ISSN 1758 8421

Criminal Law News

SALLY RAMAGE®

www.sallyramage.net

Contents -

Issue No 63 January 2014

PUBLISHED BY SALLY RAMAGE
COPEHALE, COPPENHALL, STAFFORD,
UNITED KINGDOM
TEL 01785 - 244725
FAX 01785 - 228281

Protection of Freedoms Act 2012
Comment by
Sally Ramage

The Protection of Freedoms Act 2012 provides for the destruction, retention, use and other regulation of certain evidential material; imposes consent and other requirements in relation to certain processing of biometric information relating to children; provides for a code of practice about surveillance camera systems and for the appointment and role of the Surveillance Camera Commissioner; provides for judicial approval in relation to certain authorisations and notices under the Regulation of Investigatory Powers Act 2000; provides for the repeal or rewriting of powers of entry and associated powers and for codes of practice and other safeguards in relation to such powers; makes provision about vehicles left on land; provides for a maximum detention period of 14 days for terrorist suspects; replaces certain stop and search powers ; provides for a related code of practice; amends the Safeguarding Vulnerable Groups Act 2006; makes provision about criminal records; disregards convictions and cautions for certain abolished offences; makes provision about the release and publication of datasets held by public authorities and to make other provision about freedom of information and the Information Commissioner; and repeals certain enactments.

Data hijacking
By
Sally Ramage

A number of large corporations have suffered computer hijacking. Such data security breaches and corporate data theft are very serious incidents, reminding all companies of all sizes to review their data security. Regulators are beginning to attend to this matter also, bearing in mind that legislation, especially U.S. legislation, makes it obligatory for such corporate data breaches to trigger a 'Breach Notification Obligation'.

Any unauthorized acquisition of [unencrypted] computerized data must be notified by the affected corporation to shareholders and investors including institutional investors. The timeframe for notifying parties is 'in the most expedient time possible and without unreasonable delay.'

In the United States, such data breach must be reported to third parties 'in writing (on paper and sent by mail);in electronic form (by e-mail, but only if the individual has
consented in advance to receiving the notice in electronic form); by substitute notice; by telephone (in certain countries-(note that in the United States (the states of Montana, New York and North Carolina) notification of data breaches may be performed by telephone. At the same time, certain states do not permit notification of data breach to be performed by email.

Interagency Guidance

"Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to
contact all customers affected by telephone or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

The problem is that business owners typically have a false sense of security and in fact, 85 percent of business owners believe their company is safe from hackers, viruses, malware or a cyber-security breach, according to a September 2012 survey of over 1,000 U.S. small businesses sponsored by Symantec Corp. Symantec Corp.

This is particularly true of small and midsized businesses (SMBs) that don't consider themselves targets, said Maxim Weinstein, executive director of StopBadware, a non-profit organization that provides online tools and information on how to protect against malware. Maxim Weinstein said:

'A lot of high-profile companies were targets but the techniques used in those attacks, such as spear phishing, are used against businesses of all sizes'.

As large enterprises put strong defenses in place, cyber-criminals move down the line to where there is opportunity, ie to the smaller businesses. Customer data, intellectual property and banking credentials are all valuable to criminals, no matter the size of the organization, said Michael Kaiser, executive director of the NCSA. He said: *'If a criminal can steal $30,000 from a small business in one fell swoop by hacking into a business banking system, that's not a bad day for the criminal'.*
The bulk of opportunistic security threats can be prevented by doing three things: Keeping software up to date, using the most current versions of antivirus software and training your employees about data security practices. While these sound like simple solutions, some of the most basic data security practices are not put in place and many businesses lack sufficient cyber security policies and training. Discussions about staying safe online and securing company assets simply are not happening and in fact, 77 percent of business owners said in a NCSA survey that they do not have a formal written Internet security policy for employees and of those, 49 percent reported that they do not even have an informal policy. In addition, 56 percent of businesses do not have Internet usage policies that state what websites and web services employees may use. It is in no way a draconian measure if at the very least, Businesses have policies that provide legal protection and set expectations.

Intellectual Property, Customer Information and Employee Information stolen

There are many reported cases of data theft and it is clear that business owners of all sizes need to take the time to protect their data and thus avoid becoming a victim. The first step to creating a data security plan is to understand what is at risk. Intellectual property, customer information and employee information are all 'the coin of the realm' for cybercriminals and these assets must be protected.

Strong Passwords

One of the simplest ways to protect sensitive data is by using strong passwords. A strong password would incorporate a combination of letters, both upper and lowercase, numbers, and punctuation marks.

