

Privacy vs intelligence

Managing the tension in the era of big data

Privacy vs intelligence

Managing the tension in the era of big data

Introduction

As organisations collect increasing volumes of data on individuals, tensions are rising between privacy and intelligence. One of the most pressing issues facing senior management in the private, public and third sectors revolves around the appropriate use of the information they collect on individuals. There are huge potential benefits in the intelligent management of data, for both organisations and the public; however, there are also dangers in the potential violation of privacy and the misuse of data. Neither can be neglected, and CIOs and their senior colleagues face a crucial challenge in finding the right balance between the two.

It is not a new demand. For 20 years businesses have been building databases with increasing volumes of data to provide intelligence on their customers. The technology of customer relationship management systems has been developed to help businesses better target their customers, providing a more individual service and making a more individual sales pitch to anyone who has provided information about themselves. It has been used by the private sector to increase business and the public sector to deliver services more efficiently.

But the pressures are now intensifying with the development of 'big data'. This involves the collection of data from a wide range of sources into sets that are too large and complex for regular database management tools, in volumes of petabytes (1m gigabytes), even exabytes (1bn gigabytes). It makes it possible to measure human, business or scientific patterns in fine detail and can provide highly valuable insights to support the development of products and services. It can take in streams of data from the 'internet of things' – sources such as sensors and domestic appliances – and match these with information on individuals.

Big data holds the promise of massive benefits, but also creates new risks. As organisations collect more information on individuals the scope increases for its misuse or loss, and a growing number of people regard it as an intrusion on their privacy.

There is a tension between privacy and intelligence that cannot be fully resolved: people provide personal information in order to receive services; but in so doing they give up an element of their privacy and it is this data on which the intelligence is based. So organisations need to find the right balance in how they manage data, providing the flexibility for people to set their own boundaries on how much information they are ready to provide.



This requires confidence and trust-building mechanisms such as the disclosure of information about service providers and their information management values. A right to, and mechanism for, users to challenge a service provider's information handling practices is also needed.

No forward looking organisation can ignore the potential in big data, but it has to be set against a respect for privacy, and appreciate that if it steps over the line its reputation could suffer. This white paper considers the issues around the tension between privacy and intelligence and identifies some of the measures that can be taken by CIOs and their boardroom colleagues to manage the opportunities and risks effectively.

Personal information and big data

People have been providing their information to obtain services since well before the development of digital databases and it has been used to provide intelligence for sales and marketing when everything was done by mail or cold calling. The trend continued as people carried out more transactions online and organisations took the opportunity to ask questions about their backgrounds and preferences, and to share that data with others. As the use of the internet has increased, the commercial model for some companies has involved providing a service at low or no cost while making money from sharing the data, or at least helping other companies to target their messages.

A new dimension is emerging as increasing volumes of data are being collected without people being aware that it is happening. The growth of the 'internet of things' – in which data is collected from sources such as barcodes, sensors and domestic appliances – is making it possible to learn more about people's behaviour when they are hardly aware, if at all, of passing on data. Also, the widespread use of smartphones, especially any downloaded apps, provides a stream of data to the providers; and the GPS in phones provides plenty of location data. More organisations are taking parts of our personal data, often without us being fully aware. It's not just about spending habits, but the use of utilities, healthcare, travel and communications.

This often provides benefits to both sides and has an economic value, but it also creates new risks and raises the importance of the issue of consent to use information.

The benefits of big data

Organisations are constantly finding new ways to obtain benefits from personal data, and while their priority is to think about their own interests there are plenty of instances in which they are helping customers and contributing to the social good. They can build more detailed pictures of individuals, and combine data from different sources to evaluate trends, tailor their offerings and refine their business models. Some of the main benefits are as follows:



Targeted sales and marketing

Retailers use information on people's spending habits to offer them products they are likely to buy. The more data they can obtain on individuals the better they can relate it to broader trends and identify possible preferences. While this is based on maximising profits, it can benefit consumers when they become aware of products that they will appreciate.

