Digital world and private lives

10

In this chapter, Dr Michelle Goddard and Debrah Harding of MRS review the current data and privacy landscape, the legislation which affects data and the impact it has on research, and an MRS initiative, Fair Data, which has been established to retain and regain trust in the data world.

The data landscape

Data has always been gathered on individuals. In the past, the issue was the relative scarcity of data. Today, technology has liberated the collection of data to such an extent that data is now collected on a continuous basis for most aspects of our lives. This takes place via wearables, phones, cameras and, with the Internet of Things, can happen using almost any conceivable device.

To offer some context, 90 per cent of the world's data was created in the last two years.[1] An estimated 2.5 quintillion bytes of data are being generated every day and it is estimated that, by 2020, 40 zettabytes of data will have been created, a scale so large as to be almost unimaginable.[2]

Developing in tandem with this has been a huge sea change in the way such data is held and distributed. Data is no longer necessarily held within the confines of any specific organization's mainframe or a country's borders. Instead the data cloud is the reality for digital data collection, processing and transfer.

The 'quantified self'

Significant amounts of data collected are non-personal data, such as financial and environmental data and so on. But a significant part of this growth is in

personal data, as a result of increasing amounts of data being captured from and about individuals.

Some of this is as a result of purposeful participation by individuals in activities such as social media. In 2015, it was estimated that there were over 2.206 billion active social media users, a global penetration of over 30 per cent.[3] Facebook alone had 1.59 billion monthly active users.[4]

However, it is not just social media activity which is generating the data about individuals. There is also the emergence of the 'Quantified Self': individuals engaged in a variety of physical, biological, environmental or behavioural activities where data is acquired from individuals through technology such as wearables, or portable devices, mobile apps and so on. Want to track physical activity, heart rate, happiness, mood, food consumption, travel, the amount being quantified? No problem, there is an app somewhere that can do this.

Risks and threats

With so much data being generated, the risks and potential for harm inexorably increases. Data scandals have been a common feature of the last few years, although the nature of these is evolving. Data losses and cyber-attacks are still very much in evidence, with an estimated 5.1 million incidents of fraud identified in the UK in 2015.[5] Organizations that are being hacked no longer just suffer the embarrassment of the publicity of being breached, often they are also being held to 'ransom' with their data as the 'captive'. Sony Pictures, TalkTalk, Ashley Madison and Domino's Pizzas were the unlucky recipients of these kinds of proposed 'trades'. It is not just big business that is suffering; in a recent study by KPMG, 60 per cent of small businesses that were surveyed had experienced a cyber breach of some sort.[6]

These data developments do not operate in a vacuum and, with increasing awareness of 'Big Data', the rise of data hacking and data abuse, inevitably individuals' views on data usage and privacy concerns are also evolving.

The privacy landscape

Data usage and privacy is a global issue of increasing concern to citizens. The Data Protection Eurobarometer study, conducted among the European Member

States, tracks attitudes of European citizens to data issues.[7] The 2015 study reported that trust in the digital environment continues to be low, with 67 per cent of participants stating they were worried about having no control over the information they provide online, while only 15 per cent feel they have complete control. Furthermore, 63 per cent of participants stated they do not trust online businesses and 62 per cent did not trust telephone and internet service providers.

These findings are replicated elsewhere around the globe. The Global Research Business Network (GRBN) Trust & Personal Data Study 2014 supported these findings, with 36 per cent of all participants expressing high levels of concern and 45 per cent fairly concerned about how personal data is collected and used. [8]

The value of data

With this increasing concern comes increasing awareness and with it the realization by individuals of the ability to leverage value from personal data, and to make much more nuanced decisions and data trades. A 2014 study by Orange, *The Future of Digital Trust*, identified that consumers attribute a value of approximately €15 to an individual piece of data with a brand they know.[9] This increases to approximately €19 for unfamiliar organizations. In this study, 80 per cent of participants knew their data had value for business and 67 per cent of participants believed that organizations benefited the most from the sharing of data. Studies such as this highlight the changing nature of the data relationship and the increasing tension that exists between those who provide data and those who use data, and the need to create an environment for a more balanced social contract.

