Data Protection Review Group

Consultation Paper

Contents

Introduction

The Minister for Justice, Equality and Law Reform has established a Data Protection Review Group to make recommendations on whether Irish Data Protection legislation needs to be amended to provide for mandatory notification of data breaches with penalties. (Terms of reference and membership are at **http://www.justice.ie/en/JELR/Pages/WP09000015**).

To date there has been a public request for submissions, a consultation exercise among group members, and extensive desk research. The Department of Finance has issued revised guidelines on Data Protection for the Public Service and the Data Protection Commissioner (DPC) has updated his Office's Guidelines on best practice (**http://www.dataprotection.ie/viewdoc.asp?DocID=901&ad=1**.)

The Data Protection Review Group has decided to publish this Consultation document to discuss a number of areas of the broad topic. The main regulatory options available are identified and interested parties are asked to provide comments thereon by 30/10/2009 to assist the Group reach a balanced conclusion on how Ireland should address the issue of the most appropriate legislative response to data breaches.

Feedback is welcome on any question covered but in particular, feedback on the regulatory options identified at the end of the document. (Submission arrangement details are on page 39)

While devices continue to be lost or stolen, perhaps encouragingly the most recently widely reported instances showed a greater degree of encryption in place than would have been the case previously. Both became known due to the organisations concerned (Bord Gáis and HSE) reporting to either the DPC or an Garda Síochana. What was most clearly demonstrated is that where even one unencrypted laptop containing personal data is stolen, this can give rise to significant concern about the damage and distress that could result from the misuse of this data, with a consequential degree of reputational (and potentially financial) damage to the organisation concerned

Data Breach

A data breach can happen for a number of reasons, including:-

- loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises);
- inappropriate access controls allowing unauthorised use;
- equipment failure;
- human error;
- unforeseen circumstances such as a flood;
- a hacking attack;
- access where information is obtained by deceiving the organisation that holds it.

Current Legislative Framework

The Data Protection Acts 1988 to 2003 impose obligations on organisations ("**data controllers**") that process personal data. "Personal data" and "processing" are defined very broadly to cover any information that can be related to a living individual (a "**data subject**") and anything done with that information. The principles governing the processing of personal data are that such data should be:

1. Obtained and processed "fairly"(usually involves consent)
2. Collected for a specified purpose
3. Not be disclosed to other parties
4. Kept safe and secure
5. Kept accurate and up-to-date
6. Be relevant and not excessive
7. Not be retained for any longer than necessary
8. Available to the individual concerned on request

A data controller is obliged to adopt "appropriate security measures". These are defined in the legislation as being "appropriate to (i) the harm that might result from unauthorised or unlawful processing, accidental or unlawful destruction or accidental loss of, or damage to, the data concerned, and (ii) the nature of the data concerned". The data controller "may have regard to the state of technological development and the cost of implementing the measures". The data controller must take "reasonable steps" to ensure that employees are aware of and comply with the security measures in place.

There is no specific obligation imposed on a data controller to inform either a data subject or the DPC of an incident involving the loss or improper disclosure of personal data. However, as already indicated the DPC has issued breach notification guidance which recommends that as soon as a data controller becomes aware that personal data for which it is responsible has been compromised, it should as part of the response, immediately notify the DPC.

There is a different regime in place for data held by organisations operating in the Telecoms field. The Electronic Privacy Regulations (S.I. No. 535 of 2003 as amended by S.I. No. 526 of 2008) impose more specific obligations on telecommunications providers – including an obligation to inform subscribers of any "particular risk" of a breach of security. Substantial penalties can be imposed for breaches in these Regulations.

Why Data Breaches Matter

Data breaches can damage an individual in different ways. Personal data that includes banking or credit card details can be used to defraud the individual. The unauthorised disclosure of personal information to third parties - especially if the information is of a sensitive or intimate nature - can be deeply distressing to an individual.

The possibility that disclosure to third parties may have taken place due to an inadvertent data breach can itself be a cause of distress. The measures that an organisation may advise to its clients as a precaution against fraudulent misuse can also be inconvenient and costly for an individual. These factors might militate against notifying individuals of a data breach which is unlikely to lead to any negative consequences.

