The data gold rush
Growing and protecting your position in the data ecosystem

Data is emerging from the back-office to become a major new business opportunity. Data-fever is sweeping the business world, from advertising and telecoms to financial services and energy utilities. And like the Californian gold rush, the data explosion will create its own winners and losers.
Introduction

The Data Ecosystem

Data is the commodity of the moment. Recent growth in the volume and type of data collected has been exponential, with IBM reporting that 90% of data in the history of the world has been created in the last two years.

Now being compared to previous commodity booms in gold and oil, the data boom has similarly spawned a new industrial ecosystem, creating business opportunities for entrepreneurs and established businesses alike. Cap Gemini reports that nine out of ten business leaders believe data is now the fourth factor of production.

However, unlike its forbearers, the data ‘gold rush’ is multi-faceted. Data can be broken up and collated in many different ways, easily moved across borders and organisations, and traded without huge start-up costs.

As well as creating new businesses, it is driving opportunities within and across traditional industry boundaries. Data can be used to help grow businesses and can also become an important asset in its own right.

Google and Facebook are two businesses largely built on the value of the data they hold. Meanwhile, more traditional businesses, such as retailers, have also built strong competitive advantages through their use of data to improve the customer experience. And financial services companies are sitting on a wealth of data with significant potential to create valuable new revenue streams.

Marketing

Data has brought organisations full circle in terms of how they interact with their customers. Data collection and analytics have consigned the mass marketing of the 80s and 90s to the history books. Now businesses can deliver the type of one-to-one messaging that brings real value.

Mobile and the cloud

Mobile and the cloud are conspiring to push the data opportunities one step further. Organisations can now draw on a constant, real-time and contextual flow of data from their customers and store that information for analysis at affordable costs and in significant volumes. In terms of data storage in the cloud, we are now talking in petabytes and exabytes rather than gigabytes.

Machine-to-machine

The much anticipated machine-to-machine revolution will similarly push further opportunities and bring together businesses from a variety of industries, like utilities, mobile operators and technology suppliers. Here, everyday objects such as phones, cars and household appliances can be wirelessly connected so as to share data and information and deliver an improved service or product.
Governments are also part of the data frenzy. In the UK, the Government’s open data initiative will see a flood of data from local authorities and government agencies hit the data ecosystem, opening up numerous opportunities for private enterprise.

And inevitably governments are not only collecting and sharing data, they are also trying to regulate this new ecosystem and protect the consumer on whose data much of it is based.

As with the internet itself, regulation lags technological innovation and consequently sometimes misses the commercial point. Organisations must address and plan for what is currently at worst a legal vacuum and at best a patchwork quilt of rules across different European jurisdictions, as they look to take advantage of the data opportunity.

This requires companies to establish new roles and departments within their businesses, to focus on the legal and policy impact of data collection, retention, control and security.

With these challenges and developments in mind, Osborne Clarke has drawn on its technical legal know-how and its day-to-day experience working with businesses in the data field to put together this report on managing data and the legal issues associated with it across Europe. Some key themes emerge, namely:

- The need to put data privacy at the heart of strategic decisions, and to give proper consideration to what personal information is going to be held and for how long, and how it is going to be used;
- The obligation to publish clear and appropriate privacy policies; and,
- The special considerations that need to be made where children are concerned.

The content of this report is not only driven by our own experience, but also by the views of a panel of industry experts who deal with commercial and data issues every day as part of their jobs.

Our aim is to guide our clients positively through the major legal challenges that exist in Europe, now and in the future, and to demystify the "Big Data" revolution.

We hope you find what follows a useful aide in navigating the ever-more complex data ecosystem.

Adrian Bott
Head of Digital Business
adrian.bott@osborneclarke.com
The consumer view

How do individuals think information about them should be used and managed? What value does the public put on their personal data, and in what circumstances do they approve of organisations analysing their behaviour and activities?

To find the answers to these questions we commissioned Ipsos MORI to conduct some research. The research was conducted on i:omnibus, Ipsos MORI’s online panel omnibus, between 28th August and 4th September 2012. Questions were asked online of 5,078 adults aged between 16 and 75 across five European countries (1,020 aged 16-75 in Great Britain, 1,014 16-75 in France, 1,006 16-70 in Germany, 1,024 16-65 in Spain and 1,014 16-70 in Italy). The survey data were weighted by age, gender, region and social grade, working status and main household shopper to be nationally representative for adults of the corresponding age ranges in each country. Full data tables are available upon request.
How comfortable are you about providing the following personal information to a website or search engine?

European consumers are generally much more comfortable sharing their email address than landline or mobile numbers – perhaps reflecting the less intrusive/interruptive nature of email as a medium.

While some were unsure, relatively few said they were positively uncomfortable sharing email addresses.

German consumers were much less likely to be comfortable sharing email or phone details than their counterparts in the UK, Spain, France or Italy.
Discomfort at sharing medical information may reflect concerns around its impact on insurance cover and price - among other things.

However, clearly there are degrees of sensitivity: as would be expected, consumers are less concerned about sharing details of minor medical ailments.

Some significant variance between different countries: Italians appear more comfortable sharing major/detailed medical history than are Germans in sharing data about minor medical ailments.
Are you happy to provide information about your location or details of your preferences on social activities or hobbies?

- Location
  - Comfortable: 38%
  - Don't know: 30%
  - Uncomfortable: 32%

- Interests
  - Comfortable: 13%
  - Don't know: 29%
  - Uncomfortable: 58%

**EU group** = UK Germany Spain France Italy

A significant proportion of consumers sees the benefits to be gained from sharing location data as outweighing the downsides.

However, many people remain uncomfortable or unsure - does this reflect a lack of experience of location-based services or a considered evaluation of pros and cons?

Information about social activities and hobbies is seen as much 'safer' to share than location data - where I am is seen as more sensitive than what I do with my leisure time.
The consumer view

How comfortable are you with a company collecting, storing and using information about you?*

A significant minority still feels uncomfortable allowing purchase information to be collected and used as part of a supermarket loyalty scheme.

Comparative sensitivity about location data is seen again here.

Some significant variance once more across different territories.

*Ipsos MORI

*Question asked in relation to a) what you buy in a supermarket (loyalty information) b) facial recognition information and c) information about where you are and where you’re going to?
How comfortable are you with companies storing and using your online shopping preferences?

Comparatively few consumers are uncomfortable with shopping preference information being retained and used in the online shopping environment.

The value exchange and consumer benefits of this kind of data usage appear to be appreciated.

A broadly similar response across the five territories. Although, interestingly, British consumers appear to be slightly more comfortable with offline shopping data usage.
The consumer view

What about companies using your social network contacts or your TV, film and gaming preferences?

Mobile or social network contacts

- Comfortable: 56%
- don't know: 25%
- Uncomfortable: 19%

TV film or gaming preferences

- Comfortable: 52%
- don't know: 32%
- Uncomfortable: 17%

Many consumers expressed discomfort about the idea of businesses using their social network contacts, but a significant minority was comfortable with the idea. Does this reflect a shift in attitudes to personal/social information?

Most consumers are happy with businesses using their TV, film or gaming preferences. Consumers are increasingly used to online engines serving up suggestions based on previous purchases, and appreciate this as a benefit.

EU group = UK Germany Spain France Italy

Ipsos MORI
Use of children’s data: up to what age should parental consent be required for organisations and companies on the internet to collect and record data from children?

Children’s privacy continues to be an issue of significant concern.

UK consumers seem somewhat more comfortable with a lower consent age for data capture.

Would respondents be more comfortable with lower ages for certain types of organisation, certain types of data?

---

Ipsos MORI
The consumer view

“I’d prefer if there was one area on a website where I’m kept up to date about my data, where I can chose what I share and not to share on an on-going basis”

Strong consumer support for the idea of dedicated website sections giving users real-time control over data sharing.

A significant proportion of consumers would not necessarily be deterred by a security breach. Are security breaches becoming better understood?

“I would be willing to use a company’s services after a security breach, provided I was notified in person by the company about the risk to my data”

Strong consumer support for the idea of dedicated website sections giving users real-time control over data sharing.

A significant proportion of consumers would not necessarily be deterred by a security breach. Are security breaches becoming better understood?

EU group = UK, Germany, Spain, France, Italy
The consumer view

If you chose to share your data with a company would you be comfortable if it was used for the following purposes:

- Data-sharing for the customer's benefit – service improvement or promotional offers - is broadly accepted.
- Consumers are much less comfortable with allowing businesses to sell their data.

Data-sharing for the customer's benefit – service improvement or promotional offers - is broadly accepted.
Consumers are much less comfortable with allowing businesses to sell their data.
The consumer view

Comparison of how surveyed group felt their personal data collected by companies should be used:

- Provide deals, freebies or offers in the future: 84%
- Inform that company’s future marketing activities: 50%

Consumers respond much more favourably to data usage when there’s a clear value proposition for them.
How acceptable or unacceptable do you think it is for a website to offer the same products to customers at different prices based on the personal information which they hold about those customers?

Respondents who replied “completely unacceptable” split by age and gender

- **Age of respondents**
  - 16-24: 32%
  - 25-34: 35%
  - 35-44: 30%
  - 45-54: 25%
  - 55+: 20%

- **Completely unacceptable**
  - Men: 37%
  - Women: 32%

A significant proportion of consumers are uncomfortable with differential pricing based on personal information.

Different age groups show slightly different responses on this.

Men generally seem more comfortable with differential pricing than women.
Virtual cloud services are used to manage the increasing amounts of data being collected and stored. How comfortable or uncomfortable are you with websites and companies contracting third parties to store the data you have shared with them in the Cloud?

- **Don’t know what the cloud is**
- **Don’t know**
- **Very uncomfortable**
- **Fairly uncomfortable**
- **Neither comfortable nor uncomfortable**
- **Fairly comfortable**
- **Very comfortable**

**EU group** = UK, Germany, Spain, France, Italy

Relatively few consumers are comfortable with data being stored in the Cloud. A significant minority doesn’t know what the Cloud is.
Points of view from commercial and public organisations

Data volume has been growing exponentially, and with it the availability of analysis, new technologies to gather and sift information and new regulations governing how it should be utilised. We spoke to six leading industry figures about the ways in which the ‘data gold rush’ was likely to impact on business, both now and in the future.

Expert View

James Leaton Gray, public service broadcaster:

"Both now and in the future, the value in data will be in relationship management. Knowing the likes and dislikes of the customers is the key to talking to them and keeping them as customers in an increasingly competitive world. Organisations that are willing to engage realistically in a two-way conversation with people who use their services are going to benefit far more than those that exclusively ‘mine’ their customers for short term sales and market share.

"Attitude of mind is more important than the size or database of a company. As a owners of a corner shop will remember who you are, an online company that can generate genuine connections will do far better than just identifying certain algorithms. Developing a level of understanding of the information, rather than the data mining process itself, is the most important aspect. For all the development of technology, it’s much more about the attitude, namely ‘remembering you’.

"The capacity is there to gather data on a scale never seen before and the key to the future will be the ability to analyse in a granular way that data and personalise it to a degree yet to be envisaged. For example, the advent of IPTV will bring media consumption that will define us and new levels of communications interactivity. The potential is huge and the technology within reach, but the broadband infrastructure to support it is much further away. But as the ability to manipulate data grows, so does the capacity for data loss. Data security will be key to its engagement and manipulation, as will be where you fit into a mass market.

"Legislation on data collection is driven by the idea that says that all pieces of data should be treated equally, whereas we should be differentiating and taking a risk-based approach. However, this is unlikely to be adopted, at least in the short term. Therefore one needs to take into account the different cultural responses to the collection of data in different countries."
Points of view from commercial and public organisations

Tobias Haar, General Counsel, Gameforge, Germany

"Data is certainly the gold of our times and will become ever more important to future generations. But to use the gold in your hand, the owner of such data needs to retain it and use it properly to create revenue. With IP version 6 upcoming, there will be a vast number of IT addresses to give every device its own IT address, giving ever more trackable data spread across every electronic device and building connections between those devices. The pace of change is unstoppable."

"Big data collectors such as Facebook, Google and Apple are the major beneficiaries of holding billions, trillions of single pieces of data with the potential to use it. Holders of patents for creative inventions and smart technologies to match interlinks and to anticipate trends, through analysing data, that build on these relationships will also be well placed. Given, however, the potential for vast organisations to crowd out competition, here is always the possibility that the authorities will act to prevent such monopolies in the future and break them up if they become too powerful, as happened to AT&T in the US in the past."

"The main difficulty in implementing a general worldwide approach to data collection is cultural difference; in Germany, for historical reasons, people are very anxious about personal information being collected by those they don’t know. Data collection does not stop at geographical borders, however. We need to establish common regulation of data protection, controlled through EU institutions and the EU court systems in the EU first, and later beyond. Abiding by the rules would then stabilise the global approach to data and prevent market barriers in local areas by application of different levels of data protection measures imposed on local companies competing in the global market place."