Install antivirus software

To protect against malware, employers must install antivirus software and keep such software up- to –date. Implementing policies around the types of websites and data which employees access while on a corporate network is essential.
Because of the abundant use of smart-phones or tablets at work, businesses must set some clear policies surrounding data access on mobile devices and secure email practices. For instance, sensitive customer information or intellectual property data should not be installed on devices that run the risk of being lost or stolen.

Encryption

It's also good practice to encrypt data that is accessed on mobile devices and to set up a way to remotely wipe sensitive data in case a device is lost or stolen

The all-important business of selling
Sally Ramage

For a new business, there is the juxtaposition of growing the business, refining the product and legitamately selling the product without misrepresentation or deceit.
A conundrum that many business owners and consultants experience while trying to grow their business is discovering that expertise about a product or service is not enough to generate revenue.

Regardless of the quality or usefulness of any offering, there's the dreadful fact that products, and especially services, rarely sell themselves.
No one thinks of owning a business as creating a sales job.
The salesman is the kingpin; he is the rainmaker, the revenue czar or money magnet.

The role of salesperson carries a stigma and is a mark of disgrace for some people.
Whether you like it or not, you're the company's sales force or sales team leader.
Understanding some basic sales principles will help grow your revenue.

Here is a short list of what every business owner should know about selling (country or product):

First, avoid believing that educating the buyer completely about your offerings will motivate them to buy.

That leads to the No. 1 problem in selling: talking too much.
Doing that says:
'I am not really interested in you'
or
'I'm more important than you.'

Talking too much conveys a lack of interest and respect.
Listening conveys empathy and empathy builds trust.
Everyone has experienced the desire to get away from someone who talks too much.
Giving too much information that's unimportant to the buyer increases the number of objections.
Would you be willing to pay extra for features and benefits that you don't need or want?
Use the rifle approach rather than the shotgun when presenting.
Understand value from the buyer's perspective.
Benefits are benefits only if the buyer sees them as important. Turn a feature into a benefit by tying it to a problem. Prospects will buy more quickly to solve a problem or perceived problem than they will to gain a benefit that will occur later. Studies also suggest buyers will buy to prevent a loss before buying for pleasure.
Upsell and gain add-on sales by asking questions around problems your solution can resolve or prevent.
Prospects who disclose the problems and fears they face are more likely to buy. The ability to uncover and solve customer problems on a continuing basis turns you into a trusted adviser.
Once you are in that valued inner circle of trust, the sales process becomes almost automatic. This approach also helps distinguish tire kickers from those who are sincere prospects.
Because potential customers often don't know what they don't know, they ask for proposals and presentations, or to stall the sales process.
Writing and preparing proposals and presentations requires vast amounts of time, energy and resources.
Proposals and presentations should be to prove how your solution is the right one for the buyer, not to create interest.
Save valuable resources by qualifying first. A qualified prospect means you thoroughly understand their need, you know the decision criteria, and you have qualified them for their ability and willingness to make the required investment.
An easy way to deflect an early request for a quote or proposal is to say,
'So I know what to put in it, let me first get an understanding of your situation and needs.'
Avoid using industry and product jargon if possible.
Every industry has its buzzwords, and some products have become so technologically complicated that the amount of explanation needed to make customers understand makes their eyes glaze over. Prospects usually enter the sales process with their guard up, so any jargon they don't know adds to their apprehension.
If your prospect is an expert, too, using technical or industry terms can contribute to the perception of your expertise. However, using clear and simple wording doesn't hurt you with the knowledgeable buyer, and protects you from creating even more hesitation from prospects that don't know or understand the technical terms.
Remember that hearing 'no' is a good thing.
Getting a clear decision is better than hearing a stall or excuse, which only extends the investment of time and resources. Keep reality in perspective, because not everyone will buy, you can't sell everyone, nor is everyone a prospect. It's better to find out sooner than later if someone is not going to buy.
It's also OK to say "no" to a request for services or solutions you find difficult or don't want to provide. By having clarity on your market niche and your ideal client, you'll cut expense and increase margins.

Further Reading

Garry Duncan, 'Sales: what every business entrepreneur should know', Denver Business Journal, 12 March 2012. http://www.bizjournals.com/denver/blog/broadway_17th/2012/03/sales-what-ever-entrepreneur-should-know.html

Legal Aid, Sentencing and Punishment of Offenders Act 2011

Sally Ramage

This Act reverses the position under the Access to Justice Act 1999, so that civil legal aid is not available for any matter not specifically excluded; it abolished the Legal Services Commission; made various provisions in respect of civil litigation funding and costs; made changes to sentencing provisions, and gives courts an express duty to consider making compensation orders where victims have suffered harm or loss. It reduced the detailed requirements on courts when they give reasons for a sentence; and allows courts to suspend sentences of up to two years rather than 12 months. The Act amended the court's power to suspend a prison sentence; and introduces new powers to allow curfews to be imposed for more hours in the day and for up to 12 months rather than the current six; repeals provisions in the Criminal Justice Act 2003 which would have increased the maximum sentence a magistrates' court could impose from six to 12 months; makes changes to the law on bail and remand, aimed at reducing the number of those who are unnecessarily remanded into custody.