Prevalence

Substantial data breaches have happened in Ireland. There is an increasing tendency to report them. Perhaps because of recent public concerns it is noticeable that there has been a significant increase in the use of encryption on laptops and USB keys. However in the very recent past there have been cases of unencrypted data on stolen devices. Ireland

does not seem to be outside the norm of countries for data loss and there is no evidence that this is a particularly Irish problem.

Probability

Given

- the quantities of data being held,
- the growth in types and numbers of devices which hold significant quantities of data,
- the degree to which individuals consent to handing over personal information and
- the levels of general theft and computer related crimes

it would be naive to assert that changing regulation on its own would eliminate such losses.

However better regulation can impact the probability that these devices carry sensitive personal information in unencrypted, retrievable format. This would reduce the prospects of damage being done by such losses.

Some common threads

There is substantial agreement on the financial and other damage caused by lost data. There is a real problem – which is may be underreported. It seems clear that either the number of data breaches or the number of reported data breaches in many countries is increasing (or both). There is widespread agreement that *prevention* of data loss by adhering to data protection principles is far superior to incurring reputational and regulation costs.

There is a recognition that Governments need to have a calibrated, balanced regulatory response as an element of reducing the probability of damage being done by lost data. Mandatory reporting of breaches with penalties is in place in many States in the USA, is being actively considered by many other Governments and is being introduced in Germany. A Private Members Bill has been published on the subject in the Dáil.

There is widespread recognition that individuals whose data has been lost or stolen need to be informed in a timely way, at least where there is a significant danger that the breach may cause financial or other damage to the individual. Increasingly common practical steps are being described on what should happen in cases of data breaches and how to go about reporting.

There are significant differences between countries in the underpinning regulatory structure to support the increasing recognition that reporting breaches to regulatory authorities and/or data subjects is an important step in damage reduction (legislation, guidelines, advice, best practice, codes of conduct, market imperatives). Because sensitive personal information is held by so many different types of organisation for so many purposes and in so many different forms there is a wide variety of national and international regulatory issues. There is no immediately identifiable single best practice data security standard to which organisations can subscribe which covers all industries.

Review of existing legislative framework

The Group is looking at its terms of reference under three main headings: Legal, Technical and Regulatory. The technical issues and regulatory objectives are broadly the same everywhere. However the legal approaches and regulatory frameworks vary considerably from country to country.

Legal Issues

1. EU Model.

The EU/Council of Europe model involves the setting of basic principles of data protection and providing rules for transborder flows of personal data. This model involves the establishment of an independent body to monitor the application of data protection law. The EU Directive on the protection of individuals with regard to the processing of personal data (Data Protection Directive)[1], which is horizontal in its application and applies to any operation or set of operations which is performed upon personal data for the purpose of activities which come within the scope of EC law. The directive does not provide for mandatory reporting of data breaches. This Directive is complemented by the e-Privacy Directive (Directive 2002/58/EC) which deals with data protection for phone, e-mail, SMS and Internet use. This Directive does not provide for mandatory reporting but is currently under review. Similarly, the Council of Europe data protection instruments[2] do not provide for mandatory reporting of data breaches.

Data protection legislation is horizontal in its application and covers all organisations in every sector, although there is a different regime in place for data held by organisations operating in the Telecoms field.

The breaches now under consideration are without exception breaches of one or more of the fundamental principles: an organisation has either

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108) and Additional Protocol to the Convention for the Protection of Individuals with regard to the automatic processing of Personal Data regarding supervisory authorities and transborder data flows.

gathered information it shouldn't have, not kept it under adequate security, not disposed of it when it should have or allowed it into the control of some other party. The German Federal mandatory reporting law coming into force in September 2009 provides that where data controllers who believe they have lost data which puts their data subjects into "imminent risk" must report simultaneously to the Data Protection Authorities (DPA) and directly to the data subjects with substantial fines (up to €300,000) and other actions up to prohibiting the organisation from further processing. However, no other EU country has a specific data breach notification law. Although Ireland and Denmark have begun formal consideration processes the issue is, or has been, under consideration in a number of member States.

