Privacy backlash — freedom campaigners' fantasy or imminent peril for business?

Is a consumer backlash against organisations that collect and use personal data possible? If so, what is likely to cause it, and what could be the consequences for businesses? In this article, Peter Carey, author of* 'Data Protection – a practical guide to UK and EU law'*, Consultant to Charles Russell, and Visiting Fellow at the London School of Economics, looks at what might happen, and at what steps companies could take to strengthen their positions

There can be little doubt that privacy concerns are on the rise. A growing number of individuals seem to be aware that basic freedoms are being impacted. If they don't feel it themselves, they read about it in newspapers or see it on television news programmes, talk shows or documentaries. Dinner table conversation has been extended from house prices and the state of the job market to the area of personal data privacy. Whether the conversation is about junk mail, spam email, unsolicited text messages, phone hacking or loss of data sticks on trains, there can be little doubt that privacy has gone mainstream.

An obvious question arises: where do we go from here? Will there be a peaking of interest, followed by a slow and gentle falling away of consumer attention, coupled with a resigned acceptance that we now live in a post privacy world? Will there be a non-privacy-based catastrophic event which immediately consumes headlines and diverts attention away from privacy issues, never to return to the current level of vigorous interest? Or will consumer concern continue to rise unabated?

In his book, *The Tipping Point*, Malcolm Gladwell describes the rare but volcanic change that can occur when human attention suddenly focuses on a specific issue or product, potentially causing dramatic effects for companies or whole sectors. Could a tipping point be imminent in the arena of data privacy?

If we can agree that a tipping point is at least possible, then it is arguably worthwhile for organisations to consider how they might arrange themselves to prepare for, or even benefit from, the consequences of such an event. The question as to how much time and resources should be devoted to the project essentially comes down to a simple cost/benefit analysis. How likely is the event? How much devastation to company profits would be likely to result? By what factor might company profits increase where appropriate measures had been taken to reap the rewards that might result from such measures?

The remainder of this article considers what might cause a tipping point, what might be its consequences and what steps businesses could take in order to benefit from the backlash.

What might cause the backlash?

The tipping point for a consumer privacy backlash could of course be almost anything, and attempting to predict the future is a fool's errand. Malcolm Gladwell likens the spread of causal factors that culminate in tipping points to epidemics. Knowing only what we now know, we can perhaps extrapolate as to what might cause the existing level of public concern about consumer privacy to expand into an epidemic. The following seem to be likely contenders:

Increasing quantities of marketing emails (including spam) — It should be obvious that the quantity of marketing emails we receive, both at work and in our personal lives, is increasing. Individuals can be justifiably exasperated by the use of their email address for (what they perceive to be) unauthorised purposes by companies with whom they deal or companies with whom they do not. Whilst it is true that many spam emails are sent to email addresses that are randomly generated by computers without human intervention, the recipient of such an email may be no less infuriated, even where he or she is aware of that distinction.

Spam, as well as legitimate marketing emails, clogs inboxes and takes time to delete. Some carry viruses that have potential to cause damage. Many contain language or images that people regard as offensive. Some organisations that send marketing emails make the mistake of including the email addresses of all recipients in the 'TO' field (as opposed to the 'BCC' field), causing anger and risk of greater future email traffic to inboxes. Marketing text messages can be even more irritating to citizens than spam emails, due both to the 'personal' nature of the medium as well as the reduced ability to discover the

sender (for the purpose of requesting cessation).

Of course, if there is to be a 'final straw' regarding spam quantum resulting in unabated anger amongst individual recipients, it is unlikely to happen to lots of people at the same moment. However, on Mr Gladwell's analysis, multiple simultaneous concern is not necessary in order for a tipping point to be generated — just a few key people expressing substantial upset could be enough to tip the balance of consumer sentiment, leading to massive consequential action.