Devices

Providing more personalised services – Private and public sector organisations use data from previous contacts to establish what could be the best way to solve a problem or offer a service to an individual. Information in their own databases is important, but can become more valuable when combined with the patterns established in the use of data from other sources.

Providing data to evaluate risk

The insurance industry has been at the forefront of using data from different sources – such as health records, scientific data, local crime records and environmental information – to evaluate the likelihood of potential customers claiming on a policy. Many types of business have to evaluate the risks around individuals and on a broad scale, and big data provides a valuable tool for doing so.

Efficiencies

Organisations can use digital data to save customers resubmitting their details, solve problems more quickly, prevent duplication, create more efficient ways of doing business duplication and develop better ways of delivering services. It can also be used in developing workflows and speeding up product development. The potential is immense.

Supporting strategic decisions

Data can be anonymised and collected to identify social and business trends and highlight needs and opportunities. For example, it can show where there are shortages of specific skills to support an industry or the broader economy, and where there is a need for investment. Or it can be used to provide insights into social problems – for instance, which factors are influencing crime or health problems in a specific area – and provide a case for the targeted spending of public money. It provides an evidence base for investment decisions.

Improving healthcare

Taking personal information into the realm of big data can provide valuable insights for research into health issues. The World Economic Forum (WEF), in its report *Unlocking the Value of Personal Data*¹, highlights the case of US insurer Kaiser Permanente identifying a link between expectant mothers using antidepressants and the risk of autism in children.



Anti-fraud

Organisations can use data to identify patterns in commercial transactions related to fraud and flag up any that may be illegal. The WEF points out Visa's work in this field, which it says has identified fraudulent transactions totalling US\$1.5 billion per year worldwide.

Increasing consumer access to information

Although there may be a hidden price in the supply of data, consumers enjoy a wide range of personal benefits from being able to use search engines, email, news sites and social networks without any monetary cost.

Risks of big data

Edith Ramirez, chair of the US Federal Trade Commission, outlines the rising concerns over the risks of big data in a speech on the issue². She said there are a number of privacy challenges to consumers, the full magnitude of which is yet to be seen. These have to be addressed before society can really reap the benefits.

Indiscriminate collection of data

If personal information is collected for no specific purpose, only on the off chance that it could be useful in future, it amounts to an intrusion on privacy, and threatens to undermine the quality of data as it increases the chances of it becoming out of date and inaccurate.

Undermining consumer choice

Another side to this is using data for a purpose other than that for which it was collected. People often give consent for their data to be used for the purpose at hand, without realising that it could be aggregated or passed on for secondary uses, some of which may not even have been considered when the data is collected.

This is being intensified by the collection of data from smartphones and 'smart' domestic appliances, and raises privacy and security implications that are not yet completely clear. It is further complicated by the fact that in the mobile ecosystem a number of bodies can have access to personal data – the carriers, apps providers, advertising networks and analytics companies that receive the information – and it may be impossible to identify who is responsible for any misuse.

Data breach

When personal information is stored in a large repository it provides a big temptation to criminals, inside and outside of an organisation. While most take security seriously, cyber criminals are always developing new ways to break down defences and it is inevitable that there will be major breaches in the future.



Behind the scenes profiling

Companies are using data in ways that could harm individuals' interests. This is most acute with data brokers, which collect and aggregate consumer data from a wide range of source to create detailed profiles of individuals, and whose success depends on having more and better data than their competitors. There is a danger that they will hold highly sensitive information – possibly on past financial transactions or health issues – that could cut consumers off from some services or force them to pay premium prices.

Data determinism

A possible by-product of big data analytics is that people may be judged not on concrete facts, but on inferences or correlations that may be unwarranted. In effect, they would be victims of algorithms that do not reflect their lives but exclude them from employment or admission to some institutions or deem them to be too high a risk for credit or insurance. This may be a valid approach that makes good business sense for an organisation, and many would tolerate a number of errors, but it is an injustice for the individual.