In March 2008, the United Kingdom's Information Commissioner's Office (ICO) – the UK's data protection authority - issued a guidance note on data security breach management[3] and a further note specifically addressing notification of data security breaches to the ICO[4]. The notes advise that, though there is no legal obligation to report data security breaches, the Information Commissioner believes that serious breaches should be brought to the attention of his Office. The guidance note states that notification is not an end in itself but should have a clear purpose, whether to allow those affected to protect themselves or to allow regulatory bodies to perform their functions, provide advice and deal with complaints. When deciding whether to notify the ICO, data controllers are encouraged to consider the potential harm to data subjects, the volume of personal data compromised and the sensitivity of the compromised data. The ICO will then decide whether to recommend that the data controller makes the incident public based on their consideration of the public interest.

The "Data Sharing Review Report"[5] (July 2008) considered mandatory notification of the ICO of all serious security breaches and found that placing an explicit statutory duty on organisations to report all breaches would add a significant extra burden for organisations and could produce "breach fatigue" among the wider public if it were to result in frequent and unnecessary notifications of minor incidents. They recommended however

---

3 http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf

4 http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf

5 http://www.justice.gov.uk/reviews/datasharing-intro.htm

that, as a matter of good practice, organisations should notify the ICO when a significant data breach occurs. They also recommended that in cases involving the likelihood of substantial damage or distress, the Commissioner should take into account any failure to notify when deciding what, if any, penalty to set for a data breach.

The UK's Data Protection Act was amended during 2008 to give the Commissioner the power to directly levy a monetary penalty on a data controller for serious breaches of data protection principles which were either deliberate or reckless. The sections have not yet been commenced. The maximum level of penalty is to be prescribed by regulation.

Some current EU developments on data breach reporting.

Until recently it seemed that there would not be any revision of the EU Data Protection Directive for at least a number of years. Such a revised Directive would have to address the issues raised by mandatory reporting which are discussed in this document in particular the differing EU legislative responses between Data which is held in the context of telecoms and other data.

The data protection regime provided for in the Data Protection Directive has its origins at a time when data systems and telecommunications were fundamentally separate. There has, of course, been substantial technical and industry convergence in recent years.

The EU's data protection regime was updated and complemented by a sectoral *e*Privacy Directive (2002/58/EC) dealing with data protection in the telecommunications sector. Significant penalties are prescribed by the transposing Regulations (SI 535/2003 as amended by SI 526/2008) for organisations found guilty of sending unsolicited marketing messages. This gives rise to a situation whereby the DPC has power to prosecute for the sending of unsolicited marketing messages while he has no such power in relation to data-holding organisations that lose data.

The Telecoms regulatory regime is currently being reformed under the Telecom Reform package, including a revised ePrivacy directive. This was worked through a substantial number of iterations between the European Parliament, the Council of Ministers and the Commission with input from the Data Protection Supervisor and the Article 29 Working Group of EU Data Protection Authorities during 2008 and 2009. These iterations and

discussions continued up to the last session of the outgoing Parliament and the matter is not yet resolved. As part of the discussion, Commissioner Reding made a commitment that the Commission would consider bringing forward data breach reporting as a stand alone issue preceding any general change in the Data Protection Directive.

On 11 June 2009, the Council held an informal discussion on the state of play of the Telecom Package. In its subsequent press release, the Presidency announced the Council's intention to adopt the three proposals of the package as soon as possible. It further said that "The Council is ready to work towards a solution .... and looks forward to working with the newly appointed European Parliament during conciliation." It is expected that negotiations will start shortly.

The likely time frames and the shape of the compromise (especially in respect of penalties) that may arise between the ePrivacy directive and a Data Breach notification directive will become clearer when the new Parliament and Commission consider the issue. Clearly, if a stand-alone mandatory breach reporting Directive is adopted then Ireland will transpose it. There may be some potential advantage for being an early mover in advance of knowing the shape of the Directive. This could be offset if the directive did not materialise or took a substantially different form which might require any legislation passed now to be revisited in the short term. The consensus view, where the matter has been considered within the EU, would seem to be that breach reports would be made to Data Protection Authorities and in appropriate cases to data subjects and that some mechanism of avoiding over reporting needs to be developed. As mentioned above, the new German legislation, which comes into effect in September 2009, envisages a simultaneous report to the DPA and to the data subject. The Private Members Bill published by Fine Gael envisages reporting to the DPC in the first instance and subsequently and in appropriate cases within a short space of time to the data subject. http://www.oir.ie/viewdoc.asp?DocID=10087&&CatID=59&StartDate=01%20January%202008&OrderAscending=0