Extensive and invasive identity checks — Whether as a result of legislative requirements or otherwise, some organisations demand reams of information before dealing with, or commencing a communication with, an individual. Further, face-to-face transactions are increasingly rare, meaning that proof of identification must be supplied at arm's length. To take banks as one example, anti-money laundering rules (which require extensive ID checks) perform a vital public interest function, but such rules annoy people, regardless of their efficacy. My mother recently attempted to open a savings account at a well-known supermarket bank. After sending the documentation that was requested, she was informed that she did "not exist" at her address. She has lived there since 1985.

A further related issue may be the seemingly arbitrary nature of distinctions that are made by companies seeking to establish identity – my assistant is unable to request an upgraded data package for my mobile phone because, having a female voice, she is obviously not me, whereas any male to whom I had supplied my password would be successful.

Increasing data collection (existing relationship) — Related to the point above, organisations in both the public and private sectors are demanding ever greater quantities of personal information as part of the process of initiating dealings with individuals. Further, even where there is an established relationship, additional information is regularly demanded from individuals upon specific events, such as a request for a different service or an upgrade. Companies track behaviours in a seemingly ever more obsessive fashion – from supermarkets to online movie providers – every new behaviour being added to the individual's profile and stored for possible future use.

Increasing data collection (no existing relationship) — Headlines regularly feature stories of the collection of personal information on citizens in circumstances where there is no obviously proximate relationship between the data collector and the individual. Google, frequently criticised for its apparent disregard for individuals' privacy, has been accused of collecting Wi-Fi data unlawfully, tracking mobile phone users' geographical locations, serving people with behaviour-specific advertising and providing differing search results based on users' prior online activities. Employees and contractors of News International have admitted hacking into citizens' mobile phones to obtain the content of messages sent to, and received by, both celebrities and victims of crime. Even as you read this, citizens' apathy towards what many perceive to be a corporate land grab of personal data is being tested as never before.

Technological devices — Increasingly, technological devices transmit information about individuals to one or more recipients. Examples include cookies, which make data available on internet usage (including websites visited and purchasing habits), and the transmission of geographical location data to mobile networks, app suppliers and other commercial entities. The implications and effects of this are felt initially by individuals when they receive behaviour-related and location specific advertising messages. Other implications, which include the virtual global tracking and profiling of individuals, have yet to be felt by enough people to generate either fear or outrage. Many people are unconcerned about this relatively new phenomenon, but a growing minority are increasingly vocal with their objections. They are concerned just as much by the uses of their data of which they are not aware as with the uses that are more obvious.

Data sharing — With the proliferation of relationships between private sector organisations, and ever more initiatives towards 'joined up' government, the types and number of transmissions of datasets between organisations have dramatically increased. It is reasonable to expect the continuation of this trend. Individuals can often be surprised at the number of organisations, particularly those with whom they believe they have no existing relationship, that have access to their data. Some are fearful of supplying data to organisations for the very reason that they do not know where it will end up, and they feel that they have no control over whether (and to whom) onward transfers take place.

Media attention — We are all aware that the media is a powerful instigator of public opinion. As privacy and data protection issues continue to be of interest to the public, so too will the media pages and airtime reflect that increase. The reverse is also true. Although they take a somewhat different approach in the tone of their articles, it is interesting to note that both the quality press and the tabloid press are keen to publish data privacy pieces. So too with the broadcast media. From phone and website hacking to NHS Trusts losing data sticks containing sensitive medical records, to laptops being stolen from cars, media attention will continue to feature data privacy stories until something else becomes more fashionable. Could a tipping point be reached before the arrival of the next media darling?

Failure to respect preferences — Individuals complain that their requests as to how their personal data should be used are being ignored. In some cases this is because they believe that they have opted-out of receiving marketing communications, but receive them nevertheless. In other cases they request deletion of information about themselves without success. Further, citizens are coming to realise that information stored about them online, or in the cloud, may be very difficult to erase. It appears, for example, that Facebook data are essentially there forever. Take care if you are concerned what future social historians may dig up about your life. The European Commission is currently working on a change to European data protection law which may result in the introduction of a 'right to be forgotten', allowing EU citizens to request and enforce the deletion of their

(Continued on page 8)

(Continued from page 7)
information by online businesses. But the new right, if it is enacted, will not come into force for several years, and there will be legal arguments over whether it would apply to non-EU businesses such as Facebook, Google and Twitter. Will enough people grow sufficiently angry about permanent storage and accessibility of their information without apparent legal redress that a tipping point will be reached?

