Privacy and Data Protection

Understanding the risks & opportunities for companies and their investors in the digital age.

Standard Life Investments

December 2015

Executive summary

Alix Chosson
Analyst, Responsible Investment

The right to privacy is not new - but our understanding of the concept is changing in the digital world. Telecommunications have reshaped our economies and societies, bringing tremendous benefits in terms of economic development and the advancement of democracy, but also creating new risks. Data underpins the functioning of our economies and society. The availability, use and, consequently, value of personal data in the digital space have grown exponentially and should further multiply with the growing number of connected objects. Along with business opportunities, it also creates new responsibilities and data management challenges for companies.

Why is data protection and privacy a growing risk?

Big Data and the transition to data-driven economies

Data underpins the functioning of our economies and society. The ability to collect, store and process data is growing at an exponential rate, meaning that the amount of all kinds of data available multiplies considerably every year. According to the Progressive Policy Institute, data-related products and services have generated about 30% of real personal consumption growth since 2007. Despite this, the rise of data-driven economies is only in it's infancy. According to IBM, the amount of information in the digital universe will grow tenfold between 2014 and 2020.

An increasing number of companies are collecting and processing personal information to assess past and current business trends, build customer profiles and provide predictive analysis. Big Data is changing the way companies operate and compete by enabling quicker and smarter decision-making processes.

As data becomes a vital asset for companies, data management is critical. In particular, the collection and processing of personal data requires specific privacy and security safeguards, depending on where the data is sourced, its nature (personal/anonymous) and the purpose of use. Potential solutions include de-identification, data minimisation and users' explicit consent, especially when personal data is to be transferred across jurisdictions.

The development of Big Data has been a catalyst for the growth of targeted services, including targeted advertising, targeted offering and tailored pricing. Although positive, in theory, to better meet customers' needs and improve access to numerous services, the use of personal data to profile customers bears numerous privacy risks and challenges to business ethics. This includes, for instance, the risk of discriminatory practices in housing, credit, insurance, employment, health and education.

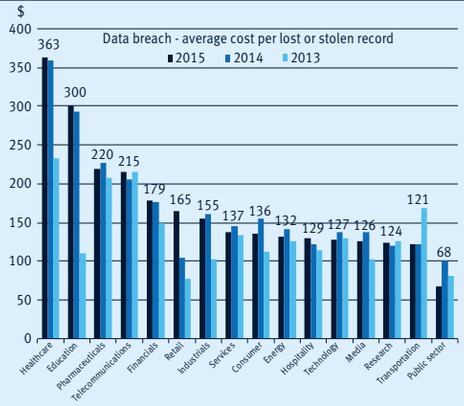
Ultimately, most of these questions are underpinned by the need to protect individual freedoms while promoting innovation and economic development. A report on Big Data, released by the US government White House in September 2014, concluded that addressing privacy risks was critical to unlocking the benefits of Big Data analytics.

Increasing number and severity of data breaches, new regulation

The risks of data mishandling and data breaches are increasing, with the occurrence and the impact of these incidents rising year-on-year. The causes of data breaches are multi-fold, from human error to criminal attacks, but also insider theft or internal systems failure. Most often, however, it is simply a combination of errors and system weaknesses. For companies, breaches can result in direct remediation and litigation costs, as well as far-reaching impacts in terms of reputational damage and loss of business.

An annual study on the cost of data breaches, published by IBM and the Ponemon Institute, concluded that a data breach cost on average $3.79 million in 2014 (when both direct and indirect costs are accounted for), representing a 23% increase since 2013; while the average cost per lost or stolen record was $154.

Chart 1: Data breach



Source: IBM/Ponemon Cost of Data Breach 2015

Regulators are imposing stricter requirements when it comes to disclosing data breaches to affected customers. This should result in increased reputational impact for companies affected by a breach, as well as potentially increased costs.

In the US, several proposed laws are being discussed to provide a robust federal framework regarding data and security breaches. In Europe, the new EU GDPR should make breach notification to all affected parties "without undue delay" a legal duty. This will be the first general personal data breach notification applicable across sectors. Only a few sectors currently have a data breach or disclosure obligations in Europe (including telecom and banks).