Australia, New Zealand and Canada have actively considered making disclosure of data breaches to Data Protection authorities mandatory but so far have not. There do not seem to be any other foreseeable developments in relation to data breaches likely to arise from Council of Europe activities over the next two years.

2. USA Model

The mandatory reporting legislation in the USA forms part of a web of different approaches resulting in high levels of awareness. There are different laws in different states. The US experience traces back to the passage of Californian breach reporting legislation in 2001, variations of which have now been passed in more than 40 states. Thresholds, reporting formats and penalties vary from State to State. The various Acts are described in Federal Information Security and Data Breach Notification Laws http://opencrs.com/document/RL34120/2009-01-29 .

It is not clear that the legislation has had the originally desired impact in terms of reducing the incidence of data loss, though it may reduce the impact by giving individuals the opportunity to mitigate harm. The number of recorded cases has continued to rise from year to year.

This may be a function of the volumes of data being held and how it is being held, or that more breaches are now being disclosed because of the legislation. It may well be that there would be even more breaches than are currently being reported if the breach disclosure laws had not been passed. The interactions under these laws are generally between the data holders who, on becoming aware of breaches, decide on balance whether or not to inform the people who are potentially harmed. While the majority of laptop/usb/cd theft/loss issues do not result in any direct harm all notifications thereof cause some degree of individual apprehension and corporate reputational damage. There is limited case law on the topic – some class actions are at various stages in the Courts system seeking damages for harm done and also for apprehensions caused by notifications.

As the US, at both federal and state level, does not have the exact equivalent of EU Data Protection Authorities, reporting of data breaches to such authorities does not generally arise. However, agencies such as the Federal Trade Commission (FTC) perform many of the functions typically performed by a DPA, with very strong enforcement powers in cases where companies have failed to live up to their privacy promises to their consumers. FTC action has resulted in the imposition of significant financial penalties on organisations that have been found guilty of data breaches.

3. Other countries

There is a variety of legislative and regulatory regimes around the world. For example India or Malaysia where legislation on hacking or theft is used to prosecute detected data protection offences including data breaches. In most cases there does not seem to be legislation in place to provide for the reporting of data breaches to data subjects.

Other Legal issues

There is a significant amount of activity on promoting international flows of data on criminal and financial activities. In the medium term there may be a UN role for a trans-continental standard for data breach reporting, however the concept of privacy varies from country to country.

Data flows around the world instantaneously. It is, therefore, very difficult to establish exactly where all data held by organisations using the data holding services of internationally operating companies is. While the concept of safe harbour (it is permissible to allow data to pass to an entity in another jurisdiction defined as being a safe harbour) is present in EU and some US legislation, there are differences in interpretation and definition of what constitutes a safe harbour.
(http://www.mofo.com/international/EU_en/news/15419.html)

A number of other practical issues arise in the context of any proposed legislation and, of course, there will also be other unforeseen issues.

Unless the legislation provided for mandatory disclosure of all breaches, reporting requires a decision to be taken on whether the particular case merits special reporting. This decision is taken by the organisation concerned in the first place. An organisation may decide to report directly to the subject or seek a secondary decision from the DPC on whether or not to report. This is a crucial decision with substantial financial and reputational consequences.

If reporting to Data Protection Commissioner were made mandatory this would potentially leave the DPC with a decision making power to assess the impact on data subjects and to decide whether the data subjects needed to be notified. How would this duty be discharged in practice? If the Commissioner decided in a case that notification wasn't necessary,

how could the data subjects have a right of appeal against a decision of which they were not aware?

What would the data subjects' recourse be if DPC decided against disclosure, but subsequently damage was done to the data subjects and they subsequently became aware of the decision?

Significant additional legal and administrative resources could be needed to discharge this sort of decision making function, especially if an augmented inspection function were involved.