Ray Eitel-Porter, Executive Director at Opera Solutions

"The value of data is in three main areas. Firstly, the ability to increase existing sales and margins through recommending additional products, cross-selling and upselling. Secondly, new revenue streams from products/services based on insights from existing data being sold to third parties. The third area is driving cost savings and efficiencies, from more specific targeting of individuals for healthcare advice to predicting breakages and necessary maintenance for mechanical items."

"Large companies have an inbuilt advantage over small and medium companies in terms of utilising data, because the costs for advanced analytics typically have a relatively high fixed component, regardless of the volume throughput. In the future smaller companies could drive R & D innovation. As mobile technology becomes more widespread and with SIM cards increasingly embedded into machines, it will give more real time information about what people do and where they are going, providing potentially valuable information to retailers and service providers, amongst others."

"Cloud computing can handle massive amounts of data with a great degree of flexibility, running incredibly intensive processes when and where they are needed, with all the resulting cost benefits. It is important that companies define the dividing line between where predictive analytics are helpful and whether they are intrusive. Data legislation is complex to put in place across different countries and many proposed solutions run the risk of adding massively to costs. Greater consistency across countries would be useful in helping companies more cost effectively to provide consistent global / multinational solutions."
Maria Gomez del Pozuelo, CEO of Womenalia, Spain

"The value of data comes in the way it allows us to understand consumer behaviour, anticipate their needs and offer them what they really need. Accumulating and utilising the data operates the same way with every sector, every country and every company, allowing companies to build a lot of loyalty amongst our customers. It enables us to walk one step before they do.

"Data accumulation is dominated by three companies that combined know everything about our habits – Google, Facebook and Linkedin. The influence of these companies is enormous. But the importance of the data they acquire comes in its analysis, and therefore from the quality of the analysts they employ. How the right people, and enough people, interpret the data will remain an important factor in its use. In future, there will be more devices and more applications bringing information from anywhere in the world, which in turn will bring greater efficiencies to businesses as the volume of information increases. Alongside cloud communication, new technology, targeted content and online tools will be very powerful.

"The main problems in the future will stem from legislation that fails to distinguish between what is private data and what is business data, yet treats all of it the same. In Spain, for example, the cookies legislation is very onerous yet there is a disconnect between how the authorities and the users react to the use of data, with people here in general very much more relaxed than the rules allow. We need to regulate all companies under the same rules and conditions in order to compete fairly in the world. Globally, companies need to operate using the same rules of data, otherwise EU countries in particular will not be competitive and business could be driven out. At the moment, they are not the same rules and we are not playing the same game. It’s like taking part in the Olympic Games and starting ten metres behind.”

Brad Bryant, EMEA Privacy Counsel at Aon

"Part of the value of data analysis is in understanding how much information is acquired in the course of doing everyday business. Working with in-house teams and using internal resources, companies are able to collect and harness significant amounts of information about clients and their employees. If firms are able to combine this information with other sources of information, particularly from companies such as data aggregators like Experian or even social media sources then companies can develop a much deeper understanding of their client base, their employees and the risks they face doing business. A deeper understanding can lead to better, more tailored product offerings, but this also requires greater transparency and responsibility in respect of the data they hold. This can be a balancing act between offering greater client service and not using data in ways that clients may not expect. As ever the trust between firm and client remains a crucial consideration.

"Large firms understand the value of data and have human capital and data expertise to use it. They are dependent on employing the right people and building the right relationships with clients. Advancing technology is important - developing the right algorithms to identify trends in the workplace, for example – but the strongest resources are human rather than technical. Developing expertise enables firms to harness the data they have to offer more innovative product solutions."
"Taking data for one purpose and using it for another carries huge risk of reputational damage, so companies must ensure they have right type of consents up front. Firms will need to pre-empt some of the challenges proposed by new privacy legislation in the EU. Regulatory change could have a large impact on ways of doing business in the future. To prepare firms should start considering how they treat data holistically as an organisation and prepare for the requirement for greater accountability by regulators and their clients. This is both a challenge and an opportunity as taking stock of how you use data as a firm can lead to new ways of understanding and capitalising upon the data you hold."

**Global GC, Adtech and media organisation**

"Data that offers day-to-day behavioural information is very valuable. It is vital to the performance of online advertising, as it gives a strong picture of the consumer and enables an advertiser to target its offers to its desired audience, thus increasing the potential return for the cost of the advertising. For example, where there is a competitive auction for advertising space, having access to a customer’s browsing behaviour or buying history enables companies to justify a higher price, or refrain from bidding, where the value of a particular individual to certain advertisers or a particular industry can be better judged."

"In this world of real time bidding, where the value of a consumer is judged and a winning advertisement is served in a split second, building and using a database of your own is essential, although it is not cheap to do. Those best placed to benefit are those parties that make the investment in infrastructure and use it appropriately. As technology advances, the market will change, with more automation and more people investing money in real time bidding. There are successful external providers including Appnexus and Google Exchange, but if it’s your database, you own its value and you have a dedicated platform without having to rely on a third party.

"My concern is that tracking online behaviour via cookies, and thus building profiles on internet audiences, will be subject to changes in legislation that will make it more difficult to operate. There needs to be a debate about the level of data protection needed under EU legislation. Currently there is a degree of uncertainty. It should be made clear that in holding behavioural data about internet audiences, we do not hold any personal data. Rather, we create an anonymous profile without knowing who a person actually is, and provide them with advertising in which they may actually be interested. If you look at breaches of data protection law which have arisen to date, most of these breaches are much more basic, such as a lost data CD. The ideal would be to clarify the law, and also continue to better educate consumers in areas such as behavioural advertising, where consumers notice that information is being collected but are not always aware of the kind of data involved, and the level of control which is available to them."
Summary

There are clearly a number of recurring themes and concerns demonstrated in the views of those involving in data collection and handling:

- New mobile technologies to gather data, the advent of cloud computing and the ever increasing volume of data will bring new opportunities to utilise and response to the data collected.
- Information gleaned from data will remain only as good as the analysis, and the analysts, involved. Expert input will continue to be vital to assess and filter data and well-developed in-house teams and databases are likely to be key to a company’s success.
- In general, large companies and international organisations are better placed to benefit from the ‘data gold rush’. This is unlikely to change, although smaller companies may well play a leading role in technology innovation.
- Machine to machine interaction will play an important role in data gathering in the future.
- Data mining is a global process that occurs across international borders, yet the frameworks for the processing of information does not always reflect that reality.

- Legislation and regulation, particularly in the EU, currently does not address the differences between personal and business information, nor the willingness of different national regimes to allow data sharing. These are in part cultural and historical differences.
- Failure to reflect a global and equal framework for data collection could lead to companies taking their business to areas where the rules are less restrictive. Parity and an international agreement would address this, although the experts agreed this was an aspiration that was unlikely to happen any time soon.
- The ability to recognise the value of data and to exploit its value presents companies with excellent opportunities and they must seize them as they arise.
**Data – where next?**

All organisations, whether commercial or public sector, now understand that data is an asset that is increasingly valuable if properly managed. The problem is that there is no overall consensus on what proper management looks like – how data is stored and what it is used for – and that puts the whole data economy at risk of stalling.

It is clear to everybody that a change in thinking is essential. But what exactly needs to be done is less obvious. To a large extent that depends where you are standing, but even then there are ambiguities to be dealt with.

For example, governments (and therefore regulators) want to protect individuals but at the same time need to enable economic growth. Individuals want the benefits that data analysis brings but, on the whole, want their data to be secure and anonymous. Organisations want to monetise the data they hold but don’t want compliance costs to make that unrealistic.

So, given the disparity in regulation across jurisdictions, the challenge is for governments, organisations and individuals to find the balance, to reap the benefits and at the same time prevent the data economy stalling.

There is no easy answer but it is clear that trust frameworks must be at the heart of the data agenda, providing transparency on how personal data is used and a clear understanding of the incentives to stakeholders for their participation.

A recent Osborne Clarke roundtable attended by leaders from the digital business sector identified a number of ways in which organisations can help the data economy, and the ecosystem it exists within, develop:

- **Address/lobby on privacy issues**: Of the three main stakeholder groups, commercial organisations are often seen as the bad guys. That needs to stop. Organisations need to be seen to be valid participants in the privacy debate, not the stakeholder group that everybody else needs protecting from.

- **Keep data flowing**: Realising the value that data has can make organisations hold it close. That stops free circulation and is a sure-fire way to make the data economy stagnate.

- **Develop the role of the Data Protection Officer**: Key elements of the DPO role are dictated by law, but they are also in-house data experts. Their expertise and opinions are as valuable in developing organisational use of data as in ensuring compliance.
Think about the customer benefits - Data is an asset that comes at a price, and as consumers become more data-aware they will extract greater value from the organisations that use their data. The organisations that proactively consider how they compensate their customers for use of their data are the ones that will see most success.

Lead thought - The world of data is largely uncharted territory. Organisations can play a key role in explaining the issues, mapping out the future and influencing and guiding individuals and governments.

Understand the legislative roadmap - Build an understanding of forthcoming legislation and the ideas that shape it. Only then can organisations play a part in shaping its development.

Avoid cat and mouse syndrome - It is tempting to get into an ‘us and them’ mindset when it comes to regulation, but there are few scenarios that could be more damaging for businesses. Transparency will be central to the development of the data economy.

When it comes to data there are no easy answers. What is clear is that organisations need to be on the front foot in developing the data ecosystem. Transparency, balance and collaboration will be needed to meet all of the challenges ahead but one thing is for certain – the prize will be worth the effort.
A changing scene in Europe

In January 2012 European law makers announced a radical overhaul of existing data protection laws. Once finalised the changes will have a huge impact on organisations with operations in, or focused on, Europe, as will the penalties for those who get it wrong. Large fines (up to 2% of global turnover have been proposed) are being lined up for non-compliant organisations.

In short, the new laws will:

• increase the regulatory burden on organisations
• raise the stakes, in terms of potential fines and brand damage, arising from non-compliance

The new laws offer opportunities as well as challenges. Savvy organisations are preparing for their introduction now and seeking to demonstrate to their staff and customers that they respect the importance of their data and will use it in a compliant way. Best practice data processing is a key route to gaining trust and confidence.

The case for taking action now to improve data protection compliance is compelling. It will take time to ingrain the level of data governance that the new laws are seeking to set. Also, recent regulator enforcement actions, in the UK and across Europe, show that poor data governance practices are already being punished by the data protection authorities. Often this is done via the imposition of an obligation to bring in costly new processes and training schemes at short notice across not only an errant company, but also its supply chain.

Most people would agree that Europe’s data protection regulatory regime needed an overhaul. The majority of the current laws were written in 1995 in a pre-cloud, pre-offshoring world and before digital business had taken anything like the form it now has.

European lawmakers have made no secret of their desire to overhaul that regulatory regime. Recently, the EC’s botched attempt to introduce new cookie/tracking technology laws in a harmonised way has led to an additional desire for a single set of EC-drafted laws to apply across Europe.

In its draft Data Protection Regulation, published in January 2012, the EC set out the new laws that it would like to see introduced. Once these have passed through the European parliamentary system, because they are in the form of a “Regulation”, they will have direct effect in every EU Member State with minimal further scope for debate or rationalisation. That process is expected to complete in 2014/5. While a more harmonised data protection regulatory landscape sounds appealing, the uncompromising approach taken by the EC’s draft Regulation is a cause for concern for business.
A changing regulatory landscape: opportunity or threat?

Key points proposed include the following:

(a) Fines – National data protection regulators will be given the ability to impose significantly higher fines of up to 2% of global turnover.

(b) Data Protection Officers (DPO) – Companies with more than 250 employees, or whose core activities involve regular personally identifiable information (PII) monitoring, as well as public authorities, will all be required to formally appoint a DPO. The DPO must be empowered to act as an independent assessor of data compliance and report to the board in doing so. DPOs will be required to coordinate privacy by design and privacy impact assessment initiatives (see below for more details on both). Responsibility for training staff is also mentioned as important. In short, the DPO must ensure that his or her organisation has adopted good data governance policies and procedures. Affected organisations now need to consider who they should appoint as their DPO, and what training and assistance that individual should be given.

(c) Audits, privacy by design and privacy impact assessments (PIAs) – Organisations will be required to demonstrate that they have undertaken regular assessments using recognised industry standards, particularly before new processing systems and activities have been introduced. Regulators will be empowered to designate activities that should always be subjected to a PIA. The Regulation sets a starting point list that includes any activity using PII about someone’s “economic situation, location, health, personal preferences or reliability of behaviour”. Large-scale storage of PII about children is also cited.

