Managing Access Security & Privacy in the Global Digital Economy

reo® Research | January 2007

In this report...

- Emerging good practice for companies and their investors
- ASP issues will be a key determinant in shaping the commercial success of the TMT companies

F&C Investments

Expect excellence

Our philosophy

reo® stands for responsible engagement overlay

The objective of ***reo***® is to use the influence that F&C has through the share ownership of its clients to encourage investee companies to enhance their business performance by adopting better corporate governance, social, and environmental practices. F&C believes that it can better serve its clients, and protect the value of their shareholdings, through sustained and constructive dialogue with companies as well as the judicious and transparent use of its votes, thereby ensuring that companies respond prudently to the emerging expectations of shareholders and other stakeholders.

Table of contents

1. Introduction – Background to this Study 4

2. Study design 5
- Purpose 5
- Participants and terms of engagement 5
- Structure 5
- Terminology 5
- Glossary of Terms 6

3. Understanding the sector 7

4. Access 8
- The challenge 8
- Malicious technical devices 8
- Content restrictions 8
- Customer intent 9
- Company experience 9
- Good practice 10

5. Security 11
- The challenge 11
- Company experience 12
- Good practice 12

6. Privacy 14
- The challenge 14
- Company experience 15
- Good practice 15

7. Responding to the outside world 16
- The challenge 16
  - Customers demand product innovation and ethical conduct 16
  - Public calls for accountability 17
  - Investors seek assurance about long-term business prospects 17
- Company experience 18

8. Emerging good practice in managing ASP 20
- From challenge to opportunity 20
- Governance of ASP 20
- Managing ASP issues within the business 21
- Managing ASP issues that originate from outside the business 22

9. Conclusion 23

10. Acknowledgements 24

Introduction
Background to this study

F&C has undertaken a study of the implications of Access, Security and Privacy (ASP**) in the technology sector. The aim of this research is to identify how Technology, Media and Telecommunications (TMT*) companies can best respond to the twin challenges of allowing users maximum access to information, while still safeguarding their security and privacy.

The technological revolution is transforming not only business, but virtually every aspect of global human interaction. This study takes as its starting point that the social contribution of technology, through the critical role it plays in enabling people to access and distribute information, has been overwhelmingly positive. However, with the explosion in information transfer have come some new concerns. These include: dissemination of illegal content, exposure of minors to inappropriate material and online 'predators', and increased vulnerability to security threats that the reliance on technology creates.

Some governments' responses to these challenges have included resorting to sophisticated surveillance technology, which raises additional concerns over the potential infringement of civil liberties. Attempts to control and restrain certain actors online have had mixed results, and present real challenges in terms of both their effectiveness and collateral effects on society.

Pressure groups have long made use of new technology to expose human rights abuses around the world, but are now also shining a spotlight on the new ways that technology is being used to track political dissidents and silence free speech. Human rights advocates have begun specifically to target the companies who, in effect, enable such abuses through the provision of systems and services – focussing in particular on Western companies operating in countries like China, where government repression has made use of imported technology. Even the UN has recognised the TMT sector as a sector with heightened human rights concerns.

The TMT sector has not sat idly by: it has moved to address certain aspects of the ASP challenge, using its ingenuity to develop technological fixes to emerging problems, and indeed, turning necessity into the mother of profitable invention in many cases. However, as the sector continues to expand globally and technologies converge in new ways, the difficulties the sector has encountered so far are likely to grow in scale and complexity.

For investors in the TMT sector, these challenges present a serious concern, as these developments may affect the very core of these companies' business models, which are based on the ability to exchange information freely via technology. A pro-active response to managing these issues is vital in order to safeguard the sector's license to operate, avoid obstructive regulation, and to maintain customer trust. This study aims to provide a framework of good practice for both companies and their investors on how to assess and manage the risks and opportunities associated with these challenges.

* Indicates a term included in the Glossary of Terms, Section 2

Study design

Purpose

F&C undertook this study in an effort to:

- Identify where Access, Security and Privacy issues arise in different segments of the TMT sector;
- Determine how they might be managed in order to safeguard long-term shareholder value, and;
- Identify elements of emerging good practice and raise awareness across the sector.

Participants and terms of engagement

F&C invited 13 global companies to participate in the study. These were categorised into three sub-sectors in order to analyse the specific implications of ASP issues in each of these different businesses.

- Network Operators: **Vodafone, Deutsche Telekom, Telecom Italia,** and **BT**
- Hardware companies: **Intel, Motorola, Nokia, Ericsson** and **Sony**
- Software companies: **Google, Yahoo!, Microsoft** and **SAP**

We initially carried out a review of publicly available material, such as company disclosure, reports from non-governmental organisations (NGOs*), academic research and relevant legislation. On the basis of our findings, we developed a set of questions to guide our discussions with each of the 13 companies. Experts from the respondents' legal, technical and compliance departments were involved in these discussions and made available internal documents to F&C on a confidential basis.[1] While the details of individual discussions are confidential, the insights we gained have been incorporated into this study.

This study does not attempt to benchmark corporate performance on managing ASP risk; as this issue is still very much in its early stages, and corporate best practices have yet to be established, benchmarking would be premature. The purpose of this analysis is to catalyse a discussion about best practice so that the findings can serve as the basis for benchmarking tools that we hope will be used across the sector. Hence, in this study, examples have been employed to illustrate challenges and possible responses.

Structure

This report is structured along a discussion of the three key issues of Access, Security and Privacy. Section 3 sets the scene by drawing out the key features of each of the three sub-sectors and the way in which they inter-relate. Thereafter, the issues of Access (Section 4), Security (Section 5) and Privacy (Section 6) are discussed in turn. We begin by identifying the challenges that each issue poses to the TMT sector and its constituents, then follow with an analysis of potential responses and practical company experiences, and conclude with good practice recommendations.

Section 7 considers how the corporate community engages with the external world, i.e. customers, regulators, civil society and investors, as these stakeholders all play a key role in shaping the ASP landscape. Section 8 draws together the findings from the previous sections into a set of recommendations for a well-managed company to address ASP issues both within and etxernal to the business. Finally, the conclusion (Section 9) sets out F&C's assessment of the ASP debate in the context of its overall investment approach, and defines next steps in taking the ASP agenda forward.

Terminology

As with all emerging debates, terminology varies. For the purpose of this study, we look at the issue in three categories:

- **Access:** The ability to gain access to and distribute information and ideas at will
- **Security:** The ability to protect customers, data and systems from outside interference and only make them available to authorised personnel
- **Privacy:** The ability to protect or safeguard personal information and confidentiality

These areas of Access, Security and Privacy are inter-related and have significant overlap. For instance, personal data security is essential to protect privacy; indeed these two are almost inseparable. Access, on the other hand, bisects both Security and Privacy; in order to control a user's access to information, a company might be required to collect sensitive personal data such as age information, and also block programmes that could inhibit privacy or lead to security threats such as spyware*.

The technology sector is marked by widespread use of specialist industry terminology that may be unfamiliar to the lay reader. The following glossary serves as a reference for terms that will appear throughout the following report.

1 It was agreed between F&C and the companies that none of these materials constituted market-sensitive inside information

Glossary of terms

ASP Access, Security and Privacy as they affect the TMT sector.

Biometric data systems Electronic systems that capture and store biological data such as fingerprints or DNA.

Blog An online diary or journal. "Vlogs" or video blogs are also becoming more common.

Digital home Emerging technology systems that network together different electronic systems in the home such as televisions, computers and home security systems.

ESG Environmental, social and governance.

Filter A piece of middleware that, because of its physical position and function, limits the amount or kind of information entering a network.

GPS Global Positioning System, a telecommunications service that enables one to track the location of a given person or object.

Hardware The material, computing equipment that enable the network to function; can also include end-user hardware such as PCs, PDAs or mobile telephones.

IT Information technology.

Layered privacy policies Layered privacy policies allow all users to read general privacy guidelines in 'plain English' or other languages, with the option to click through to the more detailed privacy policy.

Layered security levels Restrict employee access to data and allow only authorised employees to access the most sensitive data.

Loyalty cards Digital cards often used by retailers to track customer purchasing habits, which are then used for targeted marketing.

Metadata descriptors Information about the format, style, or content of a webpage. Metadata descriptors allow web page authors to describe their content in a machine-readable way; in turn, parental control tools can act on those descriptions.

Middleware Equipment such as routers or other networking devices that serve as gatekeepers to allow or prevent data from moving into or within a network.

Nanotechnology A combination of science and technology whose goal is to control individual atoms and molecules to create computer chips and other devices that are thousands of times smaller than current technologies permit.