Poor data handling practices — Some consumers have been, and will continue to be, personally affected by inadequate security measures at organisations that process their personal information. The effect of security breaches on individuals range from mere annoyance, through inconvenience, to economic loss due to fraud or identity theft. In extreme cases, physical injury or death might be the consequence of poor data handling practices — one can imagine a scenario where vital medical information is either misplaced or ascribed to the wrong patient in a hospital ward or operating theatre.

Potentially hostile online environment — Whilst researching this article, it became clear that some people, particularly the older generation, perceive the internet to be a 'Big Brother' type environment. Many are fearful of using online stores for their purchases due to their perception that they are 'being watched'. They are also uncertain where their information might end up or how it might be used against their interests. They prefer to shop on the High Street despite acknowledging that they are paying slightly higher prices to do so. There is also a perception that the complex algorithms that run various aspects of websites work against individuals by supplying differing prices to different individuals depending on their profiles, and being able to very rapidly change prices in response to particular events, e.g. the sudden fashionableness of an item. Whether these fears have a grounding in reality may be irrelevant.

The nature of the backlash

Although there are multiple potential causative elements for a tipping point to arise (some of which will be obscured from our current view and/or may not yet exist), it may be somewhat easier for us to predict the outcome of the tipping point than to forecast the basis for its inception. Although, according to Gladwell, tipping points can be traced largely to *one substantive cause*, there are likely to be *several outcomes* of the tipping point. Again based only on our experience, perhaps we could foresee that one or more of the following is a possible result of the epidemic outbreak:

Using the door — Consumers, or at least a portion of them, may choose simply not to deal with companies that they perceive to be mistreating their information. Whilst it is true that inertia represents a powerful reason for the majority of the population to stick with existing suppliers (even when they express an intention to change), there is some evidence that an increasing number of people are choosing to vote with their feet where they perceive the issue to be a serious one. Some estimates put the number of people quitting Sony (following the company's several high profile data security breaches, and consequent intermittent closure of its gaming network, in early 2011) in favour of other gaming providers as high as 15% of the customer base. Facebook is reported to have lost hundreds of thousands of customers in recent months due to privacy concerns.

Requiring full disclosure prior to dealing — Consumers are already becoming more cautious about entering into commercial relations with organisations, particularly where they are not provided with relevant, appropriate and believable assurances regarding the use of their data. Respect for customer data could even become as important to individuals as price and quality of service/ product when they are selecting their provider. Perhaps a grading system will be established by a consumer or pressure group, with each retailer being awarded a number of points for their data handling practices. Could we can imagine a headline such as 'X Bank has been downgraded from AAA to AA following the recent data breach'?

Requesting copies of stored information — The legal right for individuals to gain access to copies of their data held by organisations has existed in EU law for many years. Evidence from regulators suggests that the number of individuals making access requests increases year on year, albeit at a fairly slow rate. Part of the reason for the slow growth in the number of requests may be the limited pace of permeation of knowledge of the right into citizens' awareness. A privacy backlash could conceivably result in the knowledge about the right 'going viral', coupled with a dramatic spike in the number of requests being made, particularly to any offending organisations. Each access request can take many hours to complete and can cost hundreds, or in rare cases thousands, of pounds to handle. Even though many medium and large organisations have full time Data Protection Officers, part of whose job is to deal with access requests, many companies would be unprepared for a sudden increase in requests.

Reverting to the High Street — A privacy backlash could feature an exodus of those who are currently content to shop online, back to the High Street. The fortunes of companies like Waterstones, which is pervasive in the High Street and which was slow to establish an online presence, could turn around in such a scenario.