(d) Security breach notification – Organisations will have to notify data protection authorities within 24 hours of establishing that they have suffered a data breach or explain why it is not possible to provide full details of the breach. Slick internal procedures will therefore be required to verify suspected breaches and establish what has been lost or subject to unauthorised access.

(e) Expanded consent requirements – At the heart of this change is the requirement that consent to use PII should always be obtained in advance and on an opt-in basis before it is used. If implemented the change will mean all organisations will need to review the basis on which they process data. All processing currently undertaken on an opt-out basis (including the much debated use of cookies) will need to be moved to an opt-in basis.

(f) Data portability – Individuals will be given the right to demand that an organisation gives them any or all information held about them in a format of their choice. This to increase the control that individuals have over data that identifies them, and to make it easier to transfer business or employment relationships. It remains to be seen who will be required to cover associated costs of such an exercise, but it seems very likely that the transferring organisation will be expected to do so.
A changing regulatory landscape: opportunity or threat?

(g) Jurisdictional reach – The new laws will apply to anyone processing PII in the EU and to those outside Europe who offer goods or services to EU citizens. For a multinational organisation, the location of its European HQ will determine which EU Member States’ laws bind it, and which regulatory authority will have jurisdiction over it. That said, individuals will be given wider ranging powers to bring actions personally against an organisation, either in the country where a non-compliant organisation is located or in the individual’s local courts. Trade associations will also be empowered to bring class actions on behalf of their members. Data processors will share equal responsibility for compliance, raising the stakes for IT service suppliers.

(h) Data transfers – Europe’s painful data transfer laws will be relaxed in that more options will be made available to enable organisations to make data available to non-European third parties. Specifically, the policy implementation known as Binding Corporate Rules will be formalised as a mechanism enabling data transfer compliance, which is good news for multi-site, multinational businesses.

(i) The right to be forgotten – Individuals (under-18s are mentioned in particular) will have the ability to demand that information published about them online is deleted and is not republished. Organisations that receive such a demand must take all reasonable efforts to inform other website operators of the existence of the complaint that they have received. The right, which is particularly relevant to social media businesses, is subject to some exemptions. These include one benefiting journalists publishing stories in the public interest, raising the question of whether a blogger or someone who posts an opinion on a website is a journalist or not. More questions remain about how practical the regulation is and who would bear the costs of complying with it.

(j) PII about children - A child is defined as any person under 18, although a separate limit (13) applies to the use of children’s data in the context of “information society services”, where parental consent is required, with reasonable effort made to verify that consent “taking into account” available technology.
Developments in the US

In February 2012 proposals for a "Consumer Privacy Bill of Rights" were announced. Differences in US privacy provisions as against those of other developed countries were specifically cited in the background to the Bill, which provides a blueprint for new federal-level legislation that will be enforced by the FTC.

Key provisions include:

(a) Individual control and transparency - Organisations are required to write clear, easy-to-understand privacy policies and give consumers a way to opt out of data collection. Do Not Track technology in major web browsers can make it easier for users to control online tracking.

(b) Respect for Context - Consumers will have a right to expect that organisations will collect, use, and disclose personal data in ways that are consistent with the context in which the data was collected.

(c) Security - Consumers will have a right to secure and responsible handling of their PII.

(d) Access and Accuracy - Consumers will have a right to access and correct PII in usable format.

(e) Accountability - Consumers will have a right to have PII handled by companies with appropriate measures in place to assure they adhere to the Bill.

The National Telecommunications & Information Administration is bringing together interested stakeholders, including companies, privacy advocates, consumer groups, and technology experts, to develop and implement enforceable codes of conduct that specify how the principles in the Consumer Privacy Bill of Rights apply in specific business contexts.

With regards to the regulation of PII about children, the FTC is in the process of reviewing COPPA, the main piece of US legislation regulating this area. There has been considerable consultation with industry, and proposed changes could widen the definition of PII to include online user names. There are also proposals to tighten up the mechanism for obtaining consent, with 13 currently the age below which parental consent is required, though this may be amended.
Country focus: The United Kingdom

Open Data – public sector data bonanza

In June 2012, the UK Government published a White Paper summarising its open data strategy, entitled ‘Unleashing the Potential’. The Paper sets out a vision for opening up access to data held by the public sector to 2015 and beyond – a step that could significantly fatten the big data calf.

The paper sets out a range of measures the Government intend to take. Two obvious implications arise for private sector organisations, namely:

• Organisations working closely with the public sector should be aware that Government departments and other institutions are going to be increasingly open to scrutiny. Sufficient safeguards for commercial or other sensitive data will need to be ensured as the changes take effect. For example, the Government is introducing a ‘presumption to publish’ data for all public sector institutions. Each institution is producing an Open Data Strategy stating the datasets it intends to publish over the next two years.

• For some businesses, the increasing availability of public sector data will mean a commercial opportunity. One of the Government’s stated aims of the transparency programme is to boost economic growth: public sector institutions are required to set out in their Open Data Strategies the way in which they would “stimulate a market” for the use of the data being published. Included in the White Paper are initiatives to facilitate the use of public sector data, for example the creation of a new requirement that public sector institutions promptly make data available in a usable format.

Whilst commendable in its aims, the initiative leaves a number of questions unanswered, not least how data accuracy standards will be guaranteed. Data made available by a public sector body may well have been sufficient for the purposes for which it was originally collected, but it is not clear how the public will be protected if those purposes mean the data is not fit for other uses.

Given the number of companies operating in newly privatised sectors, it will also be interesting to see whether the Government’s definition of public sector, in terms of which organisations are required to make data open for use, is in line with commercial expectations.

Finally, privacy campaigners are increasingly questioning how the ‘mosaic effect’ of privacy infringement (i.e. the possibility of identifying individuals from released data by collating and analysing information from several sources) will be protected against.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdS</td>
<td>System administrators</td>
</tr>
<tr>
<td>AEPD</td>
<td>Agencia Española de Protección de Datos, the Spanish data protection regulator</td>
</tr>
<tr>
<td>Appending</td>
<td>Combining personal data held about a customer or prospective customer with data about that person from third party sources</td>
</tr>
<tr>
<td>Article 29 Working Party</td>
<td>The European Union working party made up of a representative from the data protection authority of each EU Member State</td>
</tr>
<tr>
<td>Big data</td>
<td>Datasets which are too large to be gathered, stored, managed and analysed by typical software tools</td>
</tr>
<tr>
<td>Database Directive</td>
<td>Directive 96/9/EC on the legal protection of databases</td>
</tr>
<tr>
<td>Data impact assessments</td>
<td>Analysis of an organisation's activities which may have implications for individuals' privacy. Also known as a privacy impact assessments.</td>
</tr>
<tr>
<td>Data minimisation</td>
<td>The practice of collecting and using the minimum amount of information possible.</td>
</tr>
<tr>
<td>Data Protection Directive</td>
<td>Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data</td>
</tr>
<tr>
<td>Data Protection Regulation</td>
<td>Draft EC regulation on data protection which it is proposed should replace the existing Data Protection Directive 95/46/EC</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th>EU</th>
<th>European Union</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSA</td>
<td>Financial Services Authority</td>
</tr>
<tr>
<td>Garante</td>
<td>Garante per la protezione dei dati personali, the Italian data protection regulator</td>
</tr>
<tr>
<td>GSMA</td>
<td>Global System for Mobile Communications Association</td>
</tr>
<tr>
<td>IAB</td>
<td>Internet Advertising Bureau</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office, the United Kingdom data protection regulator</td>
</tr>
<tr>
<td>Internet of Things</td>
<td>Where everyday objects are wirelessly connected to the internet through smart chips that can collect and share data without human interaction</td>
</tr>
<tr>
<td>MMA</td>
<td>Mobile Marketing Association</td>
</tr>
<tr>
<td>MMOGs</td>
<td>Multiplayer online games</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine-to-machine communications</td>
</tr>
<tr>
<td>OBA</td>
<td>Online behavioural advertising</td>
</tr>
<tr>
<td>OFT</td>
<td>Office of Fair Trading</td>
</tr>
</tbody>
</table>
## Glossary

<table>
<thead>
<tr>
<th><strong>Open data</strong></th>
<th>General information which can be freely used, re-used and redistributed by anyone, either free or at marginal cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal data</strong></td>
<td>Data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller</td>
</tr>
<tr>
<td><strong>Privacy by Design</strong></td>
<td>The practice of designing systems holding information to comply with privacy and data protection provisions</td>
</tr>
</tbody>
</table>
Authors

Judit Barnola
Senior Associate, OC Barcelona
Judit specialises in IT law and has been advising Spanish companies and multinationals in data protection laws and privacy for the last fifteen years.
E: judit.barnola@osborneclarke.com

Ulrich Bäumer
Partner, OC Cologne
Ulrich advises international clients on a wide range of IT transactions, and in particular outsourcing and technology driven M&A, as well as licensing and data protection issues.
E: ulrich.baeumer@osborneclarke.com

Ulrich Baumgartner
Partner, OC Munich
Ulrich specialises in data privacy law and has been advising companies and multinationals in European and German data privacy laws for over ten years.
E: ulrich.baumgartner@osborneclarke.com

Marialaura Boni
Senior Associate, OC Milan
Marialaura has specific expertise in the field of intellectual property and data protection as well as in-depth knowledge of the retail sector.
E: marialaura.boni@osborneclarke.com

Konstantin Ewald
Partner, OC Cologne
Konstantin specialises in e-commerce, entertainment, IT and data protection law and has over 10 years’ experience advising clients on complex transactions in this area.
E: konstantin.ewald@osborneclarke.com

Angus Finnegan
Partner, OC London
Angus specialises in technology, telecoms and outsourcing projects with over 18 years of experience of advising in this area.
E: angus.finneghan@osborneclarke.com
Authors and acknowledgements

Rafael Garcia del Poyo
Partner, OC Madrid
Rafael is a commercial lawyer specialising in Intellectual Property and Information Technologies’ Law. He advises clients in areas such as e-Business, telecoms, personal data protection, gaming, IT outsourcing, and cloud computing.
E: rafael.garciadelpoyo@osborneclarke.com

Paul Gardner
Partner, OC London
Paul specialises in commercial transactions and regulatory issues relating to the cross over of technology and entertainment. He has extensive experience of the contractual and copyright issues relating to content licensing and distribution.
E: paul.gardner@osborneclarke.com

Sue Gold
Partner, OC London
Sue has specialised in data protection law for over 15 years and prior to joining Osborne Clarke was EMEA Privacy Counsel at Walt Disney. She is highly experienced in reviewing complex technology transactions, developing strategies and procedures for European data protection compliance and has done leading work in the area of children’s privacy.
E: sue.gold@osborneclarke.com

Stephen Groom
Consultant, OC London
Stephen specialises in all aspects of advertising and marketing law and also advises on marketing-related data protection issues.
E: stephen.groom@osborneclarke.com

Nick Johnson
Partner, London
Nick is a leading marketing, advertising and media lawyer. He regularly advises on data privacy issues and also has specialist gambling law expertise.
E: nick.johnson@osborneclarke.com

Georg Meyer-Spasche
Partner, OC Cologne
Georg advises on regulatory and contractual aspects of new technology products and media convergence projects and is an expert for data protection solutions that work in practice.
E: georg.meyer-spasche@osborneclarke.com

James Mullock
Partner, OC Bristol
James leads our European Privacy and Information Law group. He specialises in technology and outsourcing transactions and handles global privacy issues for multinational organisations. James previously co-wrote “The Data Protection Act explained”.
E: james.mullock@osborneclarke.com
Authors and acknowledgements

Theo Savvides
Partner, OC London
Theo advises clients on the full range of intellectual property issues, with a particular focus on intellectual property disputes in the digital business sector.
E: theo.savvides@osborneclarke.com

Edoardo Tedeschi
Partner, OC Milan
Edoardo advises on corporate, corporate finance and commercial transactions with a particular specialism in IT and digital business.
E: edoardo.tedeschi@osborneclarke.com

Mark Webber
Partner, OC Reading
Mark specialises in transactions with a technology component and he focuses on innovative technology-led deals where IP, data or technology is being leveraged to add value to a business.
E: mark.webber@osborneclarke.com

Acknowledgements

David Tomley
Executive Editor

Sam Hunt
Commissioning Editor

Maryanne Beavers
Design

Sue Gold, James Mullock
Consultant Editors

Jill Parsons
Researcher

Qube Design Associates Ltd
Design Agency

Special thanks go to the following for sharing their thoughts and views
James Leaton-Gray, Public service broadcaster
Tobias Haar, General Counsel, Gameforge Germany
Ray Eitel-Porter, Executive Director, Opera Solutions
Maria Gomez del Pozuelo, CEO of Womenalia, Spain
Brad Bryant, EMEA Privacy Counsel, Aon
Luis Morcillo, Global corporate Counsel, Adconion Media Group
There is a deluge of datasets created by the digital world and it is getting easier and easier to store those datasets. Sometimes this storage is incidental, sometimes it is planned; frequently it is accidental.