It also has to be said that human decision-making is not error-free, but when the imperfection is built into a system it intensifies the fault and reinforces the perception that an organisation is an impersonal entity that does not take people on their merits.

De-identification

Other sources have claimed there is a big weakness in the major line of defence against the misuse of data. Those in charge of data analytics have often placed emphasised that it was anonymised, using only details that cannot be used to identify individuals. Alternative approaches have been to use pseudonyms, key coding or data sharding (breaking up very large databases into smaller ones).

But it is not a panacea. There have been cases of anonymised databases being undone, such as when AOL published 20 million search queries to a website in 2006, and when Netflix released details of movie ratings from anonymised customers the same year. Researchers have been able to combine two sets of data to find 'pockets of uniqueness' that provide a data fingerprint for an identity³. This can be placed against data about people that is not anonymised to point to an individual.

The UK Information Commissioner's Office (ICO) has published guidance on anonymisation⁴. It says it can be impossible to assess the risk of re-identification with absolute certainty, and that there are many borderline cases that require careful judgement based on the circumstances.

A lot of anonymised data is already being used widely for research, and there is a danger that over time more of it will fall into the hands of people who will use such techniques for criminal or malicious purposes.



In addition, the WEF report on the value of personal data makes the point that the risks are being intensified by the growing amount of data that is provided passively, through phone and credit card purchases, web browsing and the location information on smartphones. Also, the growing amount of machine-to-machine transactions that do not involve a human, such as automatic bank transfers, generates more data about individuals.

Underlying all this are two further problems – one is that once consent has been given for personal data to be used it is virtually impossible to revoke. It is rare to see an organisation providing instructions for a member of the public on how to go back on a decision, and it would be difficult to find out who to contact to revoke consent. It is likely that many do not even have a process in place in the event that an individual contacts them.

The other is that people often have little idea of how their data will be used when they provide consent. While most are familiar with the requests to contact them with news of products and services, or to share with partners, there is seldom any indication as to how it can be used in different contexts. This is not helped by the lengthy terms and conditions, often written in impenetrable legal prose, to which people are asked to agree when signing up for services. It all adds an extra layer of obscurity to the public understanding of how their data could be used.

Public concerns

As people have enjoyed the benefits of the internet only a minority have expressed worries about how their data is being used; but there are signs that this is changing. The recent revelations about the activities of the US National Security Agency (NSA) in obtaining personal data has raised awareness of the risks and made more people cautious about providing information.

There is evidence of this in a survey conducted by internet security company AVG in August 2013⁵, soon after the NSA story broke. It involved nearly 5,000 people in eight countries, including the UK, from the online panel of research firm Qualtrics.

It showed that, while 72 per cent of respondents expected technology to become more helpful in the next five years, 69 per cent thought it would also become more intrusive. There was disquiet about providing personal information in return for a service: 88 per cent said they were not happy with it, and 36 per cent limited what they provide and would never give out some types of information. Respondents also expressed awareness, and caution, about data being collected from devices connected to the internet: 86 per cent said they were aware of the privacy issues and 79 per cent had at some time stopped the download of an application or program because it required personal information.



In addition, 46 per cent said they were becoming increasingly concerned over privacy in general, and 46 per cent were less trustful of companies holding their data in a secure manner. While the survey did not delve into specific fears, it unearthed a strong sense of unease.

Similar concerns emerged from a survey run by BCS through its website⁶ at the same time. A question about whether respondents were willing to reveal personal data in return for personalised messages from specific organisations produced a more defensive response with 78 per cent saying no. When asked if they would be inclined to provide more information if they knew who was using it and how, only 13 per cent agreed: 31 per cent said they would provide about the same, 36 per cent less and 20 per cent were not sure.