NGO Non-governmental organisation, representing the interests of civil society on ethical issues, in this case of freedom of expression and the right to privacy.

PD Personally digital accessory, including Blackberry™ devices, digital organisers etc.

Phishing A method of identity theft in which a website, posing as a legitimate company, takes and exploits personal information from consumers who believe they are purchasing real goods and services.

Privacy Hierarchy A privacy standard under which more stringent privacy policies apply as more sensitive data are collected.

RFID Radio frequency identification tags. Tracking tags that enable companies to track the logistics of products throughout the supply and distribution chain.

Router A hardware device that forward or directs packets of data across networks.

Server A computer that makes services (access to data files, software programmes, and peripheral devices) available to workstations on a network.

Social-networking services Web-based services whose primary function is to connect different parties via the Internet. This may include online dating services or other web-based community groups.

Spam Unsolicited marketing e-mail.

Spyware A programme that covertly gathers information about a user while using the Internet and sends that information to an individual or company for marketing or other uses.

TMT Technology, media, and telecommunications sector.

User-generated data Information or data that is developed by a discreet customer or end-user. The user typically operates independently and is not controlled by another organisation such as a media company that might provide content.

Virus A malicious software programme whose intention is to corrupt and incapacitate a host system or network.

Web portal A website considered an entry point to other websites, often by being or providing access to a search engine.

Worm Computer code implanted illegally in a software programme designed to destroy data in any system that downloads the programme.

Understanding the Sector

F&C's study has clearly revealed that ASP issues are material to Technology, Media and Telecoms companies, but they manifest themselves differently in each sub-sector.

The TMT sector as a whole has significant influence in the marketplace of ideas and in shaping human interaction. It drives what ideas enter the marketplace, who has access to them and how they are distributed. As network operators and service providers become increasingly linked with the creation and provision of content, so they will come up against the privacy and related issues that have long been of concern to the traditional media sector. All segments of the TMT sector are closely interlinked and are converging on a number of levels, and it is important to understand how different products and services work together in order to comprehend where one company's sphere of influence may end and another's begins.

For the sake of simplicity, we have broken the sector into the following three sub-sectors. However, the TMT sector is highly complex and companies operating in this space may occupy more than one of these sub-sectors.

- **Network Operators** provide the infrastructure and telecommunications services that connect end users to one another. They operate the satellites that enable communications to bounce between countries and users, and they maintain the functionality of the network to ensure that it works properly. Network operators participating in this study include **Vodafone, Deutsche Telekom, Telecom Italia,** and **BT**

- If network operators provide and maintain the network that connects users, manufacturers of operating systems and applications (aka **Hardware Manufacturers**) provide the material equipment, or 'pipes', that enable the network to function. Hardware manufactures provide a range of products, including "middleware*," i.e. equipment such as routers* or other networking equipment that serve as gatekeepers to allow or prevent data from entering the network. Hardware also includes end-user equipment, such as mobile telephones or personal digital accessories (PDAs*) – e.g. BlackBerry™ devices – through which customers can access and distribute information. Other hardware might include semiconductors, which allow hardware to function, or data storage devices, such as servers* that warehouse sensitive data. Hardware providers participating in this study include **Intel, Motorola, Nokia, Ericsson** and **Sony**

- **Software** and **Service Providers** offer the actual web tools through which end users access and exchange information. Software products control content at the local level, i.e. they enable users to sift through the global sea of data and pinpoint the information they want. The software sector is also starting to offer online media services. Beyond controlling access to content, service providers now also own the content that passes through their web portals. Software and service providers that distribute content on multiple platforms such as the Internet and mobile phones are now facing some of the same privacy challenges that traditional media companies have dealt with for years. Examples of this new media and technology convergence include **NewsCorp**'s recent acquisition of **MySpace** and **Google**'s acquisition of **YouTube.** Software and service providers participating in this study include **Google, Yahoo!, Microsoft** and **SAP**

If one compares the TMT sector to the plumbing system of a house, the network operator is like the water company, connecting homes to the water distribution network and ensuring that the network of pipes functions properly. The hardware company provides the pipes themselves, through which the water flows, and may provide other products such as the hot water heater or cooling system. Finally, the software sector provides the tap, shower-head, filtration system, and other accessories that allow one to adjust how, when, and in what condition the water is available.

Each of these sub-sectors faces its own risks regarding Access, Security and Privacy given its different role in the architecture of the information economy. The software sector is highly exposed to technical risks, such as viruses, that can contaminate information and affect operating systems. As consumer-facing companies operating in a highly competitive environment, both software companies and network operators face high reputational risk vis-à-vis customers and the public. Hardware producers are also exposed to a range of technical challenges. Although not responsible for the data that flow through their products, hardware companies need to develop products that ensure that the data passing through their products can be kept secure and confidential. Throughout the study, we will look at the specific Access, Security and Privacy challenges that each of these sub-sectors faces in turn.

Technology convergence means that these distinctions between sub-sectors are beginning to blur. With web-enabled mobile phones and the emergence of the digital home, hardware products are now serving as host to software products, and therefore face related ASP risks. In addition, the rise of social networking services* like MySpace, Facebook and YouTube, which are based on user-generated data*, means that network operators and software and service providers will be faced with new demands for protecting data and individuals.

Access

The challenge

In the current global political environment, the ability to access and distribute information and ideas at will cannot be considered an absolute right, any more than press or broadcast media have been able to operate unfettered by legal or regulatory attention in the past. While freedom of expression and information, and the right to privacy, are internationally recognised human rights, these are qualified by national security interests and the safety of vulnerable segments of society. From a company perspective, the ability to distribute information freely also faces limits where it may negatively affect the ability to secure the network and protect customer privacy. Below, we distinguish between challenges that affect the sector as a whole and those that are specific to a sub-sector.

Key challenges for managing Access in each of the TMT sub-sectors:

Network Operators

These need to provide a quality network that delivers accurate information to a wide range of customers, but in so doing face the following challenges:

- Handling illegal content in line with laws and regulation – e.g. child pornography or material deemed conducive to terrorist activities
- Understanding social expectations to protect vulnerable customers from harmful or offensive content – e.g. children
- Meeting customer demands to control their own Internet experience and access to information
- Ensure that messages reach their destination without intervention

Hardware Manufacturers

These need to provide standard products that can be used in any global network setting, yet also meet specific customer needs. Getting this balance right presents the following challenges:

- Selling products responsibly into new markets, particularly when freedom of expression is restricted and hardware products – especially middleware* – can be used to inhibit free exchange of information

Software and Service Providers

As the Internet penetrates the last corners of the world, software and service providers are faced with requirements to limit access to the Internet on their international growth path. Challenges include:

- Meeting government-imposed requirements to restrict free speech, while at the same time meeting customer expectations of providing an open marketplace for trading ideas
- Preventing the distribution of spy-ware*, viruses*, and worms*, etc… which could seriously cripple or destroy the software products themselves and customers' own systems
- Managing traditional content regulatory requirements inherited from the press and broadcasting sectors

Malicious technical devices

Devices like viruses that get transmitted through the Internet and email are designed to alter operating codes and cause havoc to entire networks, thereby bringing IT systems at all levels to a grinding halt.

Network operators provide the pathways through which these viruses can infect millions of customers. Hardware manufacturers, while they do not control customer access to information, produce products such as routers* and filters* that enable or limit access to the network. Filters can be set to identify viruses and prevent them from entering the network. Products such as security software are designed to fight off viruses or block them if they do gain entry into the network.

The sector's ability to prevent programmes like viruses from entering the network and allowing them to interfere with customers is critical to maintaining customer trust and business continuity.

Content restrictions

Given the enormous diversity of content available on the Internet, categorising content, determining appropriate access, and enabling users to manage content is a major challenge for the sector, especially in the absence of clearly defined and globally applicable standards.

Through their networks, operators allow customers to enter the Internet space and gain access to all sorts of content, including some that might be deemed illegal or inappropriate. Regulatory standards for what constitutes illegal content are not globally uniform or legally enforceable. Similarly, different marketplaces have varying sensitivities to violent or sexual material and there are no global ratings standards for Internet content. In addition, content on the Internet is in constant flux and difficult to track down. To add a third layer of complexity, individual customers are also demanding tools to drive their own Internet experience at an individual or household level, e.g. in order to protect children from access to violent or pornographic material.