Big data is the term used for datasets that are too large to be gathered, stored, managed and analysed by typical software tools. What is clear is that analysis of big data can create value.

Although the use of large data volumes for business is not new, data storage, processing power and cloud services continue to make large scale data analysis more and more accessible. As big data moves into the mainstream and utilises the cloud to extend its scope and potential, new technologies and the associated proliferation of data creates challenges for individual autonomy and effective data protection.

There is a lot of hype around big data. As with the cloud, rather than sell the potential to technology teams, the industry is selling the potential to the Board. There's quickly a fear that opportunity will be lost to the competition and a mandate for a big data analysis to extract the hidden value.

Key legal issues

1. Big data is not like other assets and there is little legal guidance.

Data is not quite like other assets. Data can be copied, transcribed, built upon, modified, added to, combined and reconstituted, all of which alter the original elements. Worse still, although many think of "my" data and fight negotiating contracts to "own" data, such concepts are more opaque that one first thinks:

• Where personal data is involved, EU data privacy laws effectively import ownership rights to the data subject. Meanwhile the business "owner" is more of a custodian and may not be entirely free to exploit data;

• The same data can be collected or used by more than one entity simultaneously. Each may go on to change the same original data

There is a blurring of legal rights and virtual assets. Big data has a disruptive effect and as with many disruptive technologies delivers potential uncertainty.

2. Ownership

With big data ‘just because you can do it doesn’t necessarily mean you should’ is a good guiding principle. There’s clearly no “big data law” and precious little guidance. It is important, therefore, to make a legal risk assessment working from first principles and ask questions about the contemplated solution in doing so. The intellectual property rights in big data (and databases comprising big data) may not be owned. Organisations need to consider what rights may be needed to exploit and mine the data, who bears legal responsibility for how data is handled, and how that risk is apportioned when a third party provider is appointed to assist with analysis.

Where a third party does assist with analysis, who owns the output needs to be addressed. Similarly, the ownership of any resulting new datasets and databases created in performing such analysis should be clarified.
3. Big data and personal data
Big data may contain personal data. While personal data may be “controlled”, this control does not necessarily give an absolute right of use as the relevant data subject will always have rights in respect of its use – such data is often provided or shared for a limited purpose. Creeping usage beyond an original legally justified purpose is one of the biggest regulatory risks. This can infect your data and diminish its value. Be clear what has been communicated previously about personal data use and be sure that any new processing is justified.

Analysing anonymous data avoids many regulatory issues and constraints. However, organisations must take care not to re-personalise the anonymous data. There is a real risk that anonymous data gets re-identified through either combining it with personal data or, less obviously, through too granular analysis.

With consumer and customer confidence dependent on an organisation adequately safeguarding personal data, the storage of large volumes of personal data in the cloud must be carefully evaluated. This is not least because on multi-tenant shared cloud platforms there is a possibility that another user on the same system may gain access inadvertently or deliberately to the personal data stored. Ensure your competitor cannot see your data because you happen to share a cloud. Also, think about how else it can be protected and kept secure (for example via the use of encryption, sharding or other distributed storage technologies).

4. Location, location, location
Where the data analysis is conducted may present issues. This is potentially problematic in the cloud where, in processing via a third party, there is an inherent level of risk as outsourced services bypass the physical, logical and personnel controls exerted by in-house programmes.

Data may be split and stored in multiple data centres all over the world, involving multiple entities and even multiple copies of data. Considering the risks posed by the location of data and various actors in these service relationships in the cloud is important. Additionally, organisations should look at the risks of any international transfers of personal data. For example, in its July 2012 Opinion on Cloud Computing, Working Party 29 makes the observation that it has serious concerns around the potential international transfers of data. It says: “Cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider’s network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data is located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.”

5. Be clear about who is liable for inaccurate data
Ensuring any data collected is accurate is of course an important part of extracting value. However, data collected will inevitably risk inaccuracies. Considering who is liable should original data be inaccurate or incomplete is important.

6. Avoid collecting data without any clear objectives
As with any other asset, organisations are often driven to collect as much of the asset as possible to ensure they retain competitive advantage or because there may be future value in it. Taking this approach with data, i.e. retaining and storing data without clear objectives, can have legal consequences with regulators or in relation to contractual promises made to other organisations.
Big Data and cloud computing
Mark Webber, Georg Meyer-Spasche and Ulrich Baumgartner

7. Data in the cloud
If your business relies on big data it is likely to rely on cloud. As well as security, thought needs to be given to service levels, as maintaining and accessing big data is not trivial. And remember that cloud service levels should not just deal with availability. The cloud is about redundancy, so availability should be a given in the first place. Latency could prove to be a bigger issue depending on the organisation’s solution. Consider what assurances should underpin your needs.

The legal issues surrounding the use of big data and cloud technologies need clarity to capture the full potential of big data. The law needs to strike a balance between protecting privacy as well as ensuring the security of personal data and allowing business to utilise the commercial value of data and the information it contains.

What the future holds
Leveraging big data already promises to give enormous power to businesses to work with large datasets without limits. Since the cost of experimentation is low in the cloud, businesses can experiment with big data analysis often and respond to complex business questions quickly.

Clarity from new legislation is unlikely and, if it does come, probably will not be quick and pragmatic enough to keep up with real life developments. Asking the right questions to understand the solution should help companies get ahead.

Today there is some assistance for the cloud industry in terms of the issues highlighted, and with the European Cloud Partnership currently deliberating we hope to see more guidance and assistance to promote cloud adoption while ensuring respect for the fundamental rights to privacy and data protection.

If you remember nothing else
• Make sure it’s clear who is liable if original data proves to be inaccurate.
• Tread carefully when storing data in the cloud and across multiple jurisdictions.
• Avoid personalising anonymous data through, for example, too granular analysis or appending with other data. This opens up a whole new set of compliance issues.
• Watch out for usage creep. Be clear what you are collecting the data for and how it will be used, and stick to it.
In an effort to make it easier for providers and users of cloud computing services to comply with German and European data protection laws, a working group of several German Data Protection Authorities (DPAs) has recently put together a paper providing some meaningful guidance. Experience shows that such guidance will form the basis for future enforcement actions.

As a starting point, the paper identifies the following major risks of cloud computing in the data privacy context:

- Limited control for the user over the data processing
- Limited transparency of data processing for the user
- Wide and fragmented distribution of the data
- Often limited separation of data of different users
- Eventually only limited availability of the data

In a second step, the paper makes it clear that it is the user of the cloud services who is and will remain responsible for the processing of personal data vis-à-vis the data subjects. As the “controller” of the data, the user has to ensure the legality of the data processing in its entirety, including the rights of the data subjects. The cloud provider, in turn, acts as a “data processor” only.

In this context, the paper acknowledges a certain “dilemma”, as the cloud user remains responsible for the data processing, while in practice he will only have very limited control. Against this background, the German DPAs require as a minimum:

- Careful selection of the cloud provider by the user;
- Transparent and clear contracts (so-called “commissioned data processing agreements”) between the provider and the user in accordance with the specific provisions regarding processor agreements under the German Data Protection Act (detailing inter alia the location of the data processing, involvement of sub-contractors, control rights of the user, right to give instructions to the cloud service provider that guarantee the rights of data subjects, etc.);
- Transparent and detailed information by cloud service providers regarding the technical and organisational measures implemented to ensure data security; and
- Up-to-date and meaningful evidence for the implementation of such measures, e.g. certificates of recognised and independent auditors, rendering on-site checks of the users dispensable.

Finally, as regards cross-border data transfers, the DPAs take the view that the use of cloud computing services outside the (EEA) is not permissible under German data protection law as far as certain “sensitive” data is concerned.
For some time there has been growing concern from consumers and regulators that privacy policies have become too complex and no one is reading them. Attempts to promote Layered Privacy Policies have had limited uptake so it is clear that something needs to be done to get the message across to customers about what is happening to their data.

Recent research from a UK consumer organisation shows that 80% of people are fairly or extremely concerned about their online privacy. Supporting research by the Information Commissioner’s Office (ICO) shows that 94% of consumers rate protecting personal information online as their joint top concern along with cybercrime, with a significant majority feeling that more should be done to protect their personal information.

In July 2012, Twitter launched its first ‘transparency report’, inspired by Google’s efforts and a bid to improve the way Twitter communicates with its customers about the flow of information it holds.

Although the spotlight for both Google and Twitter’s transparency reports has shone primarily on the type and level of user data requests from governments, they are examples of two leading digital businesses trying to build trust through greater levels of transparency.

As data volumes increase, managing how data is collected, stored and retained in a growing ecosystem gets challenging. Add to the mix an increasing pressure for transparency about data use, from regulators and consumers, and you have some significant issues for business collecting, storing, sharing and analysing data.

Key issues

An organisation that wants to be transparent with its customers and meet regulatory demands about data use must have a firm hand on why it collects certain data and how that data is used.

1. How to be transparent – managing a moving feast.

Consumers should be aware of what is happening with their data, how it will be used and where it will go. Even if the man in the street appears to be laissez–faire about how their data is used, that doesn’t mean free rein for the organisation.

Keep in mind that any lack of transparency could mean falling foul of certain privacy regulations. It also risks consumers turning against a particular brand or product. Consumer expectations around levels of transparency are likely to be a moving feast.

Spain, for example, advocates keeping customers informed at all times about when personal data is collected. As more data is shared through smart phones and tablets, collected and used in less obvious ways and shared across numerous parties from app designers to mobile network operators, this level of transparency is increasingly difficult to fulfil.
Evolutionary challenges

Indeed the logistics of communicating disclaimers and lengthy privacy policies via mobile is itself a barrier to keeping customers informed and engaged with how their data is used. According to Carnegie Mellon research, reading all of the privacy policies an average internet user encounters in a year would take 76 working days.

Organisations must be innovative in the way they communicate their data policies. One example is Channel Four’s use of the British comedian Alan Carr to communicate with its audience about how it uses their data if they sign up for the 4OD service or its other digital products and services. This is a great way to engage and be transparent with their audience and get a clear message across.

2. Can one size fit all?

Multinational companies are increasingly looking to have one global policy to cover all locations around the world and all forms of media including apps and mobiles. This can be difficult and may reduce transparency if a consumer has to wade through a long policy to find the relevant section for a specific activity. In addition, there are specific requirements in different locations on the type of information or level of detail to be included.

3. Don’t just collect data at will - have a clear objective

Organisations put themselves at risk if they collect and store information with no clear retention policy and retain data indefinitely in the belief that one day it may have a use. There are two strong reasons to avoid this approach:

• To have commercial value, data needs to be accurate. Collecting data with no clear objective on how it will be used, stored or maintained is no recipe for success.

• Regulators in Europe are keen that organisations have a clear reason for collecting data and only collect the data that they really need (data minimisation).

Make sure you have a clear objective for any data before you collect and store it.

4. Think about how long you’re going to keep data

Technological advances and, in particular, the emergence of the cloud means we can now store vast amounts of data for significant periods of time at little cost. However, keeping data for longer than necessary is at odds with the regulatory principles in Europe and should be avoided. In the UK there is no definition of what is "necessary", although clearly if there is a legal requirement (e.g. tax) to retain specific categories of data this would be sufficient.

In Italy the Garante (the Data Protection regulator) has specified some retention periods e.g. CCTV images should normally only be retained for 24 hours but can be retained for up to a maximum of one week if limited exceptions apply. Specific rules also apply for loyalty card data where anonymised purchasing data can be retained for 12 months for profiling and for 24 months for marketing. Retention periods are also specified for credit information depending on the nature of the information provided with periods ranging from two months up to 180 days.

In Spain there are clear regulations applying to the retention of data. Personal data should be erased when it is no longer necessary or relevant to the purpose for which it was initially collected. Data may be kept for a longer duration provided the data subject consents. Similarly, in Germany data can only be stored for the defined purposes for which the data was collected and must then be deleted.
Although the lack of specific guidance might on first view seem frustrating, it is designed to allow local and commercial flexibility. This means any business retaining data needs to have a clear case to justify how long it plans to keep personal data.

Considering how long to retain data also has commercial implications. Data accuracy will degenerate over time. So, although cheap storage in the cloud might lead some organisations to be less vigorous about how long they keep data, the process and work needed to maintain data is significant and critical to its value. Build into the business case for collecting data, the process for retaining or maintaining that data.

5. Look back as well as forward

The ability to look back at historical data so as to build, for example, a picture of a particular customer’s browsing habits can be useful. However, organisations need to take care that data they already have stored comes with the right consents for any new use. When the data was collected did the privacy notifications provided cover the anticipated use? If not, additional consent may be required.

