Leveson Submission: Big Brother Watch

Much of the evidence already presented to the enquiry has focused on the illegal and deceptive methods used by journalists to acquire information. Across phone hacking, blagging or entrapment the common element is that journalists – or those acting on their instructions – were consciously breaking both the law and the PCC Code.

There is a broader issue not touched upon, which in future I expect will become a much greater problem, and where current legal regulation is lax at best. Simply, the risk of those with access to databases of personal information - whether in the public or private sector – selling on or leaking information to which they have access to the media, or of that information being lost and ending up in the media's possession.

The current legal protection, the Data Protection Act, is weak and the national regulatory body, the Information Commissioners Office, is woefully bereft of real enforcement powers. Irrespective of who the perpetrator is or their motivations, there is a clear need to consider how the media obtain information, and may do so in the future, and the privacy implications for the current data protection regime.

Big Brother Watch is a privacy and civil liberties campaign group, and in recent months we have undertaken unprecedented research on the risks to personal privacy posed by the inability of public sector organisations to maintain the security and privacy of personal information. This has covered the NHS, central government, the police and local authorities.

Our findings have cast new light on the issue of personal information and privacy, and I hope will be of interest to the enquiry.

Increasing access to databases

Across the public sector service reform is being driven increasingly by centralising information. For example, the Summary Care Record (SCR) system will hold health records of more than 98% of the population, and our research found more than 101,000 non-medical staff will have access to the SCR.

In another area, local authorities are being given increased access to the national insurance information traditionally held by central government, as part of the welfare reform agenda. This system contains salary details and other sensitive information and we believe staff have already been disciplined for wrongly accessing the database, both in the public sector and in private sector providers.

As the number of people with access to systems increases, it is clear that unless granular audit processes are in place, the fear of being discovered as the source of disclosed information will be insufficient when weighed against the potential financial gain.

This emerging issue is both a business process weakness but also an inevitable part of the 'digital by default' shift.

www.bigbrotherwatch.org.uk
55 Tufton Street, London SW1P 3QL

Our research into the Criminal Record Baurau system found how in 2011 alone almost 3m CRB checks were made by 'registered organisations', equivalent to 1 in 17 of adult population being checked.

Of the highest users of the system, 13 of the 25 were private companies, while 3,924 bodies are now 'registered' with the Criminal Records Bureau. These organisations do not need to demonstrate that the person being checked has consented to the check, and with the sheer volume of checks being performed it is not difficult to imagine a situation where a few malicious checks are included without detection.

The CRB system highlights the risk of technological solutions being implemented in such a way that the volume of use makes proper consideration of safeguards almost impossible.

As the policy agenda pursues greater data retention and sharing – from the Communications Capabilities Development Programme to NHS data sharing for research purposes – this risk is magnified.

It is often said that personal information is the currency of the digital age. This is absolutely true, the only error may be underestimating the scale of the market.

The market for personal information

In the cases of 'blagging' the individual responsible for protecting the information is not party to the investigation, and is not aware of the law being broken. However, there is clear evidence now that individuals with access to certain databases are increasingly aware of the commercial value of information to the media, private investigators or other interested parties.

There have been individuals who have done this kind of work for some time and that is well documented. However, as the growth of public databases continues, a wider number of people have access to information – making identifying sources much harder.

Furthermore, as the media landscape has shifted to more exclusive, celebrity and gossip led stories, using sources with access to confidential information is becoming an increasingly lucrative option. Indeed, as services are driven online and greater emphasis placed on collecting and processing information in centralised databases for a range of legitimate purposes, the weak link in data protection will continue to be those at the 'coal face' of administration.

The lack of any serious punishment for selling confidential information is also an issue – fines to individuals have been insignificant compared to the payments potentially available. Added to the economic reality, there is an emerging 'depressed bottom' who are employed with access to data, often in relatively anonymous roles (for example, call centres) and in environments with a high turnover of staff. This is magnified when looking at off-shore service provision, whether data storage or customer contact services.