A recent decision from the London Court of Appeal - Google v. Vidal Hall - could constitute a landmark ruling for the recognition of privacy rights in Europe and data breach compensation. In March 2015, the Court ruled that three UK claimants could sue Google over cookie privacy violation (the so-called "cookiegate" scandal that took place between 2011 and 2012). The judges qualified the misuse of personal information as a tort, and entitled for the first time the claimants to compensation for emotional damage, even if no pecuniary loss was proven. This landmark decision could have significant impacts in terms of data breach compensation claims, especially as the EU General Data Protection Regulation will make disclosure of data breaches compulsory.

Snowden's revelations – data sovereignty/localisation

In June 2013, Edward Snowden, an ex-NSA contractor, leaked to the media top secret documents evidencing the mass scale of US intelligence agencies' surveillance activities under the PRISM programme. This included collecting telephone record of tens of millions of Americans, tapping into the servers of US internet giants and spying on foreign officials, on the grounds of national security concerns. In addition to the public outcry in the US and around the world, these revelations have provoked a significant reshuffle in the technology, media & telecommunications (TMT) sector. US tech companies, accused of helping the NSA, suffered most of the collateral damage in terms of business and reputational loss.

The unveiling of massive government surveillance programmes in the US and other countries has given further traction to data sovereignty concerns. It also created a distrust gap between TMT companies and their customers that will require time, investments and transparency to overcome. A recent decision by the European Court of Justice that invalidated the Safe Harbour Scheme, the agreement through which most US companies were transferring data from the EU to the US, evidenced the far-reaching impacts that Snowden's revelations have had for telecom, media and technology companies - and many more beyond.

In reaction to the Snowden revelations and to rebuild trust with their customers, US companies have had to rethink the services they propose, especially around cloud solutions, to integrate data localisation. Many cloud computing providers have committed to build data centres located in the country where they are collecting and storing data. In some countries, data localisation is already a legal requirement.

This reorganisation increases strategic and operational complexity and incurs increased costs for global companies. It also means that some companies can be subject to conflicting legal requirements regarding data protection and privacy. Demonstrating thorough data protection processes is therefore a key market differentiator for cloud services providers.

Changing customers' and internet users' attitudes to privacy

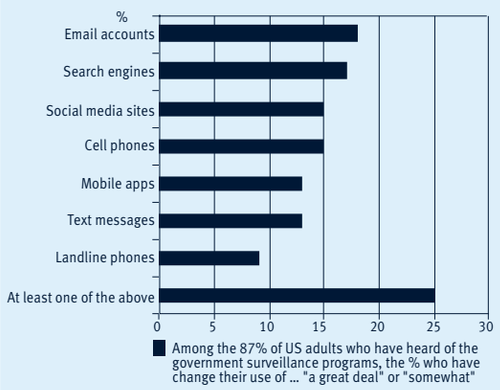
People are gaining awareness of how their data is collected and used, as well as the value of their personal information in the digital space. A growing number of internet users are taking active steps, or changing their digital behaviour, to protect their privacy and control their 'digital footprint'. This phenomenon accelerated after the Snowden revelations. Ensuring data protection and privacy is becoming crucial for customer-facing and digital companies to inspire customer trust and loyalty.

A 2014 study conducted by Symantec in several European markets shows that:

- 81% of consumers surveyed across Europe think their data holds a certain amount of value
- 32% of the respondents believe personal data is being used to improve customer experience
- 70% think their personal data is being sold to third-parties for profit
- 74% of European respondents think it is unfair that companies are making money from their personal information
- 66% of the respondents would like to better protect their personal details but are not sure how to go about doing this.

We are seeing some similar trends in the US. The outcry provoked by Edward Snowden's revelations has played a significant part in shifting attitudes towards technology companies and social media. A recent report published by Pew Research Centre examined American's digital privacy-related perceptions and behaviours post-Snowden (See Chart 2).

Chart 2: Surveillance driving change



Source: Pew Research Center, GfK (as of January 2015)

The study showed that 25% of those who were aware of the surveillance programs have taken at least one step to hide or shield their information from the government. Further, 25% of those who are aware of the surveillance programmes say they have changed how they use various technological platforms 'a great deal' or 'somewhat'.