But how can this situation be addressed? Legislation is one way to address the social contract (the 'stick' approach). An increasing number of countries are enacting some form of data protection and privacy legislation, and more are considering introducing it, as citizens become more aware of the dangers as well as the opportunities of 21st-century technology. One of the most significant developments is the new General Data Protection Regulation (GDPR), which is currently being finalized in Europe.

The legislative landscape

The finalization of the GDPR represents the culmination of the modernization of the data protection framework across the European Union (EU). Driven by dual imperatives, of giving individuals control of their data and a desire to simplify the regulatory environment for businesses, the new legislation is expected to come into force in all member states of the EU in the second half of 2018. As a regulation it will be implemented directly, replacing the current divergent national laws based on the EU Data Protection Directive of 1995 and in so doing creating a more harmonized data protection landscape. There are a number of key areas within the landscape which we should consider.

Informed consent remains the foundation for data processing

The essence of data protection legislation is to ensure that personal data is only to be gathered and used by businesses (as data controllers or data processors in data protection terms) on specified lawful grounds. The GDPR extends the understanding of personal data, which is any information 'relating to' an individual, to specifically include online identifiers such as cookies and advertising IDs used extensively in the online and mobile world. These will now be considered to be personal data, along with anything that contributes to identifying an individual, or links to such identifying information. Additionally special categories of personal data which require explicit consent have been expanded to include biometric and genetic data along with data such as race, health, sexual life, criminal offences, religious beliefs and political opinion and trade union membership.

From a research perspective, the most important of the lawful grounds for processing data will continue to be informed consent. By gaining clear consent from individuals to process their data, researchers can develop and build trust. The social contract between research practitioners and research participants relies on informed consent and respect for the rights and well-being of individuals. The importance of recognizing and reiterating this in robust data practices is reflected in the new legal framework. The GDPR introduces a higher consent bar, requiring freely given, specific and informed consent demonstrated through clear affirmative action. A key part of the test of valid consent is whether individuals actually understand what they are agreeing to, and are given a meaningful choice. This focus on securing informed and transparent consent is reflected in the sector's various codes of practice/conduct for research, such as the MRS *Code of Conduct*.

There are other grounds for businesses to process the data of individuals, such as on the basis of their legitimate interests. Using this ground is a balancing act which must take into account the reasonable expectations of data subjects and should be conducted in line with compatible purposes. As research is expressly considered to be a compatible purpose for data use, research can legally be carried out on customer databases on this ground. The GDPR also continues a research exemption (if allowed by national law) which will allow data to be processed, where no other ground is feasible, and technical and security safeguards such as encryption or 'pseudonymization', ie de-identification of the data, have been put in place.

Giving control to people by focusing on the data subject

Facilitating the control by individuals over their personal data is a pivotal part of the comprehensive overhaul of the law. The new and enhanced individual rights, over this wider notion of personal data, are the foundation of the new regime.

These include:

- New right to be forgotten or 'right of erasure' which codifies recent European case law and allows individuals to request that personal data, made public especially in online environments, be erased. Businesses will still be able to process the data if there are compelling legitimate grounds for processing to continue, but are obliged to inform other businesses who may be processing the data to delete it if this request is received.
- New right of data portability will allow individuals to request that their data be provided in a usable, transferable format, allowing them to move data between platforms or suppliers. This right will apply where the personal data details have been collected by automated means on the basis of an individual's consent or contract.
- New right, albeit of a more limited impact, to request that data processing is restricted, especially where the data cannot be deleted, such as where it is required for legal reasons.
- New general right to be informed about significant data breaches. Serious data breaches must be notified to the data protection authority and if the breach presents a risk to individuals (such as identity fraud) they must also be directly told about the breach.

CASE STUDY 1 Mydex

Businesses that enable individuals to take control of their data, empowering individuals to be more confident participants of the 21st-century digital data economy, are essential for a balanced social contract between business and individuals; and will be crucial for the forthcoming legislative changes to have the desired outcome.

In this case study, Mydex, a Fair Data enabler, sets out its role in enabling individuals to take control.

Mydex is a Community Interest Company. It is asset locked. It serves individuals by helping them manage their lives more effectively through provision of tools and services that let them collect, accumulate, organize, analyse and share the data about their lives — whether this is data that organizations hold about them, that they generate themselves, or is generated around them through daily living. Fair Data certification is an important external indicator of our commitment.