There was also plenty of caution about the use of smartphones, with only 2 per cent saying they automatically allowed them to use their location against 31 per cent saying never. Forty seven per cent answered 'sometimes' and it was not applicable to 20 per cent. As to whether they knew what information is used by apps on a smartphone, 55 per cent said yes.

Understanding of the UK Data Protection Act was also strong, with 24 per cent saying they understood it very well and 59 per cent quite well. However, the 18 per cent who did not have a good understanding was still a significant minority.

But the results suggest that respondents are not completely rigorous in their approach to consent. When asked if they read licence agreements before agreeing to terms and conditions 66 per cent said 'sometimes' and 16 per cent 'never'. Only 17 per cent indicated they were sufficiently concerned to read through every time.


A caveat should be attached to both surveys; most of the respondents to the BCS were members, who are likely to be better informed than most people about how their data is used, and the timing – immediately after the NSA revelations – is likely to have had an influence. But the results are strong enough to suggest that there is a growing awareness of the risks in passing on personal data.

Data Protection Act

The bedrock of protection for personal information in the UK is the Data Protection Act 1998⁷. It was passed for the UK to comply with the EU Data Protection Directive of 1995, and is based on eight principles.

The key points are:

- personal data should be obtained only for specified uses;
- it should not be used in any manner that is incompatible with purpose;

- 
- it should be accurate and up to date;
 - it should not be kept longer than necessary;
 - appropriate technical and organisational measures should be taken for its protection;
 - it should not be sent outside the European Economic Area unless the relevant country ensures adequate protection.

The Act predates the explosion of personal data that has come with widespread use of the internet and smartphones and there are differing views on whether it provides an effective level of protection.

Some observers see it as having worked well because it is based on principles rather than being overly prescriptive about processes. Most organisations have taken it seriously, especially large businesses and public sector bodies. While there have been violations reported by the ICO, they have often been down to mistakes or lack of understanding rather than a deliberate abuse, and there has been widespread compliance.

But others believe that sections 29 and 35 of the Act, which provide exemptions from the principles for legal proceedings, to prevent crime or support tax collection are used too widely, raising questions about the intent of some state bodies in obtaining data. Also, there are concerns that the ICO, which polices the Act, does not have the resources to ensure it is fully enforced. This tilts the balance of risk and reward towards the latter for companies with a cavalier attitude towards the regulations.

The changing landscape may soon test the limits of the Act. As more and more data is collected and analytics becomes more sophisticated there is likely to be a blurring over what constitutes personal information. If it becomes more difficult to protect anonymity within databases, there would be pressure to limit the scope of the data made available, and there could be room for argument over the appropriate technical measures to protect data. It is possible that compliance with the Data Protection Act will not ensure that organisations stay clear of any controversy around privacy.

There is a new EU Regulation on Data Protection in the pipeline. This includes a right of people to transfer their personal data from one provider to another more easily, and to be 'forgotten', demanding that their data is deleted if there are no legitimate grounds for its retention. There are also plans for a new directive that will apply general data protection principles and rules for police and judicial cooperation in criminal matters, both domestically and across the borders of member states.

But the reaction has been mixed, and the ICO has expressed concerns that the regulation as it stands is over-prescriptive, may encourage a 'tick box' approach to data protection, and fails to recognise the widespread international transfer of personal data. Some observers fear the resulting legislation may be weaker than the existing rules.



Compliance with legislation may not be sufficient to satisfy the public and protect an organisation's reputation when it comes to finding the right balance between privacy and intelligence. Businesses, public authorities and third sector organisations all need to develop strategies for ensuring that they can make productive use of personal data while providing the privacy that is expected.

Strategies

There has been a long standing tension between how organisations extract benefits from personal data and the individual's right to privacy. We are now at a point where the growing sophistication of analytics and the emergence of big data are increasing the potential rewards, while public concerns about privacy are also growing. There is no prospect of fully resolving this tension - one cannot be fully reconciled with the other - but it can be managed to ensure that organisations stay on the right side of the law and of public opinion.