As TMT companies expand globally, they find themselves operating under different regulatory regimes, including some in which they may be called upon by governments to limit access to content that is deemed politically sensitive. According to freedom of speech advocates, some 30 countries pervasively or substantially limit freedom of expression and access to the Internet within their borders.[2] From a technical standpoint, the ability to restrict access to political content can involve some of the same techniques as installing filters to protect minors. While companies may be required to co-operate with government in order to operate in a given market, they also run the risk of being accused of complicity in restricting freedom of expression. For example, in China, foreign companies are required to comply with regulations governing access to controversial content that are both broad and at times vague, and that obligate service providers to take proactive steps to address content on their services. Some human rights advocates, moreover, have raised questions about the validity of such regulations, given that other national and international legal documents also protect the right freely to express and exchange ideas. Defining appropriate and legal protocols vis-à-vis customers and government is vital for maintaining customer trust and building a stable predictable operating environment.

Customer intent

Next to diversity of content, diversity of the customer base is the second-greatest challenge facing TMT companies; this, in turn, means that controlling how customers use technology products is often impossible. This is a particularly grave concern in the case of hardware manufacturers who sell to government agencies or middlemen, because of the risk that they will misuse the technology that enables them to restrict access to information. For example, some equipment manufacturers assist customers in installing networks and setting up filtering standards. If an equipment manufacturer enables a government agency to operate a very restrictive set of filters, it could be considered complicit in limiting freedom of expression and access. This scenario arose at **Cisco Systems,** which supplies the Chinese government with networking equipment that enables it to filter Internet content within China. In 2006, this led to **Cisco**'s CEO being called before the US Congress to defend the company's actions, a shareholder proposal from investors concerned about damage to the company's brand, and sustained criticism by human rights activists. Hence, in order to be able to weigh up the potential impact on reputation and future liabilities against the benefits of growing sales, companies must develop a thorough understanding of, and engagement with, potentially sensitive customers[3].

UN Special Representative to the Secretary General on Business and Human Rights, Prof. John Ruggie has suggested that companies could conduct market-specific assessments in order to evaluate their business's impact on human rights. The International Business Leaders Forum (IBLF) and the International Finance Corporation (IFC) are developing tools to assist companies in conducting such assessments.[4] In addition, the idea of developing human rights risk indices is gaining traction among some companies and civil society stakeholders.

Company experience

Companies across the TMT sector have begun to develop practical responses to the Access challenges outlined above.

Firstly, countering malicious technical threats is a key function of any technology company. All of the companies that participated in F&C's study had sophisticated vulnerability testing models to avoid the worst-care scenario of a network going down at the hand of a hacker's virus, thereby potentially depriving the entire customer base of access. This subject is discussed further in the Security section below.

Second, companies are tackling the challenges posed by the need to offer restrictions on sensitive content across markets with disparate demands. Network operators like **BT** and **Vodafone** offer customers access to the Internet through their own-branded web portals. Within the walls of these portals, both limit access to sites deemed illegal or inappropriate according to externally-recognised content standards and policies that the companies themselves have established. **Vodafone**'s content standards policies are set according to local social, cultural and legal norms in each market. **BT** has developed its internal *Taste & Decency Guidelines* that define acceptable content standards and determine who **BT** will and won't work with. In addition its *cleanfeed software* limits access to child pornography for UK residential customers. Beyond these portals, once customers enter the World Wide Web, these proprietary access controls no longer apply, leaving customers to enter a vacuum where globally applicable reference standards do not exist. This gap poses a concern to companies operating internationally, and has prompted creative responses: **Vodafone** has developed a global Internet filter that it is rolling out worldwide. It also has tasked its local operating companies with drawing up locally-applicable lists of illegal and sensitive content. Moreover, in response to customer demand, **BT, Deutsche Telekom, Microsoft, Telecom Italia** and **Vodafone** offer parents tools that enable them to design their own customised access restrictions. Hardware company **Sony** has likewise incorporated parental controls on video game consoles.

The TMT sector has also taken steps to develop a coordinated industry response to government requirements to restrict political content. In February 2006, US software companies **Google, Yahoo!** and **Microsoft** were called before the US Congressional Subcommittee on Global Human Rights to explain their business policies for filtering, censoring and otherwise limiting freedom of expression and privacy on the Internet in China. Their practices in that

2 According to freedom of speech advocates, an estimated 30 countries actively limit freedom of expression and access to the Internet within their borders.[1] (Citation, Open Net Initiative forthcoming publication on Global Internet Filtering. Countries that pervasively or substantially filter the Internet include: Belarus, Cuba, Iran, Maldives, Saudi Arabia, Syria, Tunisia, Turkmenistan, Ukraine, and Zimbabwe. www.opennet.net/map)

3 **Nortel Networks** was also the subject of a shareholder proposal regarding its impact on human rights in China but, as a Canadian company, was not subject to congressional scrutiny. See Section 4: Company Experience for further information on other companies called before the US Congressional hearings

4 *Human Rights Impact Assessments: Discussion Paper,* prepared for U.N. Special Representative John Ruggie, 18 July 2006, available at www.reports-materials.org/discussion-paper-human-rights-impact-assessments-Jul-2006.pdf

country over the previous year had unleashed a public furore, which had been fuelled by widespread media coverage and sharp criticism by civil society groups. As a result, these companies, along with **Vodafone,** have come together with other stakeholders to discuss a set of industry principles for company behaviour regarding free expression, privacy, transparency and rule of law, including in locations where free access to the Internet is restricted. While this group is only in its initial phase, there is hope that collective action can help the sector develop a credible response to a problem that well exceeds the capacity of any single company to resolve individually. In the meantime, **Google** went ahead and introduced a new operating protocol under which Google.cn users will be notified when their search results have been limited or filtered. Similarly, **Microsoft** instituted a new policy under which blog* content that is restricted under local legal requirements will only be restricted in that jurisdiction, but will still be accessible in other jurisdictions worldwide. **Yahoo!** China, which is operationally controlled by its local business partner, **Alibaba.com**, also now provides notices to users that search results may be limited or filtered.

Companies are still struggling with how best to identify, and evaluate the risk posed by, customers who intend to use their products to restrict access to the Internet. Some stakeholders have recommended developing independent human rights risk indices to identify key markets where freedom of expression or access to the Internet might be limited. While no such index yet exists, this general strategy has proved effective in identifying other kinds of high-risk customers, such as customers who might divert products for violent or criminal activity. For instance, **Motorola** uses guidelines published by the US Department of Commerce's Bureau of Industry and Security to flag high-risk customers and apply more thorough due diligence to avoid assisting suspected terrorists or criminals.

Good practice

While many of the challenges outlined above will remain and even increase in the near future, F&C has identified some signs of emerging good practice for responding to industry challenges related to Access. Our research revealed the following elements of good practice:

1. Categorise content: Develop clear internal categories for illegal and sensitive content in each operating environment
2. Develop and deploy tools to manage content: These should restrict distribution of illegal content or dangerous technical programmes like viruses. However, standards for restricting sensitive content should reflect local cultural norms
3. Empower customers: Offer tools to enable customers to manage their own Internet experience in accordance with personal content sensitivities
4. Minimise restrictions: Where content must be restricted due to legal requirements, define restrictions as narrowly as possible both in terms of the content itself and the areas in which it is restricted
5. Clearly disclose terms of use: If content must be filtered or access denied, clearly disclose to customers that freedom of information has been limited
6. Develop *Know Your Customer* policies or risk indicators: These apply to products sold to middlemen or governments who may use those products to restrict access to the Internet

Security

The challenge

Security has always been of paramount concern to TMT companies as they facilitate the global transfer of sensitive financial and personal data. These risks will only grow as more operations rely on information technology and business models in all sectors go on-line, increasing their exposure to IT security threats. As globalisation drives information processing into new markets, weaknesses in intellectual property and technical controls further aggravate these risks.

Key challenges for managing Security in each of the TMT sub-sectors:

Network Operators

These need to maintain the stability and security of the network at all times. Key challenges include:

- Unexpected catastrophic events, either human or natural, that could take down or severely hamper the network: in an era marked by more frequent and severe weather events as well as heightened terrorist activity, telecoms operators could face acute security threats with minimal notice
- Hosting other services, such as software products, that introduce additional vulnerabilities, like viruses, to the network outside the control of the network operator

Hardware Manufacturers

These need to offer secure hardware products for storing and distributing sensitive data. Key challenges include:

- Regulatory and corporate trends to collect and store more sensitive data, which are matched by ever more sophisticated efforts to access such data illegally. This, in turn requires hardware products to keep up with demand for protective systems. For example, biometric data systems* involve storing highly sensitive personal data that would also be very valuable to terrorists
- New mobile technologies, which lead to storing secure data in new forms and locations like BlackBerry™ devices or RFID* tags on consumer goods, and require new forms of safeguards

Software and Service Providers

These need to provide innovative products that allow consumers to transact business and access content in a safe and secure environment. Challenges are heightened by the highly competitive environment, and include:

- Protecting intellectual property in an open source environment in which programming code is constantly being deconstructed and attacked by competitors and black-market hackers
- Understanding, and resolving in advance wherever possible, copyright issues for content distribution
- Offering secure software products online amidst a consumer base with varying levels of understanding of their own exposure to security risks

Threats to Intellectual Property (IP)

Safeguarding IP is critical for maintaining product integrity and safeguarding revenue streams, yet intellectual property rights are frequently ignored by consumers globally.