Personal data is valuable, and personal control over personal data requires both transparency and trust. Mydex's mission as a Community Interest Company and operator of a Trust Framework and secure platform is to demonstrate this internally and externally. Certification as a Fair Data Company and the first certified Fair Data Enabler is an important external measure of trust, as is our ISO 27001 certification for information security management.

Connecting to the Mydex Platform also delivers benefits to businesses, their customers and the long term relationship they have with each other. It reduces friction in customer journeys, effort for the customer and the organization, and back-office costs in terms of verification, data logistics and achieving compliance.

Mydex acts as a neutral, non-competing, public service platform, and is designed to embed trust in all transactions and interactions between organizations and those they service and support.

Connecting Mydex to existing systems and services is easy and the entire customer journey and brand experience remains with connecting organizations.

Mydex enables organizations to open up new channels of engagement, support omni-channels more easily and access a broader, richer set of timely and accurate information about customers, secure better insights and achieve easier personalization of services at the same time as assisting in achieving Fair Data certification.

Strengthened right to object to direct marketing

Individuals have a right to object to profiling and not to be subject to decisions based on automated processing. The profiling activities that are relevant here are those done through automated processing where a decision is made that has legal or significant effects on individuals. Importantly, this will not cover research activities such as segmentation, as these are not designed to have legal impact directly on individuals. There is also an absolute right to object to processing for direct marketing and profiling for direct marketing without being required to provide specific reasons.

Enhanced information rights

Information rights have been significantly enhanced. Individuals must be given a far greater amount of processing information, such as the source of the data and the period for which the data will be held. The information also has to be provided in an intelligible form and using clear accessible language. Interestingly. there is now a duty on businesses to promote all of these rights to individuals.

Alongside these new substantive rights are procedural rights which mean that if authorities do not act then individuals can (on their own or with representation) as can consumer protection groups (if allowed by national law).

Underpinning the strengthened individual rights is one of the key features of the GDPR, namely that it will have extraterritorial application. All organizations processing the personal data of EU residents will be required to comply with the provisions of the regulation, regardless as to where the business is located. Businesses which offer goods or services across borders, or monitor activities of EU subjects, will now be covered by EU data protection laws.

Accountability obligations

Businesses will no longer be required to notify or register with their national data protection authority. However, this bureaucratic requirement will be replaced with more detailed requirements on businesses, such as ensuring full record keeping of processing activities, conducting privacy impact assessments and embedding privacy by design and default throughout the business. For research practitioners it will be pivotal to use organizational technical and security safeguards, such as de-identified or 'pseudonymized' data. This is still personal data, but it is a mechanism for minimizing risk.

Increased obligations on data processors, which previously had fewer statutory obligations, mean that the risk profile of data processors such as transcribers, storage providers and recruiters has been raised considerably. This is in part because their role meant that they did not determine the purposes for which the data will be used. Researchers of all sizes and involved in all types of activities, from panel research to qualitative focus groups and quantitative surveys to data analytics, will need to take steps to become fully data protection compliant. Guidance from national and European data protection authorities, as well as the European Commission, will shape the precise manner in which the technical rules in the finalized framework are enforced. MRS will interpret these, looking specifically how they apply in the research context, to assist researchers across all areas of research in understanding their obligations.

CASE STUDY 2 Ark Data

The strengthening of regulators' powers, the huge increase in sanctions, and the increased obligations being placed on businesses across all touch points in the data journey, will mean that those businesses and organizations that invest in robust, well-managed processes, with partners they can trust to deliver, will be crucial for staying on the right side of the new legislation.

Here Ark Data, a Fair Data accredited company, sets out how they help businesses keep their data up-to-date.

Your data might be secure but is it up to date?

Many businesses spend vast amounts of time and money ensuring their data is secure. But what about the quality and accuracy of that customer data?

In the UK over 500,000 people die and more than 6 million people move home every year. Customer data decays rapidly and not doing anything about it can be risky:

- Assuming the identity of the deceased is the easiest way to commit fraud (currently estimated at over £52 billion per annum).
- Mailing the deceased causes upset to the bereaved, leaves brands open to criticism by the media (think of what happened to the charity sector last year) and is expensive and wasteful.