This will rely heavily on the appropriate models for consent. The practice of asking for blanket consent to use data - although it is often separated into one question for the organisation itself and another for its 'partners' - could soon look inadequate to many consumers. There is a need for a more detailed approach with more options, but which does not confuse the consumer and has a clear, user-friendly interface. People have to be able to understand what types of consent they are being asked to provide.

It is unlikely that a highly prescriptive approach will work in the long term. The uses of personal data are evolving over time, and any measures that are set in stone are likely to deny an organisation the opportunities that may emerge from new methods and technologies, and begin to fall short on providing sufficient protection for the data. Also, the diversity of organisations and their different business models make it impossible to take a 'one size fits all' approach. It is better to use a set of principles for privacy protection as the basis for action, providing the flexibility to change as needed.

The US Federal Trade Commission (FTC) has provided advice in the shape of three principles on which it urges organisations to base their approaches: privacy by design, transparency and simplified choice.

Privacy by design involves building in privacy as products and services are being developed, which requires risk assessments on the personal data that will be used. It takes in whether the data will be used in a way that could harm individuals, whether the security measures are sufficient and whether the risks can be mitigated or avoided.

An implementation plan for privacy by design is available from the ICO's website⁸. Also, a privacy impact assessment (PIA) (which is outlined near the end of this section) would be an important first step in providing privacy



by design.

Transparency involves organisations making it clear exactly how they use data. Although the FTC is not prescriptive on this score, it is feasible that private and public sector bodies could provide pages on their websites, linked to anywhere that they ask people to provide data, outlining their practices and the purposes for which it may be used, and telling people of any other organisations to which it may be passed.

Simplified choice is closely related to the consent issue, and would make it easier for people to decide if, when and how their data can be used. It needs a workable approach to respecting the 'do not track' options on internet browsers so they can opt out of tracking by websites they visit, analytics services, advertising networks and social platforms.

There is a debate over the number of options people should be given in asking to provide their consent. One of the possibilities for simplifying choice is to limit it to three when submitting information for a transaction:

- that they can complete the transaction without their data being stored;
- they will agree for it to be stored by only for use by the organisation with which they are dealing;
- they agree for it to be more widely used.

Some observers believe there could be a need for more options that are defined in a different way, especially as data is being collected from more sources, but that the number should be kept relatively small. If this becomes the case it would require a debate about the appropriate definitions, and it should all be explained in layman's language, with clear explanations of the consent people are providing.

There are other principles that are important:

Think about context

One of the principles highlighted by the WEF⁹ is the importance of context, both in terms of how data has been collected and how it will be used. Companies could commit themselves to only using data that is submitted freely, such as through filling in surveys, rather than passively through a smartphone or web browser. People could provide permission for their data to be used within a company to fulfil a customer order, but not necessarily for analytics; or they could agree to it being used for research with an obvious social value rather than a commercial purpose; or they could be asked for consent on a case-by-case basis.

There may be some purposes for which it is appropriate to use data without specific consent, such as fulfilling a service, internal operations, fraud prevention and legal compliance. But others should require contacting people to ensure they are happy for it to be used.



This is a complex issue that goes into grey areas and is partly at odds with the principle of simplifying choice; it's not so simple for an individual to choose from an array of possibilities linked to different purposes for which their data could be used. It would also increase the administrative burden on organisations seeking consent. But it has the potential to change according to circumstances and would provide the flexibility needed over time.

Make it easy to revoke consent

This would be a major step for any organisation, but it should be possible to set up a process for removing an individual's details from their databases, and from any of those being shared with other organisations. It should also be possible to provide a clearly visible link on a company website, and in any emails sent to members of the public, to a contact to check on the consent arrangements and make any changes that are desired.