If a self regulation option were relied on, how would decisions be audited?

A decision to report could have serious reputational and financial consequences even without administrative or court imposed fines arising. While a proportion of data losses certainly give rise to financial and other damage to individuals many do not. But all notifications give rise to justifiable concerns. There is a view, based on the US experience, that there can be notification fatigue where there are frequent reports and the subjects do not notice any subsequent harm arising from the breach. Against this would be the view that it is the right of the subject to know and decide what action to take in respect of each loss of their data.

There is little case law or experience on the role of informed consent. People may have, by ticking a box to gain access to a service, allowed a company to harvest and share their details with third parties without really understanding what they have ticked. They may consider that this constitutes a data breach if that company in some way decides to use the data in an unforeseen way or if the privacy statement of the company was changed after they signed up to the service.

There is emerging case law in the USA indicating that the normal practice of a company relying on such an acceptance does not constitute a valid contract with the consumer as usually the company reserves the right to change the terms of the contract without notice or notification.
http://www.theregister.co.uk/2009/04/23/blockbuster_lawsuit/

Defences

If an offence was to be created with penalties then potential defences to any resulting prosecution would need to be considered especially if the penalties were substantial. Such defences might include:

“We took all reasonable precautions”, “We did not realise the data had been lost”, “We were hacked” ,“a rogue employee” or “we weren’t informed”

From a regulatory perspective, it would make some sense that a more substantial penalty would be inflicted on a careless organisation. In reality, the cost to the organisation is likely to be a factor of the number of clients it needs to contact or offer remediation to as a result of the breach. The cost would be the same whether an organisation had been hacked or an employee had lost a laptop. Such costs can and do stretch to several hundred thousand euro. In the UK costs can arise from industry specific regulators concluding that a serious data breach is a general failure of an organisation and very big fines have been imposed (for example, the Financial Services Authority has fined HSBC £3m for failing to properly look after its customers' information and private data.) If small organisations or sole traders choose to collect personal data they must accept the stewardship consequences of this decision.

While there are individual industry standards, there is no universal security standard to which legislators or practitioners can point to determine whether an organisation had reasonable defences in place. While the German legislation identifies the importance of encryption tools, it can only specify that they be state of the art technology. Organisations which follow all relevant best practices may still experience a loss of their clients’ data either through actions of individual employees or through malicious attack. The threshold of protection is changing all the time. There is often divergence of opinion on how serious a given threat is and it is next to impossible for even diligent practitioners to keep up with all the information that is flowing towards them and to discern when they may be under sales pressure from solutions vendors. In data security, as in other fields of endeavour, every problem has a solution. Every solution may also be the root of a new problem.

Given the range of potential defences it is clear that prosecutions of offences might not be straightforward.

Need to Future Proof Legislation

The technology landscape is increasingly universal as developments such as cloud computing, massive data centres, outsourcing, social networking and small, high-capacity storage devices are everywhere a part of modern ICT-enabled economies.

They are all contributing to increasing levels of flexibility, innovation and resourcefulness in organisations which embrace them. They are also all contributing to difficulties in the organisations concerned meeting their obligations under basic Data Protection principles.

It is very unlikely that a form of universally applicable legislation or regulation regime can be brought into being which could be technology specific. The entire foundation of the internet is based on its capacity to diversely route information to avoid single points of control or failure. A number of nations and large businesses are attempting with various degrees of success to use legal means to control this flow. The degree to which this task is difficult reflects the fluidity of data in the Information age. The degree to which these controls can be evaded and information which was intended to be private is rapidly disseminated into the pubic domain, illustrates why the primary principles of Data Protection need to be supported in a balanced, practical way.

Technical issues

Technical issues are often thought of as being primarily the responsibility of technical people within an organisation. There is a disconnect between people's desire not to get into technical issues and the degree of trust they demonstrate by using technology to hold their secrets. More and more private information is being given (or taken) on the understanding that it will be held safely. Data loss, while it has a technical aspect, is almost always a symptom of human lack of knowledge, carelessness or malice. It is important for the non-technical community to know that the ICT community does not have a universal grasp of all the issues and necessary responses.