New hardware products such as the latest *iPod* can be disassembled in order to replicate them illegally. Socialnetworking and user-generated content sites create a whole suite of risks, as software developers and media companies distribute unlicensed copyrighted content and take on new litigation risks for breaches of IP law. The wrangles surrounding music exchange already have generated extensive copyright litigation, notably over **Napster's** music download service. Experts have suggested this risk will be tested again with **Google** as a result of its acquisition of **YouTube**.[5]

A company's ability to secure its own IP, as well as ensure that any products/services on offer do not breach IP laws, is core to safeguarding its business model.

Physical security risks

Several of the greatest security breaches seen in 2006 were the result of stolen laptops in which the personal, financial and health information of thousands of customers was literally stolen right out of an employee's hands. Similarly, unauthorised access to secure data centres can put data security in jeopardy. Extreme weather events or man-made disasters can also severely hamper the sector. Hurricanes or tornadoes not only knock-out telecommunications networks, but also prevent employees from getting to work and backing up data or otherwise carrying out their normal functions.

Pro-actively planning for disaster, i.e. developing effective business continuity plans, is key to mitigating the risk of extreme physical disruption.

Security products create new risks and opportunities

As companies develop innovative products, people entrust more personal and sensitive data to these technologies. For example, many consumers now pay their taxes online, consolidating what had been diversified personal financial information in one place. Providing a software product that

5 The legal and economic implications of the copyright challenges associated with this acquisition have been debated at length. A good summary of the challenges was put forth by Harvard Law Professor John Palfrey and economist Stan Liebowitz in "Does YouTube Make Google a Big Target for Copyright Suits," *The Wall Street Journal,* 11 Oct 06

enables customers to gather this information and submit it to government agencies adds efficiency and provides a valuable service. However, it also unravels some of the natural security hedges that had previously existed and creates an opportunity for a more damaging security breach. Similar scenarios apply with biotechnology, as systems and products probe the human body and store personal biological data. Such products, while increasing efficiencies and greatly aiding the medical profession in identifying patterns of disease, could also be deadly in the hands of bio-terrorists. Companies face the challenge not only of fitting their products with more sophisticated security features, but also of anticipating future trends and pro-actively incorporating these upstream in the product design phase.

Human error and Security

For companies with large numbers of employees and customers, sometimes simple human behaviour can raise additional security risks or challenges. While IT professionals typically have highly specialised skills for managing sensitive data and technology code, other employees may not, and human errors of omission or commission can cause security problems. Equally, customers' knowledge of password management, security software and other Internet security tools varies, and some customers cannot always be counted on to safeguard their own personal data. Developing a targeted response to human error through technical tools and tailored awareness raising and training is therefore highly important.

Company experience

In terms of managing security risks, companies report that security management has a clear material impact on their business. Software companies have long had to develop responses to complex security threats to their intellectual property, which typically come from outside the business itself[6]. **Microsoft** reports in its 2006 10-K filing that "Security vulnerabilities in our products could lead to reduced revenues or to liability claims"[7], and has developed dedicated teams of specialists focused on threat-modelling because Windows products are a prominent target for hackers. **Yahoo!** has also developed an internal cross-functional team of engineers, lawyers, and business people – affectionately known as "the Paranoids" – to review products and systems for data security risks and prepare for and respond to data security concerns across the business. **Vodafone** has teams of security specialists at the local and global levels that provide security expertise on business, product and technology developments and coordinate activity across its multiple markets through a Global Security Forum.

Beyond technical security management systems, software companies are keenly aware of the need to create a security "culture", both within the company and with customers. Many companies report that employees undergo security policy training, with more in-depth training for key employees. **Intel** has also introduced layered security access levels that restrict employee access to data and allow only authorised employees to access the most sensitive data.

Good practice

Security challenges will remain a hallmark of the sector; however, F&C has identified the following as indicators of emerging good practice for managing security risks:

1. Develop multi-disciplinary teams to evaluate and test security management across the business, to mitigate internal weakness and respond to external security threats. Best practice includes board-level oversight of key findings
2. Establish, distribute, and regularly test business continuity plans in case of physical security risk
3. Develop security management systems that include limited access to sensitive intellectual property or user data
4. Conduct annual staff training on security procedures that includes a segment on physical security and data security (e.g. what to do in the case of a stolen laptop)
5. Provide customer education to empower customers to safeguard their own data and systems

Customer education and training on data security has been also identified as an area where more work needs to be done to enable customers to safeguard their own personal data when it is within their control. **Yahoo!** has created a *Security and Privacy Center* on its website to educate users on how they can protect their data using simple techniques such as password protections, etc. **Yahoo!** has also developed a new "security shield" tool that will help prevent customers from phishing* attacks while surfing the web.

Companies such as **SAP** have responded to growing customer demand for security products and assurances of effective internal security management. **SAP** has installed a Global Security Management System, which is certified to ISO 27001, a standard published only in November 2005. **SAP**'s Chief Security Officer who reports directly to the board is responsible for this process. On the product side, **SAP** has developed a *Product Innovation Lifecycle (PIL)* to develop, maintain and roll out guidelines for secure programming and software assurance. **SAP** is also a founder of the *Global Security Alliance,* a platform for information and knowledge exchange that comprises leading providers of security and risk management offerings. Members include **IBM, Siemens Communications** and **Sun Microsystems.** Security issues were identified among the Top 10 issues concerning suppliers in the TMT sector in a recent customer survey.[8] **Ericsson** has equally experienced increasing expectations from customers regarding network security. Major problems can quickly devalue the brand, whereas good performance in this area can strengthen the brand. **Ericsson** has launched a global initiative called the *Information Security Improvement Programme* (ISIP) in order to build culture and awareness and to integrate information security requirements into the business process. The three main components of the programme are people, technology and processes.

Sony has a dedicated division in charge of managing information security. The **Sony** Global Information Security Policy applies to **Sony** group companies worldwide, and includes guidelines for asset management, human resources security, physical and environmental security, communications and operations management, and access control. **Sony** conducts security training programmes for all of its employees and additional specialised training is provided for divisions handling personal information.

6 One related challenge that could arise in trying to respond to IP concerns is the risk of anti-trust. In trying to protect intellectual property, companies have from time to time come up against charges of anti-competitive behaviour. This study focuses on security risk and has therefore not attempted to respond to related regulatory and compliance risks that could be associated with anti-competitive behaviour. However, significant work on this subject has been done by others

7 Microsoft 2006 10-K filing

8 The survey was ordered by Ericsson and addressed its customers and potential customers. The customers were asked a number of questions about Ericsson and other companies in the telecom sector. Security was one of the Top 10 issues among the customers in the sector

Privacy

The challenge

The question of privacy has taken centre stage as TMT companies find themselves caught in a debate over civil liberties vs. the right of government to compel disclosure of personal customer data in the interest of national or global security. These demands are likely to increase, especially in countries where the right to privacy is not well entrenched. As in preceding sections of this report, F&C has identified several privacy risks specific to each sub-sector, as well as broad privacy concerns that are common across the whole sector.

Key challenges for managing Privacy in each of the TMT sub-sectors:

Network Operators

These store and direct large volumes of private information, including personal communications and even customer locations, within their standard operations. Wireless service providers also collect information on user location, through global positioning services (GPS) and the like. This presents challenges when:

- Governments require more customer data to be stored for longer time increments, generating additional privacy and security risks
- Companies need to disclose customers' confidential information in order to comply with a request for assistance from law enforcement agencies

Hardware Manufacturers

These need to offer products for storing and distributing sensitive data confidentially, and purging that information when it is no longer necessary. Key challenges arise when:

- Customer demand for greater inventory management tools, such as RFID* tags, or customer behaviour monitoring tools, such as loyalty cards*, collect large volumes of data about personal behaviour that could be misused or compromise end-user privacy
- New emerging technologies, such as nanotechnology* or the digital home*, distribute personal information in new ways that may have unforeseen privacy and security weaknesses

Software and Service Providers

These develop software products that ensure that customer data remain confidential, and face challenges when:

- Meeting customers' and civil society's expectations for confidentiality, must be balanced against the need to co-operate with law enforcement agencies
- Customers require protection from invasive behaviour designed to dupe them into relinquishing personal information. This is frequently the result of malicious software programmes such as spyware*, phishing*, spam* etc.