The way people use the internet and protect themselves against digital risks is changing as they become aware of the tracking devices used to collect data. A meaningful example is the increasing use of the 'do not track' option when browsing and ad-blocking tools. A study by Adobe and PageFair in 2014 showed a 70% growth in the use of ad-blocking technologies, accounting for around140 million people or 5% of internet users.

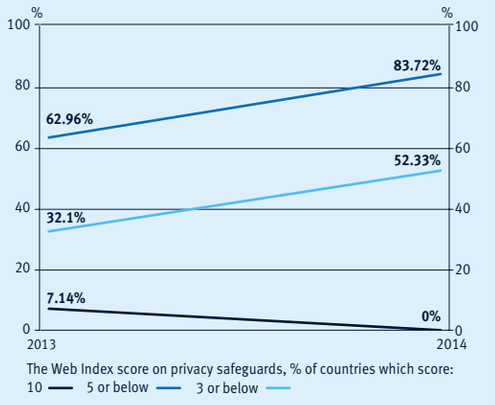
The development of new services producing and using a bulk of personal data (the internet-of-things, mobile payment, the development of wearables) will increase privacy and data security risks.

Increasing regulation

Regulation around privacy and data protection is in its infancy and extremely sector and country-dependent. It is also, by and large, unfit for the challenges of the Big Data era. Regulators in most OECD countries have committed to enhance privacy safeguards and data protection requirements, but laws take a long time to enact as legislators have to strike a difficult balance between privacy rights, national security concerns and the promotion of innovation and digital growth.

Legal safeguards against surveillance remain weak in most countries, OECD or non-OECD, and the situation is generally deteriorating. According to the annual study conducted by the Web Index, the percentage of countries where privacy safeguards were 'weak' or 'non-existent' increased from 63% in 2013 to 83% in 2014.

Chart 3: Legal safeguards against surveillance



Source: The Web Index (as of 2014)

Europe has been the strongest advocate for privacy rights. The coming EU General Data Protection Regulation (EU GDPR), replacing the current directive, will be a landmark piece of legislation for data protection and privacy. It will also have far-reaching implications well beyond Europe's borders. This regulation is directly applicable in all countries (as opposed to the current directive) and will increase companies' obligations and liabilities when it comes to collecting, storing and processing personal data, resulting in increased costs. The disruptive effect of this legislation is very difficult to assess at this stage and will depend greatly on several questions, such as the definition of personal data, what meaningful consent means and how the actual law is enforced.

EU GDPR - Changes and new requirements

- The regulation will apply directly in all EU member states (contrary to the current directive)
- One-stop-shop for data privacy regulatory supervision
- Obligation for companies to appoint a data protection officer
- Privacy Impact Assessment as part of a broader privacy compliance program (policies, processes and audits)
- Privacy by design: data protection safeguards should be integrated in product development
- Increased fines: up to €100 million or 2% of annual worldwide turnover
- New extra-territorial scope: the law applies to non-EU based organisations that process data from EU citizens
- Meaningful consent: consent must be freely given and obtained for a specific purpose – however, recognising that "explicit consent" is not always achievable
- Data breach notification: compulsory and to be reported "without undue delay"

The US has historically taken a soft-law approach to data protection and privacy issues, with the underlying intention not to restrain innovation and digital growth. Industries handling sensitive data, such as banking and healthcare, have more stringent regulatory requirements. In addition, some states have enacted specific privacy laws, creating a patchwork of legal obligations. However, the multiplication of data breaches, the revelation around mass surveillance and the consequent changing attitudes toward the internet and privacy among the American population forced the US government to take action at federal level on privacy and data protection. In 2015, President Obama proposed the Consumer Privacy Bill of Rights, setting basic safeguards on the way data is collected and used for commercial purposes, including new requirements in terms of transparency. The bill should also underline the role of the Federal Trade Commission as enforcer of data protection and privacy requirements. Although the bill was eventually opposed by the US Congress, it paves the way for future privacy regulation and highlights what companies should aim for. Pressure will surely keep mounting on this matter.

Some emerging markets, like China and Brazil, are working on new data protection regulation. This is still to be fully defined and implemented but, once it is, it should ultimately reinforce regulatory oversight and legal sanctions. In particular, the new Draft Bill of Law on the Protection of Personal Data published by the Brazilian Ministry of Justice in January 2014, strongly inspired from the EU regulation, goes quite far in the level of rights and protection given to individuals and what is asked from companies.