6. Take care with data you receive or buy from another organisation

Be as careful with the data you receive or buy from other organisations as you are with the data you collect yourself. It is your responsibility to do the due diligence to verify that the person who originally collected the data has the right consents. If there is a contractual relationship between you and the person from whom you are buying the data, make sure you have the right warranties in place in your contracts. In Germany, for example, it is usual to include broad warranties that the seller guarantees collection and storage is in compliance with local law.
What the future holds

The requirements with respect to transparent data collection, storage and retention will only increase in the years to come. Because of big data and cloud computing, data subjects and regulators will demand greater transparency. The requirements for privacy by design, as outlined in the new draft EU data protection Regulation, will also increase the demand for more transparency.

In addition, the following developments are envisaged:

- Advent of Privacy Seals in Europe to denote good privacy practices/policies.
- Development of standard wording for Privacy Policies and Regulatory specifications on the information to be provided.
- Development of more innovative ways to provide transparency on data use, moving away from the standard wording in privacy policies e.g. videos.
- Development of further self-regulatory codes of practice.
- Increased interest from regulators on retention policies with the rising focus on accountability.
In Germany, consumers are extremely wary about data protection and data security and so there should be no surprise that the issue of transparent data collection, storage and retention is fully regulated. As a general principle all data handling and its purposes must be fully transparent.

For example, Germany incorporated certain information rights of all data subjects in the local data protection act. Each data subject in Germany has a right to ask any third party who seems to have data about the data subject (i) which data this third party is holding about the data subject and where the third party received such data from, (ii) to whom the third party has transferred such data and (iii) the purpose of the data storage. The courts in Germany have repeatedly held that the third party has to render such information to the data subject within two weeks of a request. Only third parties who follow transparent data collection, storage and retention process can fulfil this strict legal requirement.

Furthermore, German data protection law stipulates that data should not be retained for longer than necessary. Section 14 of the German data protection act stipulates that data can only be stored for the defined purposes and that the storage is no longer allowed once the defined purpose has been fulfilled.

In Germany it is also customary to ask for broad warranties from a seller of data. The seller should guarantee that the data is collected, stored and transferred in line with all applicable laws, especially in line with local data protection laws and principles, and that the seller will indemnify and hold harmless the buyer in case any third party or data subject makes any claim against the buyer arising from alleged breaches. Other warranties that the buyer demands from the seller of data could be with respect to validly obtained consents from data subjects, on data portability, etc.

On the issue of dynamic IP addresses and personal data, the German position is not yet clear. On the one hand we have local German data protection agencies (e.g. in Lower-Saxony) which hold that dynamic IP addresses must be qualified as personal data in the sense of Section 3 of the German data protection act. On the other hand we have courts (like the Court of Appeal in Hamburg) which clearly hold that a dynamic IP address is not personal data because only the access provider (and no one else) can make a connection between the dynamic IP address and the data subject.
In Italy the general rule in matters of data retention is that the relationship between the period for which data is retained and the reasons for its collection must be proportional. In addition, the data owner must not retain data for excessively long periods.

However, there may be specific cases where the law allows for longer retention times such as, for example, where accounting and tax rules require certain information to be held for at least five years. In addition the Italian Data Protection Authority (DPA) provides specific rules in some cases regarding certain types of data and acceptable retention periods.

Some examples:
- **Telecommunications.** Telecommunications data cannot be stored for longer than six months for billing and payments purposes, 24 months where it relates to detailed telephone traffic or 12 months for detailed broadband usage data used in criminal investigations.
- **Video surveillance.** The general retention policy is 24 hours, but in some cases a longer retention period may be allowed because of specific security needs or high-risk activities performed by the data controller (e.g. in the case of banks). However, the period in question should never be longer than one week.
- **Consumer profiling / loyalty cards.** The data regarding items purchased by identifiable customers may be retained for no longer than 12 months (if used only for profiling) or 24 months (if used for marketing), subject to their being rendered anonymous.

If data is stored contrary to the above rules, or if the duration is considered excessive, the DPA could view the processing as unlawful or unfair - depending on the specific circumstances. The consequences can be:
- The personal data may no longer be used;
- The DPA may order the processing to be blocked or ban the processing;
- Administrative fines and criminal sanctions may be imposed depending on the seriousness of the case.
A Google search on ‘Sony data breach’ brings in over a million hits. This data breach, which hit the headlines around the world in 2011, was one of the biggest to date, with millions of customers’ details hacked.

There was an immediate reputational loss for Sony, with their ability to keep and attract customers potentially damaged. There was also a financial loss, with the clean-up costs reported to be well over $150 million, along with board resignations, share price damage and a real class action risk, not to mention the prospect of regulator fines.

Against this backdrop, the regulators are getting tougher. In the last year, the UK’s Information Commissioner’s Office increased fines for data breaches from £430,000 to £1.8 million, with warning notices issued increasing from 46 to 68.

The lesson: data is a valuable new asset for many businesses. However, it is also increasingly regulated and of public interest. Therefore, controlling that asset and how it is used and secured is critical to maintaining its position as an asset rather than a cost. This means adopting the right technical and organisational security measures and data compliance processes when collecting, storing or processing data.

Key legal issues

1. Outsourcing doesn’t mean outsourcing responsibility.

Many organisations outsource elements of their data collection and/or management to third parties, but that does not absolve them of responsibility.

In recent years, a number of companies have been fined and required by regulators to quickly roll out expensive data security technologies and procedures as a result of the mistakes made by providers they have hired or partners they have contracted with.

Essentially, if you’re the person who controls how data is used you are responsible for it wherever it goes in the data ecosystem. If a partner or supplier (or, for that matter, their sub-contractor) mismanages your data, then you are responsible.

As the data ecosystem continues to expand and specialise, this becomes increasingly important. Take the numerous players involved in delivering and operating a mobile app as an example of multi-player involvement. Delivering a mobile app involves numerous parties from the app designer and app store owner to the mobile operator and/or partners responsible for introducing a consumer to the app. This opens up plenty of opportunities to lose control if data control and security measures are not built in from the outset for all involved.

As a general rule in Europe, written contracts must be made with any suppliers or agents responsible for processing personal data on an organisation’s behalf and must include appropriate security and other data protection safeguards. These might include security and disaster recovery service levels, the company’s right to verify the application of the security measures, and indemnity protections.
Security & control
James Mullock, Sue Gold, Judit Barnola, Edoardo Tedeschi, Georg Meyer-Spasche and Rafael Garcia del Poyo

There are also a number of local laws across the EU to be aware of and which build upon this premise. For example, tough Spanish rules stipulate that security measures need to be reviewed on a regular basis to ensure that they are up-to-date and effective, particularly with reference to technological developments. These have to be properly reflected in a “Security Document” available for Spanish Data Protection Agency inspectors.

In Germany, data processing agreements that provide for auditable technical and organisational control have to be entered into. While in Italy, specific mandatory minimum security measures provided in the Data Protection Code must be adopted. More restrictive and additional security measures are specifically provided in case of sensitive data processing.

2. Unlucky or an accident waiting to happen?
As with many areas of legislation where the rules aren’t prescriptive, part of an organisation’s defence if something goes wrong is being able to show steps taken to mitigate any risk. The majority of data protection laws across Europe are heading this way. There is no clear message from lawmakers as to what constitutes “good security”—simply guidance over the need to take “appropriate measures”. The one clear message is that the more valuable and sensitive the data, the more important it is to use encryption technologies to protect it.

The UK regulator, amongst others, has clearly signalled that organisations that encrypt data are taking a clear step towards meeting their data protection security obligations and will not be harshly treated in the instance of a security breach. Regulators will look at what an organisation has done to maintain control and security of its data and mitigate risk. Organisations therefore need to decide what data governance measures are appropriate for their market and remember that these will need to be dynamic and change over time.

3. Data breach notification
In the UK, data breach notification obligations vary dependent upon the sector in which the affected business is operating. For example, financial services and telecoms providers must meet mandatory reporting requirements. For others, the requirement to proactively notify a regulator that a data breach has occurred only arises in certain circumstances, including:

- Scenarios of harm to individuals;
- When the breach impacts a large number of individuals; and,
- Where sensitive information is involved, such as health data.

In Spain, the obligation for companies to notify personal data breaches to authorities as well as to the individuals concerned was due to be implemented in May 2011 but has been delayed by fundamental inconsistencies with the Spanish Constitution’s prohibition of self-incrimination.

In Italy, the obligation to notify data breaches to the Italian regulator and/or affected individuals is a relatively new one (May 2012) and only applies to providers of publicly-available communications services.
A range of different breach notification obligations currently apply in other European countries. For instance, Austria was an early adopter of the approach taken by many US states of requiring full notification to affected individuals upon a data breach being discovered.

The position across the EU will be unified and clarified by the EC’s new data protection regulation, which proposes tough requirements for organisations to notify regulators within 24 hours of any data breach.

4. On the move

The very nature of data as an asset means it can move freely across borders, both within companies and across supplier and partner relationships. This is accentuated further as data storage increasingly moves into the cloud.

Creating numerous commercial and cost-saving opportunities for organisations, this brings added legal compliance challenges for data owners. After all, EU data laws contain specific provisions that regulate the transfer of personally-identifiable information from Europe. To avoid legal pitfalls negating these opportunities requires taking control of the data supply chain and building security into its design.

5. Do the pre-nup with partners like you would a supplier

Partnership agreements between organisations are often less rigorously documented than traditional supplier/contractor relationships. However, where sharing data is part of that partnership, the same rigour needs to be applied, with good governance and procedures built in to control and ensure the security of that data is maintained.

Governance should include considering what compliance obligations should apply to data at the end of a commercial relationship. If there is no agreement in place, problems can arise around, for example, who owns the data; who has the right to use it and when; the extent to which data can be shared; data retention, and data security obligations.

6. More than an IT problem

A large percentage of data breaches are the result of human error rather than equipment fault or hacking: the laptop left in the back of a taxi scenario. However, most organisations continue to see data security and control as an IT rather than HR or business-process issue. In fact, training key people in the business in data control and security is a sensible approach to help minimise risk.

Similarly, to ensure any data issues are managed effectively, organisations should consider what other departments might need to be involved, from a crisis management point of view, in disaster planning for a data breach. As a minimum, the PR and HR departments should always be included.
Evolutionary challenges

Big data and cloud computing
Transparent data collection and retention
Security & control
Ownership – Rights in data
Behavioural advertising
Data-driven pricing
Mobile apps
Data and games
Machine-to-machine data collection
Data and children

7. Watch out for regulator double jeopardy

In the UK, the Information Commissioner’s Office (ICO) is currently the regulator with the widest sectional remit when it comes to imposing fines for data security failures. However, there is potential for ‘double jeopardy’, depending on which sector you operate in and the powers afforded to other relevant regulators.

In the UK, the Financial Services Authority is also empowered to fine businesses in the financial services sector for data security breaches, for example. Historically the FSA’s fines have been much bigger than ICO’s, with HSBC fined £3 million and Nationwide £2.27 million, for example. And organisations should also remember that individuals can potentially sue in their own right for data security breaches.

Italian Data Protection Law imposes personal liability on those who fail to adopt certain minimum measures, with a maximum punishment of up to two years’ detention.

What the future holds

There are some important legal changes on the horizon. First are the new data governance rules due to come into play in two to four years’ time via the new EC Data Protection Regulation. That might sound some way off, but the implementation of the policies and procedures required to meet the new standards will take many organisations a long time.

We are also likely to see new laws enabling people to bring class actions following data compliance failures, raising the temperature on any likely legal action around data security breaches in the future.

If you remember nothing else

• Hard-wire data security compliance into the procurement / contractual process for both traditional supplier relationships and, importantly, more informal partnership agreements.
• Remember to look back as well as forward, consider auditing your most important existing partnership and supplier arrangements as well as new ones.
• Prepare now for the new rule changes, including data governance provisions, 24-hour notification and class actions again likely to be introduced via the EC’s Regulation.
• Training, training, training – remember data control and security is not just an IT issue. Make sure everyone who handles data is trained in the security and control of that data.
• If you are collecting and storing sensitive or valuable data, use encryption technologies to protect it.

Finally, the need to give 24 hours’ notice of any data security breach will be hard-wired into all EU Member States’ laws going forward. Compliance with this timescale might seem relatively straightforward, but it will require slick processes to identify a breach, work out what has happened and decide whether regulators should be notified within 24 hours.
Spain has some particularly rigorous rules in relation to data security. Personal data is a specialised form of data with specific rules to protect the integrity and security of the data and the privacy of the individual.