Responding to government demands for data

Alongside its immeasurably positive effects, the Internet is also increasingly being recognised as a key facilitator of global criminal activity, prompting governments to extend their reach into this realm while often relying on TMT companies to provide them with both the tools and data to do so. This means that companies can find themselves exposed to liability claims from customers. For example, in 2006, the US' National Security Agency introduced a call-tracking programme to detect terrorist plots, and requested millions of customer records from US telecoms operators, including **AT&T, Verizon** and **BellSouth**[9]; all three companies are now being sued for a combined $200 million for violating customer privacy laws. In 2004, **Yahoo!**'s Chinese subsidiary had acceded to a Chinese government demand to turn over data related to one of its user IDs. At that time, **Yahoo!** China did not know the name, identity or occupation connected to the user ID and similarly did not know any details of how the state security services might use the data provided in its transfer of state secrets investigation. Ultimately, the individual associated with the user ID was arrested and sentenced to 10 years in prison for distributing information to foreign colleagues regarding activities surrounding the anniversary of the Tiananmen Square massacre[10].

Both network operators and software companies need to have very clear protocols to assess the legality and appropriateness of any such requests for law enforcement assistance, and the consequences of responding to them. For example, the UK Data Protection Act allows companies to make certain disclosures of personal information if it is for the purposes of preventing or detecting crime, and it doesn't always require there to be a warrant or disclosure order. In addition, standards in other markets may differ substantially from the home country standards, and certain practices may be acceptable for local operators but not international companies from a stakeholders point of view.

Protecting Privacy amidst changing technologies

A further challenge lies in the increasing trend towards transfer of real-time inventory and customer behaviour data. This makes processes and systems more efficient, but is also vulnerable to abuse – as, for example, with RFID* tags on products that can, if not safeguarded properly, allow companies to track their customers' physical location. With the proliferation of GPS services by wireless telecoms providers and others, the ability to pinpoint individuals presents still more privacy challenges. Greater vigilance is required to prevent the spread of malicious software products designed to dupe users into relinquishing private information, which has contributed to a rapid rise in identity theft. This challenge will require a comprehensive technical and educational response from companies.

Company experience

Privacy is a key issue for TMT businesses, especially in the consumer-facing network operator and software sub-sectors. **Yahoo!** states that "Privacy and user trust is core to the brand; [it's] the 'bread and butter' of our business"[11], a sentiment echoed by most, if not all, companies.

In recognition of the importance of consumer privacy, **Vodafone** has adopted a global privacy policy applicable to its businesses worldwide, and established a global privacy steering group to oversee policy development and strategy. In each market, **Vodafone** has appointed a local Privacy Officer to manage compliance with the policy and provide expert guidance on privacy-related issues at the local level.

Privacy protection also is considered a potential product differentiator that could enable one company to pull ahead of its competition. As a result, companies are developing new processes to factor privacy issues into product design. To this end, **Microsoft** has created both internal processes, including the *"Trustworthy Computing"* initiative, a *Security Development Lifecycle* process, and recently published privacy guidelines for developers in order to help others factor privacy into product design.[12] For consumers, **Microsoft** has a Safety Technology and Strategy Group dedicated to developing new software products, such as spam-filtering technology that will protect customer privacy. **Motorola** has assembled internal security and privacy councils within each business unit to provide insight, advice and assistance during product development.

In response to law enforcement requests for data, companies such as **Google** have developed clear policies for empowering employees to comply with the law while still safeguarding customer privacy. **Google** has developed a four-step process for responding to law enforcement, which calls on employees to: 1) direct all law enforcement requests to the legal department, 2) evaluate the legal merits of the request, 3) require a judicial order before handing over the data, and 4) respond to such orders as necessary. This process was put to the test when the US Department of Justice requested data on one million websites and one week's worth of search queries. According to the company, this process resulted in a significant narrowing of the government's request for data, in turn generating an insufficient amount of data to put intellectual property or user search patterns at risk. **Deutsche Telekom** and **Telecom Italia,** too, have developed clear guidelines for responding to government disclosure requests; they will assess every request on a case-by-case basis and comply only if such request comes from a court rather than a government agency.

As consumers often do not want to click through pages of legal jargon on privacy, **Deutsche Telekom, Yahoo!** and others have developed layered privacy policies* in 'plain English' or other languages to advise users of what personal data is collected and how it is stored. Users can then dive deeper to get further information about privacy standards if they chose.

At **Nokia,** a Member of the Group Executive Board is responsible for overseeing privacy concerns, with support from dedicated personnel within the legal department and a Virtual Privacy Team consisting of approximately 20 lawyers company-wide. **Nokia** has set a privacy "hierarchy" that differentiates between the following three levels of access: a) general access to the Nokia website by customers/web-surfers on a read-only basis, in which case the **Nokia** Privacy Policy provides the general privacy information, b) customer contact where information is shared, e.g. through direct marketing; in such cases **Nokia** provides notification e.g. about what data are collected and how the data will be used; it complies with the opt-in and opt-out principles in accordance with applicable local data protection laws, and c) interactive customer programmes where more detailed data are collected and contractual terms are defined; **Nokia** complies with applicable local data protection laws.[13]

In response to privacy concerns about the ability to track consumers using technology, **Deutsche Telekom** is working on technical solutions such as bundling data so that precise locations cannot be determined or are hidden.

Good practice

As threats to privacy continue to evolve, F&C has identified the following steps as emerging good practices in managing these risks:

1. Develop systems for incorporating privacy standards into product development and information architecture. Privacy protection features need to be evaluated as a differentiating product criterion
2. Develop and test procedures for responding to requests for user data from law enforcement officials
3. Educate users about privacy standards by way of user-friendly layered privacy notices
4. Empower customers to control their own privacy where possible through embedded product features and other tools such as spam filters

9 This lawsuit was ongoing at the time of publication. AT&T, Verizon and Bellsouth did not participate in this study
10 The individual in question, Chinese journalist Shi Tao, remains in prison as of the time of this report's publication

11 F&C telephone interview of Yahoo, 25 August 2006
12 See http://www.microsoft.com/mscorp/twc/privacy/default.mspx
13 F&C telephone interview of Nokia 20 August 2006

Responding to the outside world

It is increasingly evident that the spread of technology has immense benefits for economic development, particularly in emerging economies. For instance, mobile telephony can have dramatic effects in re-generating rural areas. Mobile phones, provided at low cost, are transforming parts of rural India and elsewhere in areas where the capital cost of introducing fixed-line telephony is prohibitive. Similarly, extending Internet service to emerging economies and bridging the digital divide has undoubtedly brought immense benefits to many previously isolated communities.

The challenge

While the sector's positive contribution to development should not be underestimated, its more concerning impacts have slipped below the radar screen because of its historically "clean" image as an industry with relatively benign impacts on the environment and society. More recently, the TMT sector has come under heightened scrutiny from a variety of stakeholders, including customers, media, civil society groups, regulators and investors.

Key challenges are as follows:

Network Operators

These operate in highly regulated markets and touch the lives of millions of customers on a daily basis. As external expectations intensify, operators must increasingly:

- Respond to the opportunities to make significant development contributions in rural areas of poorer nations by extending telecommunications services
- Offer innovative products that are often one step ahead of the regulators, while still meeting customer expectations for taste, decency and quality of content
- Balance competing demands from, on the one hand, law enforcement authorities to assist in collecting evidence to fight crime, and on the other hand, from customers and civil society to protect confidentiality and civil rights

Hardware Manufacturers

These face customer and competitive demands for new products that can store and distribute new forms of data and content. The push for rapid innovation may lead to:

- Pressure rapidly to deploy new products that can store and manipulate data, while limiting the incidence of lawsuits or media scandals triggered by privacy and security concerns

Software and Service Providers

These need to be highly nimble in order to respond to the latest consumer trends in media and content. They operate in a weakly regulated market where rules tend to lag innovation and customer expectations are not clearly defined. Software producers must therefore contend with:

- Unclear or mixed messaged from customers and civil society regarding how software companies can balance the competing demands to offer access to the widest diversity of content while at the same time protecting customers from online privacy and security threats
- Little guidance from regulators, either locally or globally, regarding privacy and security requirements

Customers demand product innovation and ethical conduct

Customers of TMT companies often want to have their cake and eat it, too. Customers demand innovative products to exchange or access information, yet they also expect companies to promote freedom of expression, protect customer privacy and ensure data protection. Getting to grips with these myriad, and often conflicting, external expectations requires TMT companies to engage actively in the debate on what constitutes appropriate ethical conduct and a manageable pace of innovation.