There is a necessary and significant focus on laptops, usb keys and cds lost by large organisations when the issue of data loss is discussed. Of course there are many other ways that data held on servers or on paper can be lost or stolen.

The overall aim of action in this area could be seen as reducing the probability that information will find its way to people who should not have it. It was often stated in the early days of the widespread adoption of the internet that "information wants to be free". Initially the "wild west" of the internet was kept separate from tightly controlled corporate networks. Now they are closely intertwined. Technical developments operate to make it easier to carry and hold many more kinds of information in many more ways every year. Business trends reinforce the drive to do more with existing resources and to operate in many more locations. Breaking down barriers - "elimination of information silos" - is viewed as a good thing in the context of innovation; in the context of privacy and security it has a different connotation. Ease of use and security almost always operate against each other. Easy to use equals easy to lose.

If the focus is on reduction of the prospect of individuals being harmed by loss of sensitive personal data, the range of ways that data is held needs to be considered.

The rapid changes in use and abuse of technology challenge our capacity to define the concept of breach.

Some specific examples are

- Small devices such as Mobile phones, iPods, Blackberries, cameras and Personal Digital Assistants with perhaps 8Gigabytes (GB) of data, where one GB could hold thousands of sensitive records
- Microdevices (Micro SD, Compact Flash carrying possibly 8GB of data on a device the size of a fingernail)
- Web enablement of devices such as printers attached to computers which expose the computer to risk
- Organisational data held as working copy on home or 3rd party computers
- Use of local backup devices holding perhaps 500GB of data,
- Extracts of large databases being held in spreadsheet form for ease of manipulation and circulation
- Use of open email to transmit sensitive data, perhaps by means of attached spreadsheet
- The issue of concatenation: where data lost from one source is not in itself damaging (and would not trigger a report) unless linked to some other source. Such linking can give rise to significant levels of intrusion sometimes knows as "datarazzi" activity
- Increasing use of the "cloud" for individuals and organisations to hold, share or backup information with uncertainty as to where the information is held (geographically, legally, physically, virtually). Even reasonably advanced organisations may not be certain where every copy of all their sensitive data is being held
- Increasing use of social networking where individuals supply substantial quantities of private information
- Extended life span of data devices coupled with rapid change of effective ownership- where devices are disposed of with individuals believing they have cleaned them. Many studies show significant amounts of easily discoverable data
- Increasing availability of tools to recover lost data and passwords (which can be used by the data owner as an aid or by anyone else as an intrusion)
- Use of encryption where the key may be inadequate (or adequate but located with the device) giving a false sense of security
- Continuing old vulnerabilities such as poor password practice and exposure to attacks based on exploiting people's lack of awareness of risks (known as social engineering)

- Increasing levels of sophistication of malware and hacking activity making it possible for well protected enterprises to suffer data breaches

Most of the objects and techniques above can be used for beneficial or malign purposes. It is not possible for legislation to keep pace with this level of innovation on physical devices and ways of working which were not envisaged at time of legislation except at a high level of abstraction. Legislation needs to be device and media independent.

The technical complexity and cost for organisations to hold data securely against hackers and web-based malice is increasing all the time. It falls particularly heavily on small organisations with limited ICT expertise. Even large organisations can struggle to recruit and hold expertise. Loss from a small organisation can be qualitatively as harmful as that from large organisations. (Loss of medical records on a GPs surgery network could give rise to just as much harm as loss of records held by larger organisations.) As more data moves into smaller organisations the probability that it is fully protected declines.

The range of devices and the range of ways in which they can be configured to hold (or lose) data, together with the propensity of individuals to want to work flexibly, innovatively and to get round rules which they perceive as inhibiting them, would seem to call for more than a legal response. The drivers that exist to join up and examine data in new and fresh ways to gain competitive edge, to innovate or to provide better public service in effect all challenge the principle that data collected should only be used for the purposes for which it had been collected. Decisions taken in good faith by organisations to repurpose or share data (shopping preferences, Health Information, Money Laundering) could be interpreted as breaches of data subjects' rights. The substantive difference, from the subjects' perspective, would be that the breach arises from a conscious decision by a data holding organisation.