Privacy and data protection – what should we expect from companies?

Having meaningful data protection and privacy safeguards is paramount for maintaining customer confidence, protecting operations and complying with legal obligations. It is also a critical aspect of companies' cyber-security strategies, with three central pillars: technology, people and processes. Lastly, it is increasingly a way for the most advanced companies to build trust, engage with customers and ultimately enhance brands and products.

At the moment, the digital/data value chain is characterised by a lack of transparency on the flows and processing of data, including personal data. We believe that data brokers, who have thrived on the opacity of the data use and flows, will be among those most affected by new regulatory requirements in Europe and, to a lesser extent, the US. Providing transparency on when and how personal data is collected and processed will be one of the main challenges for companies operating in the digital space.

Businesses that give sufficient consideration to privacy matters tend to move away from a purely compliance-driven approach. More and more, companies understand that privacy is a way to build trust and to engage with customers - to the ultimate betterment of their brands and products. Many TMT companies now integrate "privacy by design" in their product development, something that should be further encouraged when the new EU GDPR comes into force.

Best practices are included below.

- Accountability and ownership of the issue at top management and board level. Best practices include having a Chief Privacy Officer or Data Protection Officer (this will become mandatory under EU GDPR).
- Certification: ISO 27000 family. ISO 27001 is a certification recognising best practice in terms of information security management systems. This certification is much broader than privacy but it relies on the appropriate management of data, which includes personal data. It is, however, only a management standard based on risk assessment and not a certification on the quality of IT security.
- Privacy by design in product development. This is a proactive approach to privacy that promotes privacy and data protection from the beginning of product development. It includes conducting Privacy Impact Assessments and making sure that personal data are systematically protected throughout the data 'value chain'. Privacy has to be embedded in the design and architecture of IT systems, including when using external parties.
- Data minimisation/privacy by default. This entails minimising the amount of data collected and the time during which the data is retained, to the minimum to perform business purpose and legal requirement. This is embodied in data protection legislation and should be further emphasized with the advent of EU GDPR. Of course, this is, by nature, at odds with Big Data, which involves collecting as much data as possible.
- Anonymisation /de-identification. This especially applies to companies collecting or using sensitive personal data, such as healthcare records or financial information. In theory, data that has been fully anonymised/de-identified (i.e. removal of personally identifying information) is considered free from privacy risk and can be used in the public domain, as well as for commercial purpose. In practice, fully anonymising/de-identifying personal data can be complex and costly, depending on the nature and ultimate use of the data.
- Encryption: sensitive personal data should be encrypted when transferred and stored appropriately, in order to limit the risk of data breaches.
- Employee training. Training is one of the vital aspects of creating a 'privacy culture,' as it helps raise awareness as to the importance of privacy and data protection. All employees should receive annual training on data security and privacy, including basic understanding of risks and regulation. Specialist positions involved in data management should be provided with extra training, including data protection rules relevant to their job.
- Data Security Inspection/audits on operations and suppliers. With most companies using third parties to collect, store and/or process data, inspection/audits are also an essential component for data security.

Opportunities

The way companies deal with their customers' privacy is becoming a market differentiator in many sectors. Customers are also increasingly basing their decisions on notions of privacy, including demanding that their data is securely stored and not given to third parties without prior consent.

Companies offering privacy-enhancing solutions - including encryption and crypto-hardware, data hiding tools ('do not track', ad-blocking, etc.) and enhanced protection for cloud solutions - should benefit from more stringent regulation and individuals' increasing awareness and expectations on privacy matters. A report published by Gartner in 2014, forecast that the cloud-based security services market could reach $4.13 billion in 2017. As technology and digital behaviours evolve, so too must security and data protection measures. These changes can be rapid – making it difficult to identify tomorrow's tech winners today.

Some companies have already created tools to empower customers on the management of their personal information, including privacy dashboards and commitments not to send information to third-parties. This is especially the case in the telecoms sector. Enhancing customer engagement on privacy is also a better way to collect higher-quality and, therefore, more valuable data.

Key questions for companies

Governance

- Is there ownership at top management or board level on privacy and data protection issues?
- Does the company have a Data Protection and/or Privacy Officer?