Regulatory standards vary greatly and may be unclear

The plethora and pace of new content coming to the public through different technologies outstrips the regulators' ability to oversee it. It is usually the case that regulation is developed only after new technologies and associated products have entered the market-place. Moreover, by operating internationally, companies find themselves exposed to different, often inconsistent law enforcement regimes, while offering products that by their nature transcend boundaries. Where legal standards governing Access, Security and Privacy exist, these are often developed at the national level and create potential conflicts and uncertainties for companies trying to operate across a number of markets. This may leave companies vulnerable to legal risks.

The EU has worked to harmonise data privacy standards across member states, but actual practice and regulation still vary greatly. The US is still home to a patchwork of state and local standards, while standards in emerging economies such as Brazil are only nascent. Safe Harbour laws between the US and the European Union impose limitations on the transfer of sensitive data and the locations where they can be stored. Such harmonisation of data security standards provides companies with the assurance that data stored in either jurisdiction are equally safe. Unfortunately, such cross-jurisdictional agreements do not exist which poses a significant challenge to outsourcing further into high-growth data management locations such as India.

Even where legal standards do exist, in many cases companies are unclear as to what legislation applies to them, or have failed to put adequate resources in place to ensure compliance. According to the 2006 *Chief Information Officer Survey,* approximately 30% of firms admit that they need to be in compliance with a specific set of security and privacy laws but are not. 31% of companies say they are not in compliance with the UK's Data Protection Act, 45% are not in compliance with the EU Data Privacy Directive, and 18% are not in compliance with California's security breach notification law.[14]

Faced with this degree of regulatory uncertainty, companies require particular skill and expertise to avoid the pitfalls of regulatory clampdown and liabilities.

Public calls for accountability

The last four years have seen rising calls by civil society and NGOs for TMT companies to be held to account for their impacts on society at large. Global advocacy group including *Reporters without Borders, Amnesty International,* and *Human Rights Watch* have all published reports criticising the sector's role in limiting freedom of speech, and have launched campaigns against specific companies for what they consider to be "complicit in human rights abuse."[15] This has been fuelled by intense global media coverage, which is unsurprising given the vital role TMT plays in enabling the media to exercise their role. It has now also entered the realm of global political discourse, as a result of TMT being tagged by UN Special Representative on Human Rights John Ruggie as a sector with heightened human rights concerns stemming from ASP issues. These issues can only increase as the TMT sector replaces traditional print publications and television and radio broadcasting, which had previously been subject to significant legal and regulatory restrictions that are impractical for the new technologies. The TMT sector therefore faces the challenge of engaging these actors in a dialogue aimed at reaching a shared understanding of its role and responsibilities in relation to ASP issues. Only this will prevent a backlash that could overshadow what is otherwise widely considered as the sector's highly beneficial contribution to society.

Investors seek assurance about long-term business prospects

In their quest for optimum portfolio returns, investors look at stocks both individually and in relation to the overall portfolio composition. In order to minimise risk for a given level of targeted return, fund managers seek to diversify across different sectors. TMT as an industry is growing faster than GDP and undergoing tremendous technological change. Unlike in some other sectors, clear winners and losers are emerging depending on their ability to innovate.

While their business drivers differ substantially, the three subsectors' operating environments share key features:

- **High brand recognition is high:** reputation counts
- **Ongoing consolidation and dominance of a handful of key players:** scale matters
- **Technological change:** innovation drives demand and profit
- **Emerging markets growth potential:** choosing the right partners and acquisition targets is crucial

Investment is growingly heavily in emerging market TMT companies as well as in Western market companies with emerging markets exposure, resulting in ever greater exposure to ASP risks.

Investors expect companies to disclose any significant business risks, including those associated with ASP, and demonstrate that these are being managed properly. These include any potential reputation or litigation risk to the business.

The extent to which the investor community will be sensitive to wider risk issues such as ASP is likely to increase, because of a growing awareness of the impact of ESG risk factors on financial performance. This is evidenced by the fact that 130 large pension funds and asset managers, who collectively manage over US$6 trillion, have signed up to the United Nations' Principles for Responsible Investing (PRI). In doing so, these investment institutions, which include F&C Asset Management, have committed to incorporate ESG factors into their investment analysis and decision-making processes.[16] F&C has long been engaging its investee companies on ESG matters through the exercise of voting rights and through direct dialogue.

TMT companies therefore need to ensure that their response to ASP risks properly addresses the concerns of investors, who will tend to see them through the prism of brand value, competitive positioning, regulatory risk and political risk. Companies that are perceived to fall short in this area risk meeting the fate of **Cisco Systems,** which, at its 2006 shareholders' meeting, faced a shareholder proposal on its ballot calling on the board to report on steps the company might take to reduce the risk that its products would be used to limit access to the Internet or impinge on freedom of expression and the right to privacy.[17] The vote garnered an exceptionally high level of support, at 29% of the tally. It followed a similar proposal from the previous year, which had already received 11% support;

14 The Global State of Information Security 2006, CIO magazine, 15 September 2006

15 *The Internet Under Surveillance,* Reporters Without Borders, July 2004, www.rsf.org; *State Control of the Internet in China,* Amnesty International, November 2002, and *Controls Tighten as Internet Activism Grows,* January 2004, www.amnestyusa.org/business/censorship.html; *"Race to the Bottom" Corporate Complicity in Chinese Internet Censorship,* Human Rights Watch, August 2006, www.hrw.org/reports/2006/china0806

16 http://www.unpri.org/principles/

17 The resolve clause of the proposal filed by Boston Common Asset Management asks that "Shareholders request the Board to publish a report to shareholders within six months, at reasonable expense and omitting proprietary information, providing a summarized listing and assessment of concrete steps the company could reasonably take to reduce the likelihood that its business practices might enable or encourage the violation of human rights, including freedom of expression and privacy, or otherwise encourage or enable fragmentation of the Internet.Board to publish a report to shareholders within six months, at reasonable expense and omitting proprietary information, providing a summarized listing and assessment of concrete steps the company could reasonably take to reduce the likelihood that its business practices might enable or encourage the violation of human rights, including freedom of expression and privacy, or otherwise encourage or enable fragmentation of the Internet." F&C supported this proposal

also a very high proportion for a first-time resolution on a new topic. However, the company's inability to convince investors that it had developed an effective response to these concerns one year on from their first protest vote fuelled concerns and led to heightened scrutiny of management by investors.

Company experience

Product development

All the companies involved in F&C's study emphasise that incorporating both access controls and security and privacy features into new product designs is vital to securing competitive advantage and to respond to customer demand for innovation.

Companies have responded to calls for better ASP management tools in various ways, including:

- **Yahoo!**'s family accounts: these allow parents to set customised limits on their children's access to sensitive content via the company's web portal. Additional tools include *SpamGuard,* to reduce or block unsolicited e-mail, and *DomainKeys,* which allow e-mail providers to verify who is sending e-mails and to ensure the integrity of the messages sent
- **Vodafone** has established the *Group Advisory Forum,* a cross-functional group of experts, including legal, security, public policy and corporate responsibility professionals, to review and advise upon the design and development of all new global products and services
- **Microsoft**'s *Windows Defender:* helps protect a computer against pop-ups, slow performance, and security threats caused by spyware* and other unwanted software. *Windows Vista, Windows Live OneCare,* and *Xbox* products include family safety features, including web content filters and/or ratings-based game restrictions. Going back to 2002, the company had made the strategic decision to focus on security and online safety issues across its products and software development processes when it launched its *Trustworthy Computing Initiative*
- **BT**'s free *BT Privacy* service: this enables residential customers to block unwanted calls
- **Motorola**'s security consulting services: these enable large customers to ensure they set up the best data management systems possible within its products
- **Sony** has established an internal group to ensure that its external developers and manufacturers integrate ASP concerns when developing products and services on its behalf. Each **Sony** business unit conducts product vulnerability testing on all externally sourced products, especially for products connected to the Internet, before starting production to ensure that there are no residual ASP vulnerabilities
- **Deutsche Telekom** requires that any new product pass six checkpoints, including ASP, before its launch. Every change to a product has to be checked by compliance, and from 2007 onwards there will be one single team advising on ASP issues across all business units worldwide
- In May 2006 **SAP** established the Governance, Risk and Compliance Management business unit, with a view to assisting clients in responding to ASP risks. **SAP** states that this is the only dedicated ASP service available on the market; its scope ranges from anti-terrorism, to anti-money laundering, to Basel II, to Solvency II, to data privacy and Sarbanes-Oxley compliance

Public policy engagement

The absence of consistent international regulatory standards on ASP creates significant business risks. **Yahoo!** for instance reports that "The application of existing domestic and international laws and regulations relating to issues such as privacy and data protection… in many cases is unclear or unsettled… Internationally, we may be subject to domestic laws regulating our activities in foreign countries and to foreign laws and regulations that are inconsistent from country to country… Compliance with these laws and regulations may also cause us to change or limit our business practices in a manner adverse to our business."[18]

This means that in addition to setting their own policies internally, companies have an interest in taking a more pro-active stance at the public policy level by engaging industry peers, external stakeholders, governments and regulators.