There are circumstances where a breach has occurred despite the fact that the original and proper controller of the data has taken reasonable steps to protect it and may be unaware of the breach, either because the theft has been disguised, or because an individual working for an organisation has ignored or circumvented controls.

Large scale information holdings may pose *qualitatively* different challenges including whether the operators of data centres really can account for every copy including those held on virtual machines or backup

tapes. If it were practically and theoretically impossible for an organisation to be able to categorically state that it knows exactly where every copy of all its sensitive data is, then its capacity to comply with the letter of existing or tighter legislation is open to question.

The rapid widespread growth of data holding devices poses challenges with 500 Gigabytes of storage being available for under €100. In effect these devices, many of them carrying significant personal information can become disposable. Existing data protection law and most commentary is focused on large organisations, public and private. The massive expansion in capacity poses communication challenges to individuals who are unwittingly exposing their own, their family and colleagues' information to substantial risk of misplacement.

Any proposed legislation would need to address the issues which arise where data is supplied by people who may not fully understand the implications of such mundane decisions as leaving cookies switched on or whose computers have been unwittingly infected (e.g. by a Trojan which copies any personal information it can locate). While much information exists on what is necessary to keep information on an ordinary Internet connected home computer private, it is well beyond the interests and capacity of most people to implement. Many technology oriented sites and advice fora assume a level of interest that is higher than that demonstrated by most people. The well documented rise of botnets (where hundreds of thousands of computers have been hijacked and are controlled, unknown to their owners, by criminals) relies on people not managing the security levels of the computers they own. This may be from lack of interest or lack of knowledge. The purpose of these hijackings is primarily to use them to deliver spam or targeted attacks but a side impact is that all the information on these computers is compromised.

A further challenge arises from the changing face of personal information holdings. Previously unrelated pieces of name and address information, shopping habits, location information, CCTV images, age profiles are accumulated by third and fourth parties.

The technical community would now accept that passwords are of limited use as protective mechanisms and there is a reliance on encryption. While it may be logistically difficult for a large organisation to encrypt all laptops and portable devices (and encryption is only as good as the care that is taken of the key) it is a bare minimum where personal data is being held on mobile devices of any sort. It roughly equates to locking the cashbox away. Unencrypted devices should not have sensitive data.

This precaution is now so basic and so well understood that it could form the basis for a symptomatic, risk-based enforcement approach. This would take forward recent practical developments in existing Data Protection powers in an innovative way. The underlying principle would be that if a sample of an organisation's devices were audited and found to be unencrypted and carrying sensitive information then there would be a probability that it's other Data Protection practices would be found to be deficient, which would trigger a more detailed audit. Some form of publication of the fact of an organisation having had a device audit and having passed or failed could produce a very strong result once there was a high probability that the organisation would face such an audit. Having a demonstrable certification that their devices are secure could well become a small but useful competitive advantage as organisations deal with a client base increasingly worried about the potential harm from lost data.

Regulatory Issues

It is difficult to establish the effectiveness of existing legislation in the context of data breach reporting either in Ireland or elsewhere. It can be argued that all breaches are fundamentally a breach of existing data protection principles and that existing law could be deployed to better effect.

There is a wide variety of reporting experienced internationally. It is not possible to say whether this is as a result of differences in regulation or differences in data holding practices. Some surveys have been done but it is questionable whether an organisation would publicly answer that it has had a significant breach but never reported it.

There are certainly mixed levels of awareness in organisations on their obligations under existing Irish legislation as illustrated in the submission by PricewaterhouseCoopers. Consequently there are varying levels of compliance. It is broadly in the interests of organisations holding data to hold it securely and not to allow breaches to happen. It may, however, also be in the interests of an organisation to share or exchange data with third and fourth parties and this can have unforeseen consequences. If penalties are to be introduced for data breaches arising from poor security and loss of data, it might seem to be an anomaly that there would not also be penalties introduced for cases where an organisation takes an active decision to release data contrary to the requirements of the data protection legislation and the subject disagrees with that decision, makes a complaint and has the complaint upheld.