Specific legal requirements in Spain include:

- Organisations collecting and processing data in Spain must ensure that they and their processors implement technical security.
- Contracts with any suppliers or agents responsible for processing personal data on an organisation’s behalf must include appropriate security and other data protection safeguards.
- Security measures need to be reviewed on a regular basis to ensure that they are up-to-date and effective, particularly in relation to technological developments. These security measures should be properly reflected in a Security Document available for inspection by the Data Protection Agency.
- Depending on the type of data, there are three different levels of security measures in Spain: basic, medium and high. In deciding what level of security is appropriate, organisations must understand the nature of the personal data in question based on set criteria outlined in the regulations. Those dealing with personal data of a sensitive nature logically need to implement very robust security standards and undergo biennial audits on the security measures in place.
- Failure to maintain files, premises, software programmes or hardware containing personal data within the regulations’ security standards is considered a serious infringement with fines ranging from €40,000 to €300,000. The AEPD (Spanish DPA) is the administrative body in charge of imposing these penalties.
This quote from recital 10 to the EU’s Database Directive shows that as far back as the mid-90s, when Europe first formulated an intellectual property right to protect investment in databases and the data they contain, there was a recognition of how important it would be to invest in the right systems to exploit the anticipated data gold rush.

The Database Directive continues to provide that protective framework in Europe today.

**Key legal issues**

1. **What intellectual property rights are there in Europe to protect data?**

Exploiting data in today’s digital world involves collecting data and then designing databases or systems to store, analyse and exploit that data.

The Database Directive provides two regimes for protecting databases and their contents:

- **Database rights** – database rights protect the contents of a database (in other words the data), but only where there has been a substantial investment in either obtaining, verifying or presenting the data.

- **Copyright** – copyright protects the structure of the database (not the contents or data itself), where there has been intellectual creation in the selection and arrangement of the data in the database.

2. **What data is protected by database rights?**

The answer to this is, not as much as many database owners hope. The investment required in obtaining, verifying or presenting the data must be substantial when calculated by reference to the resources used to seek out existing independent materials and collect them in a database. Resources used in the creation of data do not contribute to the assessment.

The best way to illustrate this difference is to look at the typical process used by price comparison websites to obtain data. Take, for example, a price comparison site for financial products. These sites operate by either:

- employing people to research prices and factors that affect prices;
- using computer software to scrape price and related data from websites; or
- a combination of both.

In each case, there is likely to be a substantial investment in obtaining the data, verifying the accuracy of the data and presenting the database on the website – both in employment costs and IT costs. Therefore, database rights are likely to subsist in the data contained in a price comparison website's database.
On the other hand, any bank will have a portfolio of financial products like bank account, mortgage, credit card and insurance products. The details of these products are themselves likely to be arranged in databases. However, database rights may not subsist in this data, because the interest rates, fees, costs and other conditions attached are all data that they have created. Therefore, in most of these cases, there is not likely to be any investment in obtaining, verifying or presenting the data on their financial products as “independent materials”.

3. Limited international protection

Database rights can be used to prevent the unauthorised “extraction” or “reutilisation” of a substantial part of the contents of a database. Extraction is defined as the transfer of the data from one medium to another. This is not restricted to extraction directly from the protected database, but also includes onward transfer of data that was originally extracted from the protected database. In other words, database rights protect data no matter how many hands it passes through as long as it was originally extracted from the owner’s database. Reutilisation is defined as making the data available to the public.

The assessment of what amounts to a substantial part of the database can be made with reference both to the quantity of data relative to the overall database, and also the quality of the data. In terms of quality of data, this will be assessed by reference to the amount of investment that may have gone into obtaining, verifying or presenting what may be a relatively small amount of data.

The assessment does not cover the amount of data involved in a single act of extraction or reutilization, but can cover the extraction or reutilisation of small amounts of data taken regularly over time so as to amount to a substantial part.

To monitor infringement of database rights, consideration is given to “seeding” data. Seeding involves the inclusion of artificial data in the database, namely data that has been made up rather than derived from real sources.

To preserve the commercial value of the database it is important that the database is seeded in a neutral way that will not undermine its integrity. Seeding makes it much easier to find out whether a third party is using data derived from your database as opposed to independently obtaining the data themselves.

4. Limited protection for non-European businesses

Unlike copyright, international conventions are not in place to provide for reciprocal protection of rights in data around the world. To qualify for EU database rights protection, a company must be formed in accordance with the law of an EU member state and be economically linked on an ongoing basis with a member state. This could be, for example, by having its central administration or principal place of business in the EU.

Companies headquartered outside the EU that want to exploit data in the EU need to consider whether they qualify for database rights protection, and if not, consider how best to protect their data. This could be by the alternative means identified below, or by setting up a corporate structure that provides for investment being made by a company that is trading in the EU.
5. What other ways are there to protect data outside of the EU’s database rights regime?

If database rights cannot be relied on to protect data, there may be alternatives.

If the data is not in the public domain, for example, it may be possible to protect it by relying on rights in confidential information. This will only work if the data is not freely available on a website but is instead licensed on a limited basis. In these cases, a clearly defined contract detailing how the data can be used is necessary, particularly limiting the dissemination of that data.

If confidentiality is not an option, then the last route may be to use contractual terms and conditions to limit use.

Where data is available on a website it may be possible to use the terms of use of the website to impose contractual terms over how much data may be downloaded by any user and how it may be used. The enforceability of these terms depends on how well the terms have been drawn to the user’s attention and therefore incorporated into the contractual relationship with the user.

Thought should also be given to technical measures that can limit the usage of data by any one user. For example, technical measures for preventing web-crawlers from scraping your site, as well as measures for monitoring usage, such as user accounts, may be relevant.

If you remember nothing else:

- Your data may be protected by the EU’s database rights regime but only where there has been a substantial investment in obtaining, verifying or presenting independent data.

- The EU’s database rights regime will only protect your data if your company was formed under the laws of an EU state and is economically linked with an EU member state on an ongoing basis.

- You should consider ‘seeding’ or using artificial data in a database to help monitor any infringement of database rights.

- If your data is not protected by the EU’s database rights regime, consider using confidentiality, contractual terms and technical measures to protect your data.
Ownership – Rights in data
Theo Savvides

What the future holds

There have been a number of judgments from the European Court clarifying various elements relating to database rights protection that were not clear when the rules were first introduced.

However, the question of jurisdiction remains unclear. Given the digital environment in which most businesses now operate and the possibility that a third party can extract data through the operation of servers located in a different country, the question of which country’s laws apply in the instance of international database right infringement remains a critical one. The position gets worse if the third party then makes the data available to the public in its country of origin and in competition with the original database owner from a server in a different country.

The question is, in which country is the extraction and reutilisation of the data taking place? If the servers are located outside the EU this could present particular problems because of the lack of reciprocal protection.

The ongoing Football Dataco v Sportradar case highlights this issue. Football Dataco is the licensing company for data from the football leagues of England and Scotland. Sportsradar is a German-based provider of competing football data, some of which has been extracted from the Football Dataco database.

Football Dataco alleged database right infringement in England but Sportradar claimed the German Courts should have jurisdiction. The English Court accepted jurisdiction initially but ultimately referred the issue to the European Court. The key question is: If a company uploads data from another company’s ‘protected’ database and then responds to a request from a user in another country to send that data to their computer where it can be stored in the computer’s memory and displayed on its screen, is the sending of that data an act of ‘extraction’ or ‘re-utilisation’, and if so, in which country does that extraction or re-utilisation occur?

The European Court’s finding both in this case and others like it will be closely watched.

Contact details

Theo Savvides
Partner
E: theo.savvides@osborneclarke.com

© Osborne Clarke 2012
Terms and conditions | osborneclarke.com
**Evolutionary challenges**

Big data and cloud computing
Transparent data collection and retention
Security & control
Ownership – Rights in data
Behavioural advertising
Data-driven pricing
Mobile apps
Data and games
Machine-to-machine data collection
Data and children

---

**“Behavioural advertising” or “behavioural targeting” has for a long time been marketing’s holy grail. If you can develop a comprehensive profile of each consumer based on their product preferences, shown by their purchasing or browsing history, it is a win-win scenario.**

Behavioural targeting allows marketers to better concentrate their resources where they matter and avoid consumers being assailed by irrelevant marketing messages. John Wanamaker’s famous words “Half of the money I spend on advertising is wasted, the trouble is I don’t know which half” can effectively be condemned to the dustbin.

However, with the advent of Big Data and the ability to collect, store and analyse data on an unprecedented scale, real privacy concerns have surfaced. These concerns are amplified by the type of personal data capture that smart phone, mobile apps and tablets can facilitate. Europe's privacy laws have attempted to keep pace.

**Key legal issues**

Europe's privacy laws pose a number of challenges for behavioural advertisers. Here are just three:

1. **“Appending” pushes the behavioural envelope**

“Appending” is the well-established practice of combining personal data held about a customer or prospect, with data about that same person available from third-party sources. The abundance of behavioural and attitudinal data available online and in particular on social media platforms has the potential to take the practice to a completely new level. For instance it could be invaluable for an online retailer to discover from a customer’s Facebook page that they particularly like a product line they have not previously bought from that retailer. Or a customer’s email address may be found when previously only their postal address was held.

However, there are potential privacy law hurdles with appending. For example, there are detailed requirements imposed on data controllers where personal data has not been obtained from the data subject. Unless it involves “disproportionate effort”, which in most cases is impossible to show in the digital world, the data subject must be told about this within a reasonable period; an unattractive step for some marketers.
Evolutionary challenges

2. Email marketing and the use of tracking technology

Email marketing combined with tracking technology gives advertisers exciting possibilities. Busy IT animals called “gifs” allow marketers insights into whether emails they send are opened and when. But does this technology give rise to privacy concerns? With the arrival of the Privacy and Electronic Communications Directive (“PECD”), and its provisions dealing with the “Confidentiality of communications”, the answer is yes.

These rules required that web users received clear and comprehensive information about how information was stored or gathered from a user’s PC or laptop. An opportunity to refuse this access or storage also had to be given. In the UK, the first versions of guidance issued by the Information Commissioner’s Office (ICO) clearly indicated that the use of gifs and similar technology in the context of email marketing would be caught by these provisions. This arguably remains the position today with gifs and certainly with more sophisticated tracking technology used by some promotional emails. And with the law now requiring consent for this (see below), email marketers should take heed and look for instance at obtaining “cookie consent” by way of the disclosures given when individuals sign up to receive marketing emails.

3. “Cookie consent” law

When the behavioural tracking capabilities of what were known as “cookies” dawned on European MPs, it was late 2009 and they were in the final throes of pushing through changes to the PECD. Largely under the radar of Europe’s marketing industry, the provisions dealing with accessing and storing information on web users’ laptops, mobiles and tablets were changed. Out went the obligation to allow users a way of stopping cookies, gifs etc and in came language that in most cases only allowed their use if the subscriber or user had given consent.

Debate has swirled around Europe about how compliance might be achieved without killing European e-commerce. All this time, the global behavioural targeting ecosystem continued to grow and diversity in leaps and bounds, with third-party cookie-based ad networks chiefly instrumental in driving the Big Data era.

Industry stakeholders and bodies such as the Internet Advertising Bureau struggled to get traction for the US-originated “Self-regulatory Programme for Online Behavioural Advertising”. At its core was a set of “Good Practice Principles for Online Behavioural Advertising” and an “advertising option icon”. This was to appear whenever ads appeared on screen as a result of the use of tracking cookies. The icon provided information about the ad’s source and an opt-out opportunity. The scheme has so far largely failed to take off in Europe, however, in no small part due to its failure to deliver the “consent” envisaged by the amended Directive. Having said this, websites and marketers benefiting from third party tracking cookies
Evolutionary challenges

but looking to be transparent with their users and customers could do worse than investigate participation in the scheme. In conjunction with suitable steps to ensure compliance with the “cookie consent” rule, it could serve to demonstrate a responsible attitude to users and monitoring or investigating regulators.

Turning back to the law, the majority of EU member states have now bitten the bullet and implemented the cookie consent rule. Approaches have varied, with states such as Germany taking no steps because they felt their existing laws sufficed.

In the UK, “implied consent” has been officially sanctioned by the ICO for many cookie-use scenarios and websites have grabbed with both hands the opportunity offered by this and ICO’s indication that it may be permissible for consent to be obtained after cookies are set, provided this happens quickly.

Spanish rules do not require “opt-in” or express consent. However, they also do not give a clear route to getting the necessary consent. The Spanish Data Protection Authority is currently working to clarify this issue. These guidelines, when they emerge, should provide answers as to the type of user consent needed and the categories of cookies likely to be affected. However, it is expected that, given Spain’s vigorous approach to data protection, the guidelines may eventually require service providers to obtain “opt-in” and express consent in order to install not all but certain categories of cookies on users’ devices.