One promising example of such concerted action is the *Internet Content Ratings Association,* which has developed a method for applying metadata descriptors* to web pages so as to allow parental control systems effectively to filter out mature content.[19] A second initiative that is only in its infancy concerns the *Principles for Free Speech and Privacy on the Internet,* which seeks, through consultation between civil society and several companies, to develop a voluntary standard for TMT companies on how to respond to requests from government to limit access to the Internet and turn over customer data. Although the result of this initiative is yet unclear, its ambitious objectives and the high degree of participation by various stakeholders offers at the least the possibility of an industry standard to emerge for responding to requests for law enforcement assistance, whether in emerging or developed markets.

Corporate participation in public policy development has been visible in several instances to date. These include:

- **Deutsche Telekom,** who was very actively involved, along with others, in lobbying efforts concerning the EU Data Retention Directive. The Directive had, in its original form, sought to store more user data for a longer period of time, but as a result of industry intervention, now requires that data be stored for only two years, while additional data collection is not necessary
- **Microsoft,** who, together with several others, is actively lobbying in favour of pending US legislation to create a federal privacy standard that will level the playing field across the industry and resolve local and state privacy differences
- **Google** and **Yahoo!**, who, along with other Western companies operating in China, are calling on their own national government representatives to intercede at intergovernmental level to promote free access in that market
- **SAP** is collaborating with EU governments and industry partners to develop ASP standards such as those being contained in the *Global Security Alliance.*[20] Through "Deutschland sicher im Netz", an initiative sponsored by the German Ministry for Commerce and Labour, major IT vendors and consumers, such as **Microsoft, SAP, T-Online International** and **EBay** are working together to identify risks and security measures in information and communication technology

In addition, companies have begun to turn to external experts for independent perspectives on the challenges facing their business. These include:

- **Intel**, who has established an independent Privacy Review Board made up of outside experts; these review internal privacy and security policies, and ensure that new products meet those standards without unleashing new privacy challenges. The Privacy Review Board emphasises "choice" in any new product or service the company provides, enabling customers to "opt in" or "opt out" of providing non-essential data
- **BT** called upon the UK's Henley Centre Headlight Vision, an international strategic futures consultancy, to provide an independent analysis of the trade-offs between privacy and the advances in network technologies and to propose future recommendations to **BT.** Such institutional knowledge can then be built into strategic decision-making and research and development plans

Good practice

Outside pressures will always influence how companies conduct business in the global digital economy, and present opportunities for positive outreach to external actors. F&C's research points to the following good practice standards for engaging outside stakeholders:

1. Incorporate ASP reviews into research and development and product testing procedures to meet customer demands for innovation and security
2. Join with industry peers to develop common ASP operating standards where common problems exist, such as operating in countries where free speech is restricted
3. Engage with governments to develop clear ASP regulatory standards. Clearly disclose any public policy and lobbying efforts
4. Engage outside stakeholders, including critics, so as better to assess ASP risk and potential solutions
5. Incorporate ASP into existing risk management systems and internal controls, especially when expanding into new markets

18 Yahoo! Inc 2005 10-K filing
19 www.icra.org

20 See Section 5: Company experience for further details on the Global Security Alliance

Emerging good practice in managing ASP

From challenge to opportunity

While Access, Security and Privacy issues pose significant business risks, they also have the potential to be strongly positive business drivers and competitive differentiators. Consequently, the management of ASP is an integral aspect of business strategy, developed by the board and executed by management. This section sets out the responsibilities of the board as the body accountable to shareholders and ultimately responsible for the management of the company. It then summarises the operational aspects of managing ASP issues that arise both from within and from outside the business, as discussed in previous chapters.

Governance of ASP[21]

As the body responsible for setting and testing strategy proposed by the executive,[22] the board needs to ensure that emerging strategic issues like ASP are properly factored into strategy. The board delegates power to executive management to implement strategy, and receives and questions the report of the executive on the conduct of the business. Its ability to do so effectively largely depends on its composition, i.e. the quality and mix of skills and perspectives of its members and how they work together.

A well-governed company ensures that its board is fully and regularly briefed on any emerging environmental, social and governance issues, and conducts regular evaluation of the board's performance and its effectiveness in identifying any developmental needs. Assigning clear board responsibility for ASP is important, as is the effective use of external and internal expertise. While the audit committee would normally be the body overseeing ASP issues within a risk management framework, the board as a whole should receive regular reports.

The board not only sets the strategy but the tone for the company; it defines the culture and oversees the company's code of business conduct and ethics. As this study has shown, ASP issues overlap and can originate both from within as well from outside the business, thereby requiring a co-ordinated response across the business, beginning with the board. Effective communication of the board's ASP strategy is vital for ensuring its effective implementation, as is cross-functional co-operation to give justice to the complexity of ASP issues.

Based on F&C's research, the following elements of good practice for governance of ASP by the board have emerged:

1. **Factoring ASP into corporate strategy:** The board needs to keep abreast of ASP issues and ensure that the company is in a position to respond to both risks and opportunities
2. **Overseeing risk management and internal controls:** The board should receive and review regular reports from the audit committee on the effectiveness of internal controls, and assure itself that ASP is sufficiently covered by these
3. **Setting ethical standards for business conduct:** The board should demonstrate leadership in enforcing an accountable and transparent business culture, and ensure clear and effective communication of expected standards of conduct to all employees and business partners. Strategically, the board has to assure itself that early warning systems that can detect ASP risks, such as whistleblowing systems, work effectively and are available to employees and external stakeholders alike
4. **Ensuring transparency and accountability:** The board needs to ensure that the company's disclosure is timely, accurate and comprehensive enough to allow shareholders and other stakeholders to understand company strategy and management. Such disclosure ought to cover any pro-active involvement in shaping the regulatory framework, such as lobbying. Furthermore, effective communication entails making the board available for consultations with shareholders

Managing ASP issues within the business

Internal business managers will be responsible for executing the board's ASP strategy. F&C's research has highlighted the importance of clear ASP policies and management systems. What follows is a summary of indicators of good practice for managing ASP issues within the business:

Policies	**Publish company policies governing Access, Security and Privacy as they apply to employees.** These should clearly communicate what information employees can access within the company and through company networks, any restrictions on interacting with sensitive data, and company policies governing employee privacy.
	Incorporate physical security risks into traditional information and data security policies. Companies can incorporate restrictions on moving sensitive information on mobile devices, to avoid the "stolen laptop" problem. Business continuity plans should also be mapped against data security policies.
	Develop clear policies and procedures for responding to law enforcement requests. Companies need clear protocols both for assessing the legality of official requests for enforcement assistance, and for obtaining internal approvals prior to acting on such requests.
	Establish "Know Your Customer" guidelines to identify illicit or unethical activity by customers. Companies should establish protocols for identifying customers that are likely to use their products for purposes deemed either harmful or controversial, and/or which could have a negative impact on a company's reputation.
Management Systems & Oversight	**Establish cross-functional committees to manage ASP issues.** These should draw in senior staff from a wide range of disciplines in order to challenge established thinking and stimulate innovative responses.
	Develop monitoring and compliance systems to ensure that ASP issues are considered across the business. Include an ASP review process in product development and quality assurance testing.
	Conduct ASP due diligence when entering into joint ventures or business partnerships. Incorporate ASP factors into vetting procedures for third-party agents and other business partners, and any regulatory risks related to ASP when entering new markets or sub-sectors.
	Incorporate ASP issues into product design and research and development. Invest in research and development programmes that respond to ASP challenges experienced by customers.
	Ensure the ready availability of top quality legal advice to evaluate emerging legal issues such as requests for law enforcement assistance, copyright challenges, etc.
Training & Communicating	**Train all employees on the significance of ASP issues and how to identify them.** Include basic ASP training in all new employee induction training, and conduct in-depth training for employees most exposed to ASP issues. Encourage business managers to identify key ASP risks to their business and communicate those up as well as down.
	Communicate ASP case studies and lessons learned throughout the business. Guidelines on what constitutes an ASP issue should be communicated throughout the company in order to create an ASP-aware culture.