Choosing EU-based businesses — In many cases the threat of damage to EU-based businesses derives from the poor data handling practices of US-based businesses, where there is no universally applicable data protection law. Unfortunately most EU-based consumers are unlikely to draw sensible conclusions from this distinction. But if some consumers do indeed perceive the threat to come mostly from the US, they may develop a preference for EU-based websites, or even shun US websites altogether. Thus, HMV may be a preferred source of online DVD purchases to Amazon, since HMV is a UK company.

How organisations can prepare

Given that a privacy epidemic is a real possibility, it is likely to be worth spending some time considering what actions could be taken to mitigate against any potential loss that might arise from it. Organisations should realise that they may suffer from the fallout of a tipping point without having contributed to its cause. Several of the following suggested actions may have the effect of streamlining internal systems, thereby saving costs. Some may, even before any possible epidemic builds, result in increased sales and profitability due to the increasing propensity of customers to choose organisations that offer privacy guarantees.

"Given that a privacy epidemic is a real possibility, it is likely to be worth spending some time considering what actions could be taken to mitigate against any potential loss that might arise from it. Organisations should realise that they may suffer from the fallout of a tipping point without having contributed to its cause."

Pare down data collection — Given the possible concern amongst citizens that organisations hold too much information on them, and the fact that many organisations do collect more data than they actually need for the contemplated purpose of the collection (on the basis that the additional information may, one day, be useful for something), it may be sensible to reduce the quantity of information that is collected to only that which is strictly necessary for the contemplated immediate purpose of the collection. Such a move also benefits from reduced storage (including back-up and archiving) costs.

Remove 'optional' fields on forms — This relates to the above point. The practice of requesting non-compulsory information is rife. We see it in both online and offline forms, usually delineated by the familiar asterisk (or lack of it). Consideration should be given as to whether there is really a benefit to organisations in requesting such data.

Increase the authority of the data privacy lead — Whether it's the Data Protection Officer, Privacy Officer, Compliance Officer, In-House Lawyer, Information Officer or other staff member, someone in the organisation should have overall responsibility for ensuring compliance with internal data privacy procedures. In too many cases the person ascribed this responsibility, who may themselves lead a team of compliance personnel, is not given enough power to instigate and enforce relevant measures. The UK Information Commissioner has recommended that data protection compliance personnel within organisations should be given enough authority to ensure that their instructions regarding data protection measures be carried out by all staff members. Policies and procedures developed by compliance personnal should carry significant weight within the organisation, with dismissal of staff members being a possible sanction for their breach.

Publicise data handling excellence — Although in its infancy, the practice of publicising data privacy procedures within advertising messages is set to grow exponentially. It is reasonable to expect an increasing percentage of consumers to make purchasing decisions which are at least partially based in data privacy considerations. Thus we are set to see hitherto 'hidden' (for example in a company's online Privacy Policy) data privacy statements bursting into the mainstream advertising space. Such statements might include "we never send unwanted marketing materials to our customers", and "we never send our customers' contact details to third parties", and "your personal information is secure with us — we use the highest quality information security techniques". Companies should seek to become known as the leading privacy friendly company in their field. Of course, companies will need to ensure that they actually do what they say they do — an organisation that promotes its excellent data handling practices will be punished by consumers where the reality is palpably otherwise.

Promote internal data handling excellence — The making of promises to customers about how their data will be handled should be backed up by appropriate attention to the enforcement of relevant practices and procedures within the organisation. Many companies, some of which have been on the receiving end of enforcement action by the data protection regulator, already acknowledge the importance of this approach by instigating staff training procedures on well thought-out internal codes of practice. Other companies take matters to, perhaps justifiable, extremes — Barclays, for example, has taken extraordinary measures to force privacy messages into its employees' consciousness, including the display of the notice "Privacy Matters" above each urinal in the male staff toilets. Staff should be consulted on data protection issues and should be asked for their suggestions on what can be done within the organisation to improve data security. A useful question might be: "suppose we were storing and using information on your 10-year old daughter—what should we do differently?" Special attention should be paid to the types of data (if any) that staff should be allowed to take away from the premises (for example on laptops and USB sticks).