Processes and due diligence

- Is the company certified ISO 27001 or other certification from the ISO 27000 family (depending on activity)?
- Does the company conduct privacy impact assessment regularly on existing services and systematically before developing new products and services?
- Does the company conduct data security inspection on its own operations and at contractors and suppliers?

Upcoming regulation

- Is the company prepared to implement the new requirements from the EU General Data Protection Regulation?
- For US companies: what is the impact of the invalidation of the Safe Harbour scheme? Does the company believe it has policies and management systems in line with the new requirement from the EU General Data Protection Regulation?

Management of personal data

- Does the company have a privacy policy that is publicly available?
- Does the company sell or provide personal data (non-aggregated, non-anonymised) to external parties?
- Does the company use a data minimisation approach when processing personal data?
- Does the company use de-identification methods when processing personal data?
- Does the company allow customer / users to access their personal data? Does the company delete data after a certain amount of time?
- Does the company use encryption technologies when transferring critical data?

Data breach

- What is the company's policy on data breach disclosure?
- Has the company experienced a significant data breach in the last year and has the cause/weakness been identified?

Conclusion

The self-regulatory and borderless nature of the digital space has been a strong catalyst to the Internet revolution. However, as digital technologies increasingly underpin everything we do and the way public and private organisations function, regulators across the world are taking steps to set-up new rules of the game. This exercise is not easy, as legislators have to strike a difficult balance between privacy rights, national security concerns and the promotion of innovation and digital growth. It is, however, extremely likely that we will progressively see the emergence of a new set of digital rights (e.g. the right to be forgotten) that could have massive implications for digital companies' business models. Globally and across sectors, higher data protection requirements and obligations will result in increased compliance costs and litigation risks for companies. They will also add complexity for businesses operating globally, especially when privacy requirements differ between jurisdictions.

The technology sector is characterised by a lack of transparency around data management. As regulation is growing and users are increasingly aware of the privacy risks associated with their digital activities, TMT companies will need to provide greater transparency on the collection and processing of personal data in order to maintain customers' trust. Reputation is a key asset in the digital space, where the value of a business is largely driven by the number of users or clicks.

The benefits that the internet has brought to the world are undisputable. However, digital companies can no longer hide behind socio-economic benefits and need to take responsibility to ensure the safe use of their products. Rebuilding reputations and customers' trust involves providing greater disclosure on individual business models, including data management practices and empowering internet users and customers on controlling their personal information. We will continue to engage actively with companies operating in the digital space to promote greater transparency and better practices.

Responsible investment team

Amanda Young
Head of
Responsible Investment

Alix Chosson
Analyst, Responsible
Investment

Rebecca Maclean
Analyst, Responsible
Investment

Andrew Mason
Analyst, Responsible
Investment

Katharina Lindmeier
Graduate, Responsible
Investment

EXTEL RATED No. 1 TEAM

2015 UK Leading Asset Management Firm for SRI/ESG

Important Information

This material is for informational purposes only. This should not be relied upon as a forecast, research or investment advice. It does not constitute an offer, or solicitation of an offer, to sell or buy any securities or an endorsement with respect to any investment vehicle. The opinions expressed are those of Standard Life Investments and are subject to change at any time due to changes in market or economic conditions.

Third party data services disclaimer

Any data contained herein which is attributed to a third party ("Third Party Data") is the property of (a) third party supplier(s) (the "Owner") and is licensed for use by Standard Life**. Third Party Data may not be copied or distributed. Third Party Data is provided "as is" and is not warranted to be accurate, complete or timely. To the extent permitted by applicable law, none of the Owner, Standard Life** or any other third party (including any third party involved in providing and/or compiling Third Party Data) shall have any liability for Third Party Data or for any use made of Third Party Data. Past performance is no guarantee of future results. Neither the Owner nor any other third party sponsors, endorses or promotes the fund or product to which Third Party Data relates.

**Standard Life means the relevant member of the Standard Life group, being Standard Life plc together with its subsidiaries, subsidiary undertakings and associated companies (whether direct or indirect) from time to time.

If you would like to find out more about our strategies, please visit www.standardlifeinvestments.com where you will find contact details for your location.

Visit us online

standardlifeinvestments.com

INVBGEN_15_1500_Data_Protection_White_Paper_TCM 1215