- Internal analysis and reporting using out-of-date and inaccurate customer data means businesses are working on potentially dangerous information.

The Ark is a data quality business that owns and publishes two data products: the **National Deceased Register (NDR)** and a 'gone away' suppression file called **Re-mover**. NDR is a database used by our licensees to identify and remove customers and prospects who have died from their own databases and lists. Re-mover does exactly the same but for customers and prospects who have moved home.

The Ark's clients span many sectors including financial services (banking and insurance), retail, charity, utilities and mail order. The Ark is a **Fair Data**™-accredited organization and its people are passionate about raising the profile of data quality, working hard to encourage compliance with best practice in data suppression and adherence to the Fair Data principles.

The Ark offers a **free data audit service** to help businesses understand the weaknesses in their data and show how we can help businesses avoid unnecessary risks involved with relying on inaccurate data that could lead to potentially expensive outcomes.

High sanctions are part of the enforcement toolkit

Data protection authorities have been given a much wider range of powers for enforcement of the data protection rules. The new level of administrative fines have grabbed the headlines and are significant. Penalties currently imposed in different jurisdictions of the EU pale in comparison to the new approach. For example, the highest penalty previously imposed in the UK is £350,000; in Germany it is €1.1 million and in France €150,000. All of these fines are much lower than the maximum allowed penalties under the new law of up to 4 per cent of worldwide turnover or €20 million. In addition to fines, the authorities also have greater investigative powers to compel information from businesses and gain access to premises.

Shaping the new social contract

Compliance needs to be placed at the core of operations by enshrining privacy by design as a default. This goes hand in hand with the recognition of the social contract and the value exchange for data that powers the digital economy.

In this new environment it is critical that data-intensive business, such as research, continues to demonstrate respect for individual rights and enshrine this within their business operation. Adopting an approach that embeds privacy at all stages and all touch points in the data journey – from collection through to analysis and reporting – should be the overriding and primary consideration for businesses. As awareness of data protections and rights increases, the commercial implications and reputational impact means that focus across all industries on securing consumer and customer trust will accelerate.

So where do we go from here?

The growing sense of imbalance in the data-sharing relationship between individuals and business, the deterioration in trust, the commoditization of personal data and the increasing legislative environment all point to a more complex data environment – so what can we do?

Fair Data

In January 2013, MRS launched a new ethical consumer mark for personal data, called Fair Data. The trust mark means that members of the public are able to easily identify between those organizations that collect, use and retain personal data properly and ethically, and those that do not (and is more of a 'carrot' approach to data compliance).

As can be seen from the research, consumers gravitate towards companies they trust. Recognized ethical marks help consumers make choices, separating trustworthy brands with those which share their values. This has been learned from other industries such as Fairtrade, Investors in People (IIP), recycling symbols and so on. Launched for all those organizations – public and private sector – that collect and use personal data, Fair Data is becoming a recognizable standard for organizations that can be trusted to do the right thing with individuals' data. It has been designed to be used internationally, integrating and complementing business-to-business initiatives like the data transfer arrangements such as binding contracts, the US/EU Privacy Shield and the Data Seal of Approval initiative in Europe. Fair Data has also been exported to other markets, such as Singapore.

FIGURE 10.1 The role of fair data in corporate responsibility

Fair Data uses ten principles based on rules from the MRS *Code of Conduct*, and data protection legislation, which have been re-positioned to aid consumers' understanding of their rights and organizations' obligations in terms of protecting their personal data.

By signing up to be a Fair Data organization, organizations agree to: adhere to the Fair Data principles and to use the Fair Data mark in all relevant dealings with customers and participants.

By creating a seemingly simple approach of ten principles, the scheme can be easily understood by a wide range of organizations. To highlight this, two different organizations – personal data store Community Interest Company Mydex, and data quality specialists Ark Data – explained in the case studies why they become Fair Data accredited.

However, for all its perceived simplicity, the accreditation is a robust all-encompassing approach. Through the ten principles all minimum legislative requirements have been covered, and in addition broader ethical requirements including the ethical treatment of vulnerable citizens, and ethical supply chain management and procurement are incorporated. Table 10.1 summarizes the ten principles demonstrating the higher standards that are being met by those organizations that have achieved Fair Data accreditation.