It would be difficult, if the data had been shared with numerous organisations, to ensure that every one of them removes it from their systems. But it would be a step in the right direction to include the obligation to remove data on request in sharing agreements.

While this would probably be seen as a burden early on, as public attitudes change it would be a major step in building long term trust and enhancing an organisation's reputation.

Regularly refresh data and consent

There is an opportunity to build trust by returning to the individuals on a regular basis – once a year would be feasible – to check that the data is up-to-date and that they remain happy for it to be used for specific purposes. This could be aligned with the need to consider context, making it more specific to people how their data is being used as new uses are developed. Again it does create an administrative burden, but it would assure people of the organisation's good intent and do much to preserve the quality of the data.

Provide people with easy access to their data

Most organisations provide online access to basic account details for customers or members, with requests to update any changes; but there is also scope to let them see what data is held about any transactions or behaviour, and anything on them held by the organisation which is supplied by third parties. This has the potential to cause some disquiet, but over time it would also help to build the relationship of trust.

Analytics companies

Many organisations will not have the capability to run big data operations themselves, but will see the value in providing data to an analytics company to provide intelligence. The Cutter Consortium consultancy has listed a number of questions¹⁰ to ask before taking up such a service:

- Is the company combining your data with that from other sources?
- Will it use your data for analytics for other customers?
- How has it handled the anonymisation of the data?
- How does it collect the publicly available data it uses?
- Have you discussed the plans with your information security, privacy or compliance specialists?

There should be clear answers to these questions that are appropriate to the nature of the data before going ahead.

Ensure the proper security measures are in place

It is crucial to maintain high standards of information security. The appropriate technology and processes should be put in place, monitored and regularly reviewed.

Educate staff

Make employees who are handling personal data aware of its sensitive nature, the appropriate uses, the issue of consent and that they have responsibilities towards the people who have supplied it. They should be aware of best practice in data handling and of the limits on how specific data sets can be used.

Take responsibility at the top of the organisation

While the day-by-day scrutiny of how the principles are being applied has to be delegated, CIOs need to stay in regular touch to be aware of any pressures that are emerging, possible transgressions and be ready to change processes if needed. They also need to keep the board fully apprised of any developments.

Build a new relationship between IT and business

CIOs, and possibly heads of IT, are going to have the best grasp of the issues around privacy and intelligence. Traditionally they have been tasked with supporting the business priorities of the organisation, but in this case they should take a more proactive approach, making it clear to business departments what they can and cannot do with personal data. They should be setting the rules within which other teams will work. This may cause some friction, but it would give an organisation a better chance of avoiding any controversy over its use of data.

Voluntarily adopt a set of principles

There are no widely agreed principles for the use of big data in place so far, but if an organisation creates a set of principles and makes a clear statement of its position it will take another step towards winning public trust. It should also be ready to revise the principles as the use big data evolves.

Comply with the data sharing code of practice

This is a statutory code, available on the ICO's website¹¹, covering the legal



aspects of data sharing, the factors to consider, conditions for processing, transparency, governance and the rights of individuals. There is also a list of what to avoid – which includes sharing data when it is not necessary and misleading people about whether their information will be shared – and a checklist for compliance with the code.

Follow the ICO's advice

The ICO provides advice on its website on the conditions for processing personal data as they relate to the Data Protection Act¹². It covers the conditions around legitimate interests, sensitive personal data and 'necessary' processing, and the meaning of consent. It should be regarded as a prerequisite for legal compliance.

Privacy impact assessment (PIA)

The ICO provides guidance on PIAs in the form of a handbook¹³, although it makes the point that not all of the information will be relevant to any project.

A PIA should be carried out before a project is up and running, and go beyond compliance with existing privacy laws. It involves an initial assessment that identifies the stakeholders and looks at the privacy risks, followed by a full scale assessment that analyses the risks, consults with the stakeholders and produces solutions. There can also be small scale PIAs for specific elements of a project, and there are compliance checks for privacy laws and data protection.