This runs across the public and private sectors. Our research earlier this year highlighted how more than 900 police officers and staff we discovered misusing their access to national police databases, and in one case an employee of a gambling company sold the details of 65,000 customers to a rival company.

Equally, with the proliferation of portable devices capable of storing large volumes of data, deliberately capturing information becomes easier and quicker. Whether people in call centres using camera phones to grab a screenshot or someone walking out with a concealed USB stick, the issue is one which will get much, much worse if action is not taken urgently.

The accidental discovery problem

In cases where information is deliberately gathered without permission and sold on, there is a clear causal link between the actions of the person with access to information and the journalist.

However, Big Brother Watch's research has found that there is a significant risk to privacy in information being lost, stolen or being visible in non-secure environments.

In hundreds of cases across local authorities and the NHS, information has been left in public places, documentation and unencrypted storage devices lost and not recovered. Indeed, it could be suggested that in some local authorities and health trusts a private investigator or journalist would simply have to keep a watchful eye on waste bins, such is the frequency that confidential information is disposed of improperly.

In this situation, it would be difficult to argue that the person recovering the information was breaching the Data Protection Act, and proving theft would be difficult as we have found a great deal of reluctance among public and private organisations to admit when information is lost or improperly disposed of.

For example, we discovered that in Derbyshire a council laptop was sold to a member of the public without being properly secured. As a result, council and social care data remained on the laptop. Indeed, we found 35 local authorities that had lost or had stolen information relating to children and young people. Were a journalist to have bought this laptop, no law would have been broken by the journalist if they were to go on and publish the information. The only action would be against the council for breaching the Data Protection Act, and subsequent disciplinary action against the council employee.

As data is moved off-shore and commercial services take on an international dimension, I expect the occurrences of data leakage in this fashion to massively increase.

Regulation of the press:

The enquiry has heard much about the commercial pressures modern journalists work under. Time, and money, is at a premium with little potential for thorough investigation. The potential to use public information to corroborate stories is clear, as is the potential for information to overcome obstacles during investigations. The greater future threat in my opinion lies in journalists using public or private databases as the source of stories, under the guise that such information has been leaked to them or simply 'found' and without any necessary wrongdoing on the part of the media organisation.

The regulatory question here is whether the burden should be on the media organisation to demonstrate that the law was not broken in obtaining information – for example, through Freedom of Information requests or interviews with other sources.

The growth of database-led services, with increasing amounts of personal information held within them, is a clear threat to privacy. The temptation for those with access to either deliberately extract information, combined with the likelihood of some information being accidentally lost or disclosed, means the issue cannot be ignored when discussing the broad question of press conduct.

With specific regard to regulation of the press, and whether the press should be subject to additional constraints, I would argue that the issue is protecting information at source, rather than publication. If the individuals responsible for accessing information feared the repercussions of disclosure – with or without intent – then the risk would be much better dealt with.

Furthermore, in the UK there is no legal right to be notified if your personal information is accessed or lost – we would argue that such a process would further enhance privacy.

However, there remains a risk that personal information could be accessed by the media and with this regard there is a clear regulatory gap.

This could either be addressed through a new public interest test in disclosing information, within the remit of the press regulator, or an addition to the Data Protection Act which could cover the disclosure of information (including by publication) which resulted from a breach of the Act.

The reliance on IT systems for the delivery of public services means the amount of centrally held information, in both the private and public sectors, is only going to increase. The question must be whether there are sufficient legal safeguards in place to protect privacy and ensure that confidential information is not disclosed purely in the interests of circulation. At present, that is not the case.

Ultimately, it remains an absurdity that those deliberately breaking the law (s55 of the Data Protection Act) cannot be sent to prison for their crime, and if there is a single regulatory change that will protect privacy and ensure the media do not find it so easy to access personal information, I believe it would be the introduction of custodial sentences.

Nick Pickles

Director

Big Brother Watch

Statement of Truth

I believe the facts stated in this witness statement are true.

Signed ..

Date ... 16th June 2011