Fair Data is a unique innovation, which addresses an issue that is impacting business, society and citizens. Fair Data is the only data trust mark scheme

TABLE 10.1 Fair Data Principles

Data Topic	Fair Data Principles
Consent	1 We will ensure that all personal data is collected with customers' consent.
Data use, retention and quality	2 We will not use personal data for any purpose other than that for which consent was given, respecting customers' wishes about the use of their data.
Data access	3 We will make sure that customers have access to their personal data that we hold, and that we tell them how we use it
Data security and transfer	4 We will protect personal data and keep it secure and confidential.
Protection/avoidance of harm	5 We will ensure staff understand that personal data is just that – personal – and ensure that it is treated with respect.
Vulnerable adults and children	6 We will ensure that the vulnerable and under-age are properly protected by the processes we use for data collection.
Clients, suppliers and the supply-chain	7 We will manage our data supply chain to the same ethical standards we expect from other suppliers. 8 We will ensure that ethical best practice in personal data is integral to our procurement process.
Staff training	9 We will ensure that all staff who have access to personal data are properly trained in its use.
Professional reputation	10 We will not use personal data if there is uncertainty as to whether the Fair Data Principles have been applied.

to receive support from the UK's data protection regulator, the Information Commissioner. It is a scheme that brings all constituencies together, and embeds trust, in a world where the digital data economy is the driving force for businesses, society and citizens. Fair Data has also been recognized more widely, including winning Best Innovation at the Association Excellence awards 2015.

Conclusion

For business, the Corporate Social Responsibility agenda is becoming increasingly important as brands strive to differentiate themselves.

This is not about businesses being legal: for any brand or business to survive it needs, as an absolute minimum, to meet its legal obligations. But as the public becomes more wary of data issues, the brands that thrive will be those that put ethical, customer-centric business practices at their core. With Fair Data, MRS is providing a framework to help businesses to do this.

Research studies such as Orange's *Future of Digital Trust* report highlight that opportunities exist for those organizations and businesses that are intelligent, consensual and responsible in their use of consumer data, with trustworthy data use becoming increasingly a fundamental requirement, which will have a significant impact on companies' overall reputations. Equally, as the public become more mindful of sharing their personal data, the effect could have long-term implications for businesses and society.

There is clear value for business in not only *saying* the right things, but *doing* the right things. But to be responsible – to be trusted and meaningful – requires not only investment in processes and procedures, but a fundamental re-think about data. Technology enables businesses to do amazing things; what is often forgotten, however, is the question of whether they should be doing these 'amazing things'! What looks like a transformative data technology approach to a business can look scary and intrusive to a customer.

In the words of Andreas Koller, 'Data is people in disguise.'[10] Businesses need to re-orient their thinking about data; yes it it is Big Data, Smart Data, Actionable Data, Insightful Data, or however else you wish to describe it, but data *is* people. Treat the data as you would the human. Think of data in the same way as if the human behind the data were standing in front of you. The businesses and organizations that are able to put this 'human' data mindset at the heart of what they do, will be the ones that gain the trust of people, and will be the ones that flourish. Researchers, with their exceptional skills understanding people, are uniquely placed to serve as the bridge between organizations and their data, giving people a voice for the benefit of all.

References

1 IBM www-01.ibm.com/software/data/bigdata/what-is-big-data.html
2 IBM www.ibmbigdatahub.com/infographic/four-vs-big-data
3 *Social Media Today* www.socialmediatoday.com/social-networks/kadie-regan/2015-08-10/10-amazing-social-media-growth-stats-2015
4 Facebook http://newsroom.fb.com/company-info/
5 Office for National Statistics: http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/index.html
6 KPMG https://assets.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf
7 Europa http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#431
8 GRBN http://grbn.org/trust/
9 Orange http://www.orange.com/en/content/download/25973/581975/version/2/file/Report+-+My+Data+Value+-+Orange+Future+of+Digital+Trust+-+FINAL.pdf
10 Andreas Koller: http://blog.andreaskoller.com/2014/02/data-is-people-in-disguise/ [7 February 2014]