The effects of any action taken should be reviewed as the project goes on, and if any new elements are added the organisation should think seriously about a new PIA.

Ensure that anonymisation is as effective as possible

While the ICO acknowledges that it may be possible to re-identify individuals from anonymised data, its report on anonymisation provides guidance on how to meet the requirements of the Data Protection Act.

This includes the use of a 'motivated intruder' test, which considers whether a competent intruder would be able to identify an individual from anonymised data. It assumes that they would have access to the internet and public sources of information, but no hacking skills or specialist equipment, and would not have to resort to burglary. Techniques include web searches to see if a date of birth and postcode can point to an identity, comparing press reports with crime map data, and using social networks to link a user's profile to anonymised data.

Other factors to take into account include the possibility of a potential intruder having prior knowledge of individuals, information that is publicly available on groups of people, and the distinction between recorded information, established fact and personal knowledge.



Skills

Managing the tension between privacy and intelligence demands a new element in the skillsets of CIOs and their teams. There is a case for developing the role of full time privacy professionals, but realistically most organisations will require existing staff to extend their own skills.

There are four elements that stand out in the strategies as areas in which new skills need to be developed: refreshing data and consent; the appreciation of context in the use of information; carrying out privacy impact assessments; and developing the mechanisms to simplify consent.

The first of these is straightforward, relies on a rigorous approach to standard processes, and could easily be delegated within an organisation.

The second and third require a deeper appreciation of the benefits and risks in using personal information, the trade-offs between the two and how they can be affected by circumstances. It needs people who can appreciate the nuances in a particular context and the ability to make sound value judgements. This places it firmly in the hands of CIOs and their more senior staff, who need to stay abreast of how the various applications of big data affect privacy, any new risks that emerge and the development of best practice. This has to be incorporated into all of their thinking about the use of the data, with a willingness to forego the benefits when the risks are too high.

They also have a role in the fourth in simplifying the consent mechanisms, and need to work closely with web designers and data architects to ensure that they are user-friendly and align efficiently with the organisation's databases and workflows. It requires an appreciation of what the public can easily understand and how it can be related to the different contexts in which their information is used.

All this goes beyond the traditional need to comply with data protection laws, requiring a deeper understanding of where privacy fits within the use of big data. This will be a key element of the role of the CIO in the future.

Personal data stores

Looking to the long term, there is a potentially valuable option in the form of personal data stores. They have begun to work on a small scale in a few countries, and offer an alternative approach to the management of data.

An individual lodges all of their data with the provider, which is independent of any of the organisations that want to use it. It is then made available on request, and with the individual's consent, on a one time basis for a specific purpose. People can ensure that the information in the personal data store is accurate and up to date, and retain a strong sense of control that should give them more trust in the organisation using the data.



It will take time to establish if and how this could be used in analytics. People may be ready to make their data available for a cause of which they approve, although it is likely that it would restrict the scope for using it for commercial purposes.

But it would provide a method of dealing with the more straightforward uses of personal information, in which people agree for an organisation to process their data for routine purposes or to be kept informed of what an organisation can offer them, and would help to build a climate of trust.

Personal data stores still have a low public profile and are not widely used; but this can change if more people become active in managing their personal information. The question is if and when enough people will want to use them to make them a compelling choice for managing the privacy issue. CIOs will be watching their development closely over the next few years.

The long term

There is scope for the development of a set of standards, managed by an independent professional authority, to which organisations could refer in setting up a policy to deal with the pressures on privacy in the age of big data. However, realistically this would take years to emerge, and would need examples of existing best practice and the input of professionals experienced in the field to give it credibility.

There is a role for professional organisations such as our own in developing and promoting the standards for the ethical use of personal data. It is possible to support the education and training of CIOs, IT teams and employees who handle data in how to do so while respecting privacy, aimed at ensuring that best practice becomes the norm.