Under the new 'no real prospect' test, people would be released on bail if they would be unlikely to receive a custo1dial sentence; makes provision to ensure that, where a person aged under 18 has to be remanded into custody, in most cases they would be remanded into local authority accommodation; amends provisions relating to the release and recall of prisoners; gives the Secretary of State new powers to make prison rules about prisoners' employment, pay and deductions from their pay. The intention of these provisions is that prisoners should make payments, which would support victims of crime; introduces a penalty notice with an education option and provision for conditional cautions to be given without the need to refer the case to the relevant prosecutor
This Act creates a new offence of threatening with an offensive weapon or an article with a blade or point thereby creating an immediate risk of serious physical harm. A minimum sentence of 6 months' imprisonment would normally be given to persons over 18 found guilty of this offence.

Corruption in the Police Service

Sally Ramage

The word 'corruption' was defined in 'Police Guidance on Corruption' , published in 2010.Corruption is there defined as including: 'any attempt to pervert the course of justice or other conduct likely to seriously harm the administration of justice, in particular the criminal justice system; payments or other benefits or favours received in connection with the performance or duties amounting to an offence in relation to which a magistrates' court would be likely to decline jurisdiction; corrupt controller, handler or informer relationships; provision of confidential information in return for payment or other benefits or favours where the conduct goes beyond a possible prosecution for an offence under section 55 of the Data Protection Act 1998; extraction and supply of seized controlled drugs, firearms or other material; attempts or conspiracies to do any of the above.'

In the past year, 2010/2011, over 2,400 referrals, for all types of incidents, were received by the IPCC from police forces and other law enforcement agencies. Of those, over 200 were classified as cases of serious corruption. A similar number of corruption referrals were received in both 2009/10 and 2008/9. The current system requires forces and authorities to make a judgement that a case meets the threshold for referral to the IPCC and then make the referral. In addition to this, cases of corruption may also be referred to the IPCC on a covert basis.

During 2010/2011, the IPCC received 44 covert referrals. In 2009/10, the number made was 45, and in 2008/9 there were 29 covert referrals. The report sets out six specific cases that the IPCC has dealt with which have now come to a conclusion, and details the lessons and recommendations that have been made as a result. The IPCC found that in several cases, wrong- doing was not detected due to lack of or inappropriate supervision. There had been a failure to identify issues that lead to officers being involved in criminality. In many cases, computer systems had been misused by individuals and the IPCC found that a lack of system safeguards had in some cases, aided the misuse. Due to not having a robust police, police expenses claimed inappropriately were facilitated.

Further Reading
Corruption in the Police Service: Part 1 can be accessed in full at:http://www.ipcc.gov.uk/Documents/Corruption_in_the_Police_Service_in_England_Wales.pdf

Community sentences

Sally Ramage

A report has been published following a national enquiry, which looked at whether community sentences are more effective than short prison terms in stopping persistent, low-level offending. 'Community or Custody: which works best?' is the final report of the enquiry commissioned by the group named Make Justice Work. It found that community sentences can be cheaper, tougher and more effective than prisons for persistent, low-level offenders, but reoffending can only be reduced if certain standards are met.
The enquiry lasted one year and gathered evidence from victims, offenders, judges, magistrates, police and probation officers, prison governors and voluntary and private sector providers delivering intensive community services across the country. The subsequent report stated that community sentences do have an important role to play in meeting both the expectations of the public and the victim's expectations.

The US/UK 2003 Extradition Treaty

Sally Ramage

It is of critical importance in the prevention of disorder and crime that those reasonably suspected of crime are prosecuted and, if found guilty, duly sentenced. Extradition is part of the process for ensuring that this occurs, on the basis of international reciprocities.

The practice of extradition originated in the ancient middle and far-eastern civilisations. The earliest recorded extradition treaty dates to 1280 B.C., between Ramses II, the Pharaoh of Egypt, and King Hattusli III of the Hittites, providing for the mutual return of criminals. The first, similar provision appeared in Western Europe in 1174 A.D., between Henry II of England and William the Lion, King of Scotland.

Treaty of Amity 1794

The 1794 Treaty of Amity, Commerce, and Navigation, or, the Jay Treaty, was the United States' first treaty and it was with Great Britain. The Jay Treaty provided for either UK or US government to deliver persons charged with murder or forgery to the other government 'on requisition' but only on evidence of criminality that would justify apprehending and trying the defendant in the country where he was located if the offence had been committed there. Unfortunately, the Jay Treaty provided no specific procedure for extradition.