If you remember nothing else

• Take care when ‘appending’ one set of personal data to another.
• Many marketing emails drop tracking devices on the recipient’s terminal. If they do, the EU “cookie consent” rule must be observed.
• EU cookie laws are now largely in force across Europe. Although the UK has apparently sanctioned “implied consent”, some countries are going down the “express consent” route, so tread carefully.
• Websites and marketers using tracking cookies should investigate participation in the IAB’s “Self-regulatory Programme for Online Behavioural Advertising”. Though not a solution to the consent conundrum, this could help demonstrate a responsible attitude to regulators.

What the future holds

Seemingly limitless behavioural advertising opportunities are offered by social media.

Quintillions of bytes about users’ product and brand preferences, lifestyles and “likes” are generated every day on Facebook, Twitter, Pinterest and other social media platforms. But the elephant in the room is how this can be accomplished whilst still complying with the fundamentals of EU data protection and electronic communications legislation.
Evolutionary challenges

And of course this is not just a challenge for the Facebook or Twitters of this world. The data is also on display to brand owners and marketing agencies, but they must take care before looking to harness the data riches apparently offered on a plate.

Collection of non-personally identifiable behavioural information for research purposes may circumvent the Data Protection Directive rules. However, the harvesting of behavioural data relating to identifiable individuals in order to append this to other data already held about them must come with a loud privacy health warning. A careful analysis of all relevant circumstances and legal principles is essential, including the terms and conditions governing use of the platform by both the consumer and the data gatherer. It should also include whether the appending of any such information to data already held about that individual would constitute illegal processing of that data.

And then there is engagement with consumers within social media. If a potential brand ambassador is found, or a consumer who is criticising your brand, it is tempting to make contact. But care is needed as the platform’s use terms or electronic communications laws may for example be breached.

And finally, aside from any legal risk, there is one other, potentially far more damaging, exposure which could be faced by those contemplating tapping into social media’s behavioural goldmine. This is its power to irrevocably damage even the strongest of brands with one Tweet or post, something that might just be triggered by one false promotional move using behavioural data.
Browse travel site Orbitz with a Mac, and you’ll see a different – and more expensive – set of offers than those displayed to Windows users, according to reports in June 2012.

Given that Apple owners are statistically more inclined to buy top-end goods and services, the business logic of this differential treatment is hard to dispute.

In fact, Orbitz doesn’t offer different prices to different user groups – it just steers them towards the inventory they’re more likely to want. But with increasingly rich customer data becoming available, we are moving towards a world where offers and pricing could be varied based on data-driven segmentation.

Key legal issues

Many businesses – and particularly those operating online – now have access to large volumes of data on customers’ location, age, gender, credit history, browsing patterns and multiple other factors. This unlocks the possibility of tailoring deals and pricing based on an individual’s profile, and that profile’s correlation with qualities such as long-term loyalty or price insensitivity.

1. Discrimination law

European law (the Services Directive) prohibits retailers from discriminating against consumers (including in their pricing) based on nationality or place of residence, unless this can be directly justified by objective criteria. In the UK, the Equality Act additionally bars discriminatory pricing based on particular protected characteristics: disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation and (from 1 October 2012) age. Similar restrictions apply in other European countries, for example under German anti-discrimination law.

Businesses that enjoy a dominant market position also need to worry about challenges under competition law, because price differentiation could amount to an abuse of their dominance.

2. Data protection

Some personal data will generally need to be processed in the context of allocating the user into a pricing or offer category. Depending on the disclosures given to data subjects, and any consents obtained from them, processing of their data for this purpose could be argued to be in breach of European data protection law.

In the UK, the OFT has set out its stall and appears to see this as a significant and very live risk – see sections 8.10-8.15 of their May 2010 report on online targeting of advertising and prices.
3. Consumer protection law

Differential pricing activity could be vulnerable to challenge under consumer protection laws, if consumers are not adequately informed of the existence and basis of segmentation activity. Again, the UK's OFT has publicly warned that it sees lack of transparency in this area as potentially actionable as a misleading omission. While that is arguably stretching the limits of UK consumer protection law, much may turn on the kind of data and behaviours being used as the basis for segmentation.

If you remember nothing else

Businesses looking to tailor their offerings based on customer profiling should tread carefully:

- Delivering a different user experience and showcasing different inventory is one thing, but charging a different price for the same product is another, and will be much more risky.
- Segmenting offers based on age is already problematic in Germany and will get more problematic in the UK from October 2012.
- If you can navigate the risks under discrimination law and the EU Services Directive, transparency and disclosure to customers will be key in ensuring compliance with data privacy and consumer protection laws.
- Leaving aside legal and regulatory concerns, do not underestimate the resourcefulness of the internet community. If there's a way to spoof your profiling system, someone somewhere will work it out and spread the good news.

What the future holds

Media interest in this area has been relatively muted to date, but there are some big stories here waiting to happen. Differential pricing takes all the social mobility and two-tier internet concerns raised in the net neutrality debate and ups the ante with a good dash of “Big Brother” data exploitation narrative, and the potential for outrage over racial, sexual and other forms of discrimination. Proceed with caution.
Mobile apps run on some of the most advanced devices and smartphones available and connect users to the online digital environment. As with anything that interacts with the digital world, mobile apps come with their own privacy challenges, not least because of the sophisticated digital fingerprint an app can assemble.

Mobile apps represent a sea change in the type and level of data available and the potential value in that data. The way we use our mobile devices and apps is largely user-generated and reveals significantly more about our preferences, location and behaviours than is available from other devices.

In 2012 Viviane Reding, the Vice President of the European Commission, observed to the UK’s Channel 4 News: "They are spotting you, they are following you, they are getting information about your friends, about your whereabouts, and about your preferences."

With heightened publicity and awareness, privacy has escalated to become a major concern for the average mobile app user. There is increasing awareness that all personal and identifiable data on a smartphone or tablet does not necessarily remain on that smartphone or tablet.

Some iOS and Android apps will access and share data. Sometimes they do this without the user even knowing. Sometimes nothing is shared and there is no personal information involved.

Key legal issues

1. Be clear what your app does from the start

A simple app can initiate complex interactions between multiple parties or organisations, from the mobile network operator to the app store. Each party can have a stake in the relationship with the user. The mobile app owner cannot control all those acting in the background and therefore needs to pay greater attention to how it manages and controls data.

Right back at the point of conception of the mobile app, the owner needs to think about what the app is going to do, what types of information it may process and whether there are any potential privacy challenges. The app can then be developed and launched with these challenges in mind and the consequences of data use provided for. There is a genuine need for effective privacy-by-design, which considers and anticipates the privacy challenges before they eventually arise.
2. Understand and communicate data uses

In February 2012, the Global System for Mobile Communications Association (GSMA) did us all a favour by launching its “Global Privacy Design Guidelines for Mobile Application Development”. This example of self-regulation promotes “transparency”, “choice” and “control” for mobile app users over how mobile apps use personal data. These principles are core to any responsible privacy framework for the mobile ecosystem. Any responsible player in the mobile app market should be open and honest with users about how and why they are using consumer information and with whom they are sharing it. Introducing an element of control for the customer and ensuring their personal information is protected and secure will ensure credibility.

3. Be open - particularly where children may be involved

Any mobile app or service directed at children or adolescents poses additional compliance hurdles. Whilst the Data Protection Directive does not instil any specific child protection measures, the age of consent does vary across EU Member States, and minors cannot enter binding contracts. More easily compromised, their information needs to be handled with extra care, not least because of the PR harm that may result if mistreated. For more detail see the section on Data and children later in this report.

4. Dealing with shared devices

Another complex area is shared devices and how to regulate and practically approach the challenges these present. Both children and their parents can share the same device, and in app interactions and transactions, this can cause real problems when the real user cannot be distinguished.

5. Area of regulatory focus

It is worth noting that mobile apps are increasingly a focus of regulatory scrutiny in Europe. The Irish data protection regulator has been looking into the area, which is particularly important given it is the European home to many US digital businesses like Facebook.

Mobile apps are also high on the agenda of Europe’s Article 29 Working Party, the body of European data protection regulators tasked with advising on European data protection policy.

6. Take care with T&Cs on the small screen

With the mobile app there is reduced space to communicate the core privacy and contractual messages. A good developer will use this space wisely. As ever, where consumers are involved this should be kept clear and accessible and remain in plain and intelligible English.
Evolutionary challenges

If you remember nothing else

• Be clear what information the app might process, and the regulatory impact, at the start of the design process.
• In the absence of official regulation, consider some of the self-regulation options to future-proof your product. This will help with the increased scrutiny from European regulators.
• Identify where you might be directing services at children and make sure you comply with the rules
• Write the contractual and core privacy messages so that they are clear, concise and accessible on a mobile interface

What the future holds

It will take years for regulators and the courts to clarify the legal boundaries relating to mobile apps. In the interim, there has been a surge in self-regulation and the promotion and sharing of best practice. Whilst not the law, the self-regulation coming through is often sensible, and tends to strike the right balance between individual rights and everyday commercial desires. If you are launching a mobile app you can reduce risk and future-proof your product by adopting a privacy-by-design approach, minimising the use and sharing of personal information and adopting some of these best practices. Furthermore, be advised to reign in some desires to harvest and collect data – just because you can, doesn’t mean you should.
Evolutionary challenges

In the computer games industry, the word “transition” is generally used to refer to the introduction of a new generation of games consoles.

However, the games industry is currently in the midst of a different kind of transition, as it moves from the sale of games as physical products in retail outlets, to the digital distribution and streaming of games direct to consumers.

The nature of game playing is also changing. Traditionally seen as a solitary activity, predominantly undertaken by young men, gamers are increasingly meeting and interacting with each other, albeit virtually, through the online functionality provided by PC and console games like Call of Duty, or in so-called massively multiplayer online games (MMOGs) such as World of Warcraft and Eve Online. The growth of mobile and social games has also made game playing a mainstream activity.

All of these changes mean that a publisher of a MMOGs or the operator of a social game can collect a considerable amount of data about the players. In addition to all of the usual issues that the collection and processing of data creates, there are some unique issues in relation to games:

Key legal issues

1. User names and avatars

To set up an account with an MMOG, a player needs to provide an email address and choose a user name. The user name will be unique to that player and will be the name of the player that appears in the game. Some MMOGs also enable a player to create a character, known as an avatar. In some MMOGs this is very simple process with limited variables, but in others, sophisticated avatar creation tools enable players to create unique avatars.

A player's user name and avatar will be linked to the player's account. It follows that for the MMOG publisher, data relating to that user name and avatar will be personal data. However, the players themselves will not know the identity of each other from the user names or avatars that appear in the game. Nevertheless, it is still possible for user names and avatars to be personal data.

The Article 29 Working Party has expressed the view that it is possible to “single someone out” without knowing the name of that individual. A player's user name or avatar may therefore become that player's “digital identity”. Potentially this opens the data up to compliance with the European Data Protection Directive and avatars could be construed as personal data. This may become more of an issue as celebrity players emerge and as greater functionality is developed for players to engage and interact with each other in guilds, clans or other groupings within MMOGs and social games.

2. Children's data

An important consideration with gaming is the potential to collect information about children. There are various requirements around parental consent across Europe, which we have covered in more detail in the later section on Data and Children.
3. In-game advertising

Many social games and some MMOGs rely wholly or partially on advertising revenues. As with any online advertising, an advertiser or advertising network will try to target the players most likely to be interested in the advertised products or services. To be successful, they will want as much information as possible about the players, such as how often and for how long they play the game, their progress in the game, their age and their gender.

An advertising network will then use anonymous user data to build a profile of that user. Although the European Data Protection Directive only relates to “personal data”, many privacy regulators in Europe consider this anonymous data to be personal data, because although the data does not identify any individual player, the profile of a player will be used to serve targeted advertising to that player.

In addition, to comply with the European Privacy and Electronic Communications Directive, a player’s consent is required before data can be accessed from or stored on that player’s PC or games console for any reason that is not “strictly necessary”. The use of this data for the purposes of advertising will fall outside this limited exception, and so the consent of the player is required.

4. Legal challenges of an international footprint

Data privacy laws struggle with the international aspects of data collection and processing and an MMOG is a good example of these difficulties in practice. MMOGs are available worldwide. Players can live anywhere in the world, an MMOG can be hosted on servers anywhere in the world, and the publisher of the MMOG might have operations anywhere in the world. Trying to determine which laws apply and when can be complex.

This has been demonstrated by the recent changes to the use of “cookies” and similar technologies, which are relevant to game sites.

What the future holds

Data and data privacy issues will only grow in importance for computer game publishers. The future changes in European data privacy law are likely to have significant implications for any publisher that does business in Europe, wherever they are established.
Evolutionary challenges

If you remember nothing else

- MMOGs and social games can grow extremely rapidly. It is therefore essential to plan ahead and consider privacy issues from the outset and before substantial amounts of data are collected.
- As MMOGs and social games grow, publishers must monitor and track developments and make relevant people in the organisation aware of the key privacy issues. It is not uncommon for a development team to add or change functionality in a way that raises privacy considerations, but be completely unaware that this may be an issue.
- Make sure you know what is ‘personal data’ and therefore subject to the European Data Protection Directive, particularly with regards to avatars and in-game advertising.