Initiate easy customer preference selection — In appropriate circumstances, individuals should be allowed to access their account online and to easily and quickly adjust their own privacy settings. This should give individuals a feeling of control over their relationship with the organisation.

(Continued on page 10)

(Continued from page 9)

Provide obvious and clear opt-in and opt-out clauses — Although some organisations have clear opt-in and opt-out clauses, with appropriate back-office procedures to respect those choices, many do not. Some organisations have poorly, or negligently, drafted clauses; others use deliberately misleading clauses. Clauses should be clear (no double negatives) and unambiguous, as well as being prominent enough (especially in the case of opt-out provisions) to be obviously noticed. Brave organisations may choose to set all consent provisions to opt-in rather than opt-out. Although this is not a legal requirement (except in some limited cases), it may have the effect of engendering the trust of customers.

Set up or improve SAR procedures — Organisations should prepare for a potential increase in the number of requests they receive from individuals for access to the information held on them by the organisation ('subject access requests'). Consideration should be given to establishing a new (or streamlining an exisiting) procedure to ensure that requests are handled within the 40-day time limit specified in the Data Protection Act.

Contact individuals upon data acquisition — Information on individuals is always obtained either from the individual his or her self, or from a third party individual or organisation. In the latter case it is rare for the acquiring business to inform the relevant individual of the data acquisition, despite this being a legal requirement in most cases. Whilst potentially expensive (especially where post is required due to not having collected electronic contact details), this could have the effect of reassuring individuals as to which organisations hold their data.

Set the default to maximum privacy — The default settings of customer accounts are often set at the position where they will be of most value to the commercial entity. In a reversal of this process, companies could set the default for customers at maximum privacy, with the consumer being able to revise the settings if they wish to do so.

Staff education — The UK Information Commisisoner has stated that all staff members who use personal data in their jobs must be given training in data protection issues, with senior staff members (e.g. Heads of Department, Company Secretaries and other decision makers) receiving more in-depth training. Compliance personnel, who themselves should be highly trained, should be responsible for rolling out such training. Regular updates/reminders should be put in place to effectively invest in the organisation's privacy future.

Consumer education — Many of the fears that consumers have around using technology stem from a lack of understanding about the reality of e-commerce. Can businesses afford to let the ignorance and fear pervade further, or should they instigate measures to redress the misperceptions?

Conclusion

According to Gladwell, tipping points can happen very suddenly, and are rarely proportionate responses to their causes. "We need to prepare ourselves for the possibility that sometimes big changes follow from small events, and that sometimes these changes can happen very quickly," he says.

It could be that the current heightened consumer interest in privacy will itself prevent a tipping point from arising. This will occur where companies recognise the problem and act accordingly.

There is already some evidence of organisations taking action based on the privacy concerns of their customers. Following the phone hacking scandal in June 2011, the Telecoms Group O2 said, "We share the concerns of customers and employees about these quite shocking claims." Sainsburys went one stage further by withdrawing its association with the *News of the World*: "Due to the rising concerns of our customers we are suspending any advertising in the NOTW until the outcome of the investigation." Ford, Vauxhall, Virgin Holidays and Boots followed suit. The newspaper became commercially unviable, and closed in July 2011. Its parent company News International lost its ability to bid for the satellite broadcaster BSkyB. On the other side of the Atlantic, in an attempt to head off the exodus of customers from Facebook, the company announced in August 2011 that it was bolstering its privacy procedures — including the cessation of photo tagging without consent — and making its privacy settings more transparent and easy to use.

Will the corporate world's response to increasing privacy concerns come quickly enough to head off any potential epidemic, or will the few companies that adopt radical new privacy -friendly procedures reap all the rewards?

Peter Carey
Data Protection Consultant
peter.carey@dataprotectionlaw.com