Definition of extradition

Today, the United States has extradition treaties with over a hundred countries, including many former British colonies that adopted by state succession, the 1931 Treaty with the United Kingdom, with 'extradition' meaning:

'The surrender by one nation to another of an individual accused or convicted of an offence outside of its own territory, and within the territorial jurisdiction of the other, which, being competent to try and to punish him, demands the surrender.'

An international extradition treaty obligates the host country to surrender to a requesting country a person charged with or convicted of an offence in that country. The willingness of countries to accept limitations on their state sovereignty stems from four purposes which provide the theoretical foundation for international extradition: to obtain reciprocal return of fugitive offenders; to facilitate the punishment of wrongful conduct, and thereby promote justice; to avoid harbouring within their borders those who may commit offences similar to those which they are accused of committing in another jurisdiction; and to avoid international tensions caused by one country's refusal to return a particularly sought-after accused offender.

The US/UK Extradition Treaty 2003

The most recent extradition treaty between the United Kingdom and the United States was signed in Washington on 31 March 2003. David Blunkett signed the 2003 Treaty, as the then Home Secretary, for the Government of the United Kingdom. Parliament was not consulted and the text of the treaty was only made public after it was signed. Even though the 2003 UK/US Extradition Treaty does not differ substantially from the 1972 US–UK many believe that it was negotiated and signed in secret and removed the fundamental protection of providing evidence for those in the UK facing extradition requests from the US, and this was the bitter complaint of the 'three former NatWest bankers' who later pleaded guilty engaging with fraud with former senior officers of Enron. According to a U.S. Justice Department indictment, the bankers became involved in one of Enron Chief Financial Officer Andy Fastow's many offshore vehicles, which eventual discovery triggered the bankruptcy of the Houston energy-trading giant, Enron.

Another controversial extradition request from the United States was for the extradition of Ian Norris, the former chief executive of Morgan Crucible, who was charged in the US with cartel activity and perverting the course of justice by seeking to frustrate the subsequent criminal investigation in the US. In 2008, the House of Lords held that Norris could not be extradited to face the price-fixing charges in the US, because the alleged conduct was not criminal under English law at the time it was alleged to have been committed, but that the related charges of obstructing justice meant that Ian Norris must be extradited to the US. Norris' case went to the UK Supreme Court and then to the European Court of Human Rights in Brussels. In dismissing Norris' appeal, the Supreme Court stated that: 'It is of critical importance in the prevention of disorder and crime that those reasonably suspected of crime are prosecuted and, if found guilty, duly sentenced. Extradition is part of the process for ensuring that this occurs, on the basis of international reciprocity.' The 2003 Treaty continues to generate

controversy with the request for the computer hacker Gary McKinnon posing a problem for the new UK Coalition Government. Nick Clegg had suggested, on 25 May 2011, that it might not be straightforward for the Coalition to prevent Gary McKinnon's extradition, although the UK Government did later announce that it would conduct a comprehensive review of the 2003 Treaty.

German securitisation

Sally Ramage

It was reported that, in 2003, Deutsche Bank, HypoVereinsbank, Dresdner Bank, Commerzbank and DZ Bank formed a joint venture with state-owned Kreditanstalt fuer Wiederaufbau. The venture was reported to hold a fund of up to 50bn Euros (£35bn; $54bn), in investment-grade loans. This fund was divided chopped into pieces and sold to investors as bonds, a process known as securitisation.

German authorities denied that it was a bail-out, but it was a sign of the depth of the difficulties that have afflicted the banking sector since the German economy began a slow-down. The banks had admitted that this strategy shifted sufficient risk off their books to allow them to step up lending to small- and medium-sized German companies, although many German firms complained that the weak state of bank finances has made routine loans hard to secure. The German government, although concerned that it would slow-down the economy, considered a tax break for the venture.

Securitisation

Securitisation can be a useful way of making unreliable financial assets more attractive to investors. A credit-card company may face considerable risk from each individual unsecured card loan, for example. But when those loans are bundled together into a fund, the risk of serious default is diminished, and the card company is able to sell off bonds backed by that debt at a favourable rate. This technique has sparked the creation of all kinds of exotic debt markets, especially in the United States (' US'), notably for bonds backed by pooled mortgage payments. In Europe, tax laws on this sort of investment were less favourable.

Printed and published by Sally Ramage® Copehale, Coppenhall, Stafford, ST18 9BW, UK. Registered as a Newspaper at the Post Office. ISSN 1758-8421.