Contact details

Paul Gardner
Partner
E: paul.gardner@osborneclarke.com

Konstantin Ewald
Partner
E: konstantin.ewald@osborneclarke.com
Most data currently collected has been user-generated. The ‘Internet of Things’ involves data collected from machines.

Essentially, it describes a future where everyday objects such as phones, cars, household appliances, clothes and even food are wirelessly connected to the internet through smart chips that can collect and share data without human intervention.

A key technology involved in the ‘Internet of Things’ is machine-to-machine communications (M2M). This involves devices actively communicating using wired and wireless networks. They are not computers in the traditional sense, but use the internet in some form or another.

The impact of M2M communication is wide-reaching and the effect on our everyday lives is likely to be substantial. M2M communication could incorporate managed connectivity, transport, utilities and sustainability: anything from your central heating being turned up remotely from your mobile, to your fridge adding milk to your on-line shopping order when stocks are low. Undeniably a new opportunity that could generate significant benefits, it does come with regulatory and privacy concerns. In particular, concern exists over the current rules and whether they provide the necessary balance between economic and societal benefits in the context of an environment where machines will gather, exchange, process and store information automatically. The ability of one provider, or a cartel, to exercise unfair control over data by running key parts of the environment is one concern.

In 2012 the EC consulted on wirelessly-connected devices or the ‘Internet of Things’, seeking comments on privacy and information security issues. The Commission aims to “unleash the potential economic and societal benefits while ensuring an adequate level of control of the devices gathering, processing and storing information”.

Key legal issues

The use of M2M is shifting the market from one where users have a relatively limited number of communication devices to one where they have thousands, or in the case of business users, potentially millions. As with any new areas of technology, the law is playing catch up. There are some key areas that businesses in this market need to consider:

1. Privacy and security

M2M certainly impacts privacy and security. Although it is accepted that not all M2M services on their own will give rise to privacy issues, many are concerned by the compound extent that a proliferation of smart networks and devices might bring and the detailed view into a user’s life that could be assembled. If several devices are communicating per person, then there will be a significant increase in the types of information gathered on individuals, such as health data, reading habits, location data, energy use, driving style and eating habits. This could, of course, be of huge value, especially to advertisers.

When assessing privacy issues in the use of M2M it is not enough to look at the service itself, because the communications network used for the service will add a layer to the privacy assessment. Similarly, the sharing and combining of data through cloud services will increase the locations and jurisdiction where personal data sits and so may expose the services to a wider scope of privacy regulation.
Machine-to-machine data collection
Angus Finnegan

2. Communication infrastructure and services
The ideal M2M communication technology would allow secure access to the internet anywhere in the world at any speed. It would work equally well indoors and outdoors and have unlimited range whilst costing virtually nothing and consuming no energy.

With this comes a variety of general requirements together with associated compromises. There is no one technology that fits every requirement for the efficient use and economic development of M2M. What is clear is that choosing the right M2M communication solution is not as simple as connecting a communications device on to a machine. The challenge will be assessing whether the chosen system is future proof or not and whether it can cope with changing demands.

For policy makers it should be clear that when relying on M2M in some form to support policies, there are compromises and these compromises will impact the viability and success of a project at every level.

The future of M2M
M2M communication will play a key role in the Internet of Things. The sale of M2M communication will grow across industries such as consumer electronics, automotive and energy. Indeed, in July 2012 seven mobile operators teamed up to create an alliance to collaborate in the M2M space.

The EU Commission is taking note. The Commission hopes that through its consultation, the public’s views on the key issues of privacy, safety and security, security of critical infrastructure, ethics, interoperability, and governance and standards will feed into the Commission’s Recommendation on the ‘Internet of Things’. These recommendations will be published by summer 2013.

Boosting the ‘Internet of Things’ remains a priority for the Digital Agenda for Europe and although it could take up to three years for a legislative proposal to emerge from the dialogue between the European Parliament and EU member states, the open debate will be welcomed by the first adopters and service providers of M2M.

If you remember nothing else
• For those developing elements of M2M networks, an ability to prove independence, openness to the consumer regarding data usage and best practice security are key.
• Regulators and legislative bodies may struggle to accept that economic benefits outweigh privacy concerns, but that is where providers are likely to take the debate.

Contact details
Angus Finnegan
Partner
E: angus.finnegan@osborneclarke.com
Children and young adults are often part of the target group for internet-based services, whether those are online games, mobile apps or social networks.

From a legal point of view a minor is not just any other customer. A service provider who wants to expand its target audience to include minors has to consider the special regime that the law creates to protect children – especially when it comes to their personal data. Even in the European Union there are no common rules for dealing with children's data.

Key legal issues

1. Age of majority: Who is considered a minor?

At the outset, the most important question is who is considered a minor. In connection with online services there are basically two different legal perspectives: civil law and data protection law.

Almost every jurisdiction has age thresholds and age-based restrictions to protect minors from negative business decisions. In Germany and France, for example, children and adolescents under the age of 18 generally cannot enter into and enforce contracts without parental consent, whereas in Scotland the age limit is 16. Across Europe, the age of majority varies between 16 and 18, and worldwide the variance is between 14 and 21.

Even the legal consequences of these age limits differ significantly. In Germany, for example, a person under the age of 18 cannot enter into a contract – except if this contract is "exclusively legally advantageous". In England, on the other hand, children generally can enter into contracts, but such contracts cannot be enforced against them (voidable).

In a nutshell, the legal meaning of the term "minor" varies from jurisdiction to jurisdiction. That makes things complicated, but also opens opportunities to find individual solutions. If you look closely, many jurisdictions offer practical ways to provide services and products to minors, as long as their protection is not undermined.

2. Data protection: Minors and their data

A key aspect when dealing with minors is data protection and privacy, since consenting to collection of data is a different legal matter from entering a binding contract. Whereas the United States has established the Children’s Online Privacy Protection Act (COPPA) to restrict collecting and processing of children's data, there are, again, no common European rules, even if the national rules tend to be quite similar. In many EU member states, the minimum age for consenting to the processing of data depends on the cognitive faculty and capability of understanding of the individual person in the specific situation. This has two implications: First, there is no safe age limit you can strictly rely on. You always have to consider the specific situation. Second – and this is the good news – you may be able to influence this situation and thus the minimum age for consent, for example by providing information about privacy and data protection in a child-friendly and easily comprehensible way.
Data protection authorities in many countries have provided “rules of thumb” as a rough assessment for the legal age for data protection related consent. In England, for example, collecting data from children under 13 years usually requires parental consent. In Germany it is assumed that minors can start deciding about the use of their data for themselves somewhere between ages 14 and 16 – depending on the specific context. Most authorities in other European countries recommend similar age spans. Some examples are set out in the table below:

<table>
<thead>
<tr>
<th>Country</th>
<th>Restrictions and recommendations for collecting data from minors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>No explicit legal restrictions and no case law yet. Validity of consent for regular data depends on capacity of understanding although 14 is often taken as the relevant age. For sensitive data, parental consent is required for all minors.</td>
</tr>
<tr>
<td>Belgium</td>
<td>Under 12 parental consent is needed 12 – 14 years there is a presumption that the minor has the mental capacity and parental authorisation is not required (but presumption can be reversed); above 14 years parental authorisation is not required unless it is proven that the minor does not have the mental capacity.</td>
</tr>
<tr>
<td>Denmark</td>
<td>Practice of the Danish Data Protection Agency: Consent cannot validly be given by children under the age of 15. Consent between 15 and under the age of 18 requires that the person understands what their consent entails.</td>
</tr>
<tr>
<td>France</td>
<td>Minors cannot validly declare their consent. The French Data Protection Agency (CNIL) considers collection and use of minors’ data without parental consent illegal in many situations, including use of a minor’s image and transfer of a minor’s data obtained through games and lotteries to any third party. The only data that may be collected from minors in connection with newsletter subscriptions is an e-mail address and age.</td>
</tr>
<tr>
<td>Germany</td>
<td>Parental consent required for under-14s and parent usually has to provide the information. Between 14 and 16 consent may be needed depending on the specific context, and capacity of understanding.</td>
</tr>
<tr>
<td>Italy</td>
<td>No specific data protection law rules. Minors (under 18) cannot validly declare their consent, at least not where data is collected in connection with the provision of goods and/or services.</td>
</tr>
<tr>
<td>Portugal</td>
<td>Generally, only persons who are 18 years or older have full capacity to contract. Consent from minors age 16 and over is likely to be valid.</td>
</tr>
<tr>
<td>Spain</td>
<td>Minors can validly grant consent at age 14. Under the age of 14, verifiable parental consent is required.</td>
</tr>
<tr>
<td>Sweden</td>
<td>Consent requires that the person can fully understand the information in the consent declaration. As a rule of thumb, a person under 15 does not meet this requirement, but everything depends on a case-by-case assessment. Some specific rules restrict use of minors’ data, e.g. commercial communication may not be sent to anyone under the age of 16.</td>
</tr>
<tr>
<td>UK</td>
<td>Depends on complexity of data and proposition and a risk-based approach. Guidance from the UK Data Protection Authority in their on-line Code of Practice states that parental consent is normally necessary to collect data from children under 13.</td>
</tr>
</tbody>
</table>
Evolutionary challenges

3. How to get parental consent

This can be particularly challenging online where you do not necessarily know if you are dealing with a parent. The mechanisms to get consent are not generally prescribed and can vary from a simple tick box, email notification and response or even provision of ID documents (Spain) or credit card number (US COPPA).

4. Tact, sensitivity and communication

There are various different restrictions to be aware of as a provider of online services directed to children. The processing of children’s data is a touchy subject that needs a tactful and sensitive approach. What kind of data do you really need from children? Can you provide dedicated solutions for a younger audience? What kind of precautions and measures are necessary to provide a harmless and safe experience for children on a specific platform?

Many problems in connection with children in the audience can be solved with a little creativity, but the challenge is to communicate privacy and data protection issues in a clear, easily comprehensible and child-friendly way. The crucial point is a comprehensive and customised strategy, considering the several legal frameworks as well as the specific needs of your young customers.

Other key challenges

New media, particularly in the form of social networking, brings additional challenges, such as where children create profiles, provide photos, create avatars, play games, include photos of other children, enter competitions and include videos and photos. Additional issues arise where children provide information about other children and the need to get parental consent to cover other children in photos or entering competitions.

Issues also apply to who can have access to data, such as moderators, and the vetting of moderators or other third parties who may access information. If children are involved in product testing, for online games for example, then information will be collected in this context.

Other areas to consider, particularly with social media, are the risks of collecting sensitive data about health or issues where children indicate an intention to harm themselves or others. Consideration is needed on whether information can be disclosed to the police or other authorities and a policy should be in place for dealing with such issues.

Security is always a concern when collecting data but becomes of even greater importance when storing information about children and the increased sensitivity and risk in the event of disclosure.

Issues may also arise with viral marketing and “send to a friend” type mechanisms which could result in children providing personal information about other children. There may also be other considerations in relation to marketing, which restrict advertising to children on websites or the sending of commercial emails.
Evolutionary challenges

If you remember nothing else

• Check the structure of your audience and try to define your target group as precisely as possible – especially regarding the location and age of your visitors.

• Try to define the type of data you want to collect from your users. Distinguish between data you need to collect and data you want to collect. Keep in mind that you should keep the data collected to a minimum – in particular when you collect it from children.

• Now that you know your target group and the type of data you need to collect, try to define a minimum age for your users. Take into account where your audience is from, the complexity of your product, the sensitivity of data and the features and measures you will take for data protection. Try to form an opinion on your own product from a neutral point of view.

• Check your products and services and try to design them in a way that meets the specific needs of your young audience. If you target your product to minors with a minimum age of 14, make sure that a 14-year-old adolescent is able to understand all necessary information about your data processing. Use simple language, illustrations, small educational games or videos - whatever is needed to make your message clear.

• Look at some form of “age gating” online and be aware of different ages in different locations.

• Consider the mechanism for obtaining parental consent and look at the potential risk to determining the form of consent, i.e. the greater the risk, the more stringent the mechanism.

What the future holds

The European Commission is planning a new legal framework to unify data protection legislation in the EU. A proposal for a new Regulation was published in early 2012.

According to this document, the processing of data will require parental consent for all minors, defined as persons under the age of 18 years. The draft Regulation reduces the age for parental consent for online activities to 13, but requires “verifiable consent”. No guidance has been provided on how to achieve this. At this point amendments are expected but it is clear that a common set of uniform rules is on its way.

Contact details

Sue Gold
Partner
sue.gold@osborneclarke.com

Konstantin Ewald
Partner
konstantin.ewald@osborneclarke.com