., 'The two Western cultures of privacy: dignity versus liberty', *Yale Law Journal*, vol 113, 2004, pp1152-1221.

Wiener, Norbert, *Cybernetics or Control and Communication in the Animal and the Machine*, New York: Technology Press/John Wiley & Sons, 1948.

Wiener, Norbert, *The Human Use of Human Beings: Cybernetics and Society*, Boston: Houghton Mifflin, 1950.

Williams, Christopher, 'BT and Phorm: how an online privacy scandal unfolded', *The Telegraph*, 8 April 2011.

Wilson, Jennifer Fisher, 'Health Insurance Portability and Accountability Act Privacy rule causes on-going concerns among clinicians and researchers', *Annals of Internal Medicine*, vol 145, no 4, 2006, pp313-6.

YouTube, *Terms of Service*, available online.

Zuckerberg, Mark, 'From Facebook, answering privacy concerns with new settings', *Washington Post*, 24 May 2010.





The ICAEW is a founder member of the Global Accounting Alliance, which represents over 775,000 professional accountants in over 165 countries worldwide, to promote quality services, share information and collaborate on important international issues.




ICAEW is a professional membership organisation, supporting over 136,000 chartered accountants around the world. Through our technical knowledge, skills and expertise, we provide insight and leadership to the global accountancy and finance profession.

Our members provide financial knowledge and guidance based on the highest professional, technical and ethical standards. We develop and support individuals, organisations and communities to help them achieve long-term, sustainable economic value.

**Because of us, people can do business with confidence.**

ICAEW  
Chartered Accountants' Hall  
Moorgate Place  
London EC2R 6EA UK

T +44 (0)20 7920 8100  
E [informationsystems@icaew.com](mailto:informationsystems@icaew.com)  
[icaew.com/informationsystems](http://icaew.com/informationsystems)

 [linkedin.com – ICAEW IT Faculty](https://www.linkedin.com/company/icaew-it-faculty)  
 [twitter.com/icaew\\_itfaculty](https://twitter.com/icaew_itfaculty)  
 [facebook.com/icaew](https://www.facebook.com/icaew)

£45.00