21 See F&C General Corporate Governance Guidelines available on www.fandc.com
22 It is also responsible for succession planning of both the executive and the board as a whole

Managing ASP issues that originate from outside the business

As the causes of ASP issues are often external to the business, in order to fully operationalise the board's ASP strategy, management must maintain effective communication systems with outside stakeholders such as customers, end users, regulators, and industry peers.

As F&C's research has shown, this will help protect corporate reputation, maintain user trust, and incentivise responsible user behaviour. What follows is a summary of indicators of good systems for responding to externally-driven ASP issues:

Transparency & Disclosure	**Publish company policies for limiting access to information.** Companies required to limit access to content in certain markets should clearly disclose when content has been removed from the web. Best practice is also to remove as little content as possible from as narrow a geographic region as possible, i.e. by removing it only from the local server rather than the global server.
	Use "plain English" in describing data security systems. Companies should clearly explain to customers what data are collected and how they are stored and distributed. They should offer customers the choice, where possible, to remove data or limit how the data are used. They should clearly disclose the process under which customer data could be turned over to law enforcement agencies.
	Post 'layered' user privacy policies. To ensure that consumers are properly engaged in the process of protecting themselves from ASP risks, they should not have to click through pages of legal jargon on privacy. Companies should therefore make use of 'layered' privacy policies to communicate critical privacy information, including what data collection is required and what is optional.
Education & Empowerment	**Educate customers on ways to enhance their own online experience.** Companies can offer customer tips on how they can protect their own privacy and better improve the security of their data.
	Empower customers to control their ASP experience. Give customers the choice to "opt in" or "opt out" of providing non-essential personal data. Offer customers tools to control what content is filtered within their own homes or businesses.
Engaging Externally	**Team up with industry peers to develop common standards.** Companies should work with industry partners where possible to develop common responses to ASP challenges, such as is currently underway with the *"Freedom of Speech Principles".*
	Engage external stakeholders to flag emerging ASP risks and opportunities. Companies should utilise outside expertise, including academics or civil society groups experienced in human rights, privacy and free speech to inform management about emerging risks and identify issues of concern, that can then be incorporated into customer service and product development plans.
	Engage actively with government to secure clear regulatory standards covering ASP. Companies should include ASP regulations in their lobbying strategy, and review membership in any trade associations to ensure that the companies' and the associations' public policy positions are aligned.

Conclusion

This study has set out to demonstrate that Access, Security and Privacy issues present significant commercial risks as well as opportunities to TMT companies. These companies therefore need to place ASP issues at the core of their business strategy if they are to keep ahead of the competition, anticipate customer needs and win the trust of society at large.

F&C's research has highlighted how ASP issues are very much two sides of a single coin. On the question of access, TMT companies are expected be as liberal as possible in order to safeguard freedom of expression, yet also protect their business and customers by putting up barriers to viruses, illegal content, and online predators. As regards security, companies need to develop ever more sophisticated products to satisfy customers who need protection from security threats, while at the same time responding themselves to threats to their own systems. As for privacy, TMT companies face demands from authorities to store data for longer and to relinquish user information, while at the same time having to protect customer privacy and avoid security breaches. Given the rapid expansion of the TMT sector into new markets and new technologies, ASP challenges are not only here to stay, but certain to grow in scale and complexity.

At this relatively early stage in the development of this issue, F&C's study has sought to define the challenge that faces TMT companies, and identify and collate elements of good practice that are beginning to emerge across the industry. In the process, this study has also has shone a light on some key unresolved questions:

- Given the very close interplay between Access, Security and Privacy, companies run the risk of solving one problem only to aggravate another; they will therefore need to evaluate all three in tandem when developing solutions to ASP challenges.
- Whereas security threats may more easily lend themselves to technical solutions, privacy and access issues force companies to interact with entities where the standard rules of business no longer apply. This requires careful negotiation with governments and other stakeholders, which opens the door to competing opinions, values and legal norms, particularly in the trans-national sphere, which TMT products inhabit by their very nature. Where does corporate responsibility end and customer or government responsibility begin?

This study has identified some standards of good practice that have emerged for managing ASP risks and opportunities. However, these are not yet the norm across the industry. Companies will need to evaluate their own business practices to ensure that their ASP management capabilities are sufficiently developed and internal roles and responsibilities clearly defined.

If the way forward is for TMT companies to engage the external stakeholders who shape the landscape in which their business operates, what role should these counterparts play in achieving a productive progress? F&C believes that prudent investors should focus on the extent to which ASP issues can shape the long-term commercial prospects of the TMT companies in which they invest. This means gaining a thorough understanding of the following:

- What ASP risks have been identified as being significant to the business?
- How are ASP concerns factored into company strategy, including product development?
- What corporate ASP policies have been developed and how are these communicated in order to establish an ASP culture?
- What systems and internal controls are in place to ensure that these risks are managed?
- How is the company working with other stakeholders to establish broad-based ASP standards?
- Has the company identified good practice standards, such as the ones referenced in F&C's ASP study, against which it benchmarks its practices?

F&C believes that ASP issues will be a key determinant in shaping the commercial success of the TMT companies in which it invests. As such, it will engage on a one-to-one basis with the companies in its portfolios to encourage effective management of ASP risks and opportunities, with a particular focus on the extent to which they meet the good practice standards outlined in this report.[23] In addition, given the complexities inherent in addressing the industry-wide, multi-stakeholder and trans-national implications of ASP issues, F&C will actively contribute its shareholder perspective to multi-stakeholder efforts aimed at fostering the development of effective ASP standards.

Acknowledgements

We would like to thank the following individuals and their colleagues for their time and involvement with this study.

BT
Chris Tuppen, Head of Sustainable Development and Corporate Accountability
Susan Morgan, Sustainability Manager

Deutsche Telekom
Ignacio Campino, Vice President Corporate Sustainability and Citizenship

Ericsson
Elaine Weidman Grunewald, Director, Corporate Responsibility

Google
Peter Fleischer, Privacy Counsel – Europe

Intel
Malcolm Harkins, Director of Information Security and Business Continuity
David Hoffman, Group Counsel and Director of Privacy and Security Policy

Microsoft
Chuck Cosson, Policy Counsel
Dan Bross, Senior Director, Corporate Citizenship

Motorola
Bill Boni, Corporate Information Security Officer
Tim Harr, Senior Counsel
Tama McWhinney, Corporate Communications
Dan Swartwood, Data Protection Officer
Sheila Voth, Manager, Corporate Responsibility
Jim Wyatt, Director, Global Trade Compliance

Nokia
Anne Klemetti, CSR Manager;
Pia Vapaavuori, LL.M Data Protection Law

SAP
James Farrar, Vice President Corporate Citizenship

Sony
Hidemi Tomita, General Manager, Corporate Social Responsibility Department

Telecom Italia
Paolo Nazzaro, CSR Director Telecom Italia Group

Vodafone
Charlotte Grezo, Director of Corporate Responsibility
Stephen Deadman, Executive Solicitor

Yahoo!
Michael Samway, Vice President & Deputy General Counsel
Marta Nichols, Vice President, Investor Relations

We would also like to thank:
Dunstan Hope (Business Social Responsibility)
Tony Stoller, CBE (Joseph Rowntree Foundation, Radio Authority, OfCom)
Colin Maclay (Berkman Center for Internet & Society, Harvard Law School)

Contact us

+44 (0) 20 7628 8000

+44 (0) 20 7770 5487

www.fandc.com

For further information on this report please contact:

Claudia Kruse
Associate Director, Governance & Sustainable Investment
claudia.kruse@fandc.com

Alexis Krajeski
Analyst, Governance & Sustainable Investment
Alexis Krajeski@fandc.com

UK
Michel Bernard
(Client Servicing)
michel.bernard@fandc.com

Simon Males
(Consultant Relations)
simon.males@fandc.com

France
Bruno Moneron
bruno.moneron@fandc.com

Germany
Claus-Dieter Heidrich
claus.heidrich@fandc.com

Ireland
Graham Brooks
graham.brooks@fandc.com

Netherlands
Anja Meijer
anja.meijer@fandc.com

Portugal
Joao Santos
joao.santos@fandc.com

Switzerland
Christian Zeitler
christian.zeitler@fandc.com

USA
William Boardman
william.boardman@fandc.com

Private Investors: **+44 (0) 8000 085 2752**

F&C Asset Management plc
Exchange House, Primrose Street, London EC2A 2NY, United Kingdom
Tel: +44 (0) 20 7628 8000 Fax: +44 (0) 20 7835 2134

www.fandc.com

F&C Investments

Expect excellence