We could also contribute to consumer education, so people become aware of how their data could be used and take more responsibility for protecting their privacy, and to the technical development of clear user interfaces for providing or withholding consent to use and share personal information.

But more immediately, organisations that are keen to deal with the issue could set the pace by developing their own standards, basing their processes on these and promoting their efforts to their counterparts and the public. Over time, the people who use their services will decide what works best, and those that win public trust will take on a higher profile and provide the examples of best practice. This would be good for the public, and for those organisations that show they are getting to grips with the tension between privacy and intelligence.

Endnotes

- ¹ *Unlocking the Value of Personal Data: From Collection to Usage*
World Economic Forum, February 2013. Prepared in collaboration with The Boston Consulting Group.
http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf
- ² *The Privacy Challenges of Big Data: A View from the Lifeguard's Chair*
Keynote Address by FTC Chairwoman Edith Ramirez, Technology Policy Institute Aspen Forum, 19 August 2013
www.ftc.gov/speeches/ramirez/130819bigdataaspen.pdf
- ³ *Broken promises of privacy: Responding to the surprising failure of anonymization*
Paul Ohm – UCLA Law Review 1701 – 2010
www.uclalawreview.org/pdf/57-6-3.pdf
- ⁴ *Anonymisation: managing data protection risk code of practice*
ICO, November 2012
www.ico.org.uk/news/latest_news/2012/~/_media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx
- ⁵ *Confusion and intrusion: consumer trust eroded as multi-device culture takes hold*
AVG, 9 September 2013
<http://mediacenter.avg.com/content/mediacenter/en/news/confusion-and-intrusion>
- ⁶ *Protecting Your Privacy Poll*
BCS, The Chartered Institute for IT, August 2013
- ⁷ *Data Protection Act 1998*
www.legislation.gov.uk/ukpga/1998/29/contents
- ⁸ *Privacy by Design Report Recommendations: ICO Implementation Plan 2009*
www.ico.org.uk/for_organisations/data_protection/topic_guides/~/_media/documents/pdb_report_html/PBD_ICO_IMPLEMENTATION_PLAN.ashx
- ⁹ See report in endnote 1, and *Rethinking Personal Data: Strengthening Trust*
World Economic Forum, May 2012. Prepared in collaboration with The Boston Consulting Group.
http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf
- ¹⁰ *Big Data: Part 1 – New Privacy Concerns*
Cutter Consortium, Data Insight & Social BI Vol. 13 No. 1
www.cutter.com/content-and-analysis/resource-centers/business-intelligence/sample-our-research/biau1301.html
- ¹¹ *Data sharing code of practice*
ICO, 2011
www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing
- ¹² *Data Protection*
ICO
www.ico.org.uk/for_organisations/data_protection
- ¹³ *PIA Handbook*
ICO
www.ico.org.uk/pia_handbook_html_v2/html/0-advice.html



About the author

Mark Say is a business writer who has more than a decade of experience in covering information management and technology. He has been editor of *Government Computing* and *TechRadarPro*, written research papers for Kable and Ctrl-Shift, and worked with BCS, The Chartered Institute for IT, on the relationship between IT and business issues.

About BCS

We help global enterprise align its IT resource with strategic business goals. We work with organisations to develop people, forge culture and create IT capabilities fit to not only lead business change but to meet companywide objectives and deliver competitive advantage.

IT has been gaining momentum within global business for decades and we've been there from the beginning, nurturing talent and shaping the profession into the powerhouse that's now driving our digital world. Today organisations partner with us to exploit our unique insight and independent experience as we continue to set the standards of performance and professionalism in the industry.

BCS The Chartered Institute for IT
First Floor Block D North Star House North Star Avenue Swindon SN2 1FA
T +44 (0) 1793 417 655 enterprise.bcs.org

© BCS, The Chartered Institute for IT is the business name of The British Computer Society (Registered charity no. 292786) 2013

If you require this document in accessible format please call +44 (0) 1793 417 600