There is no existing evidence of the role played by awareness of existing legislation where breaches have happened. Such evidence could show whether offenders knew the law but ignored it, or just didn't know that either they shouldn't have had the relevant data in the first place or should have protected it better. Ignorance of the law would not be a defence in a specific case. But if it were demonstrated that there was a widespread pleading of ignorance as cases arose, then targeted information raising campaigns could be useful.

In general, it would seem that a penalty-backed enforcement regime would be a fundamental change in the underlying principle of the existing law as it has been applied in Ireland to date other than in the telecommunications area. The practice of fines for breaches of existing law is widespread in

Spain where the use of administrative fines is part of mainstream administration. However the incidence of breach reporting there is comparatively low. It is not possible to say whether this is because organisations, in response to the regulatory regime, take better care of their data, or underreport to avoid fines.

We have been asked to blend the needs of a Regulatory Impact Assessment with the work of the Group. All proposed legislation should now be informed by such an Assessment which is best done at the earliest stage.

There is a general role of regulation in forming part of a national reputation. A country perceived to be correctly regulated would be positively viewed externally. It is likely that the most recently developed regulatory regimes across a number of areas of activity would have common features. In this context, a breach reporting regulation (whether by law or otherwise) should be an example of the sort of regulatory regime in place in the country as opposed to being separate from other sorts.

Any change in the regulatory regime will need to take account of the work of the High Level Group on Business Regulation led by the Department of Enterprise, Trade and Employment which is developing Risk Based enforcement policies to support the Government's strategy for economic recovery. Emerging policies include a consolidated inspections programme to reduce the number of inspection visits to business and a risk based assessment to minimise the burden on businesses.

An Impact Assessment of proposals to improve regulation on data breaches gives rise to a number of specific questions. These are discussed below:

How can we accurately determine whether the prevalence of the problem confirms the need for improved regulation? While the number of reports of breaches is increasing is there any evidence that the incidence of data breaches is increasing or reducing?

While there are many reports of data breaches (http://www.privacyrights.org/ar/ChronDataBreaches.htm) the meaning behind the data is not immediately clear. It is possible that the incidence is static or reducing while the reporting proportion is increasing. However the likelihood is that there are more breaches than previously and more than are reported. It is not possible to say whether there are more breaches as a proportion of data being held. Although the data is drawn from the USA,

the issues raised are likely to be more general. Consequently it seems that the existence of breach reporting legislation in the USA is raising awareness of the issue but not necessarily having the desired impact. It may be that there is a lag between the passage of legislation and its impact on organisations.

Is the current non legislative reporting expectation an effective method of regulation?

DPC have reported more organisations now choosing to report breaches to them as good practice and in their own interests. There are no recent instances where an organisation has contacted the DPC in the context of a breach and where the DPC has formed the view that the organisation should notify its clients but the organisation has declined to comply with the advice. Therefore, where organisations have come forward to DPC under existing guidelines there has been a subsequent notification to clients where the organisation or/and the DPC considered this to be justified. By definition, if organisations do not come forward, it is not possible to know for certain unless those unreported data losses subsequently become public because the data turns up. There is certainly a belief that there are more losses than are reported.

Any proposals for a changed regulatory regime would need to be structured to encourage *early* reporting. The reaction of an organisation which has discovered a breach and can approach the DPC with a view to establishing what needs to be done, including reporting to its customers may be different to the reaction of the same organisation faced with notifying the DPC and its customers and also a prosecution and substantial fine.

How is the public interest determined and accounted for when either the organisation itself, or the organisation in consultation with the DPC, are deciding whether or not to release details of a breach and what form the release should take?

It could be a calculation for a company to make that, unless the penalties were very stringent, they might run the risk of the lost data not turning up in any damaging way as the financial and reputational costs of disclosure are likely to be substantial, regardless of whether the lost data is ever misused. Even where a report is being made to the DPC under existing guidelines complex decisions need to be made on the probability of harm being done and the timing of a notification. Most organisations would, probably correctly, ultimately conclude that once they become aware of a loss of

data it is unlikely that the matter will remain private and it is in their interests to contact the DPC and/or an Garda Síochana at the earliest stage. There may be a need for a more formal liaison between these two organisations on what steps to take where, for example, there is a view that notification might hinder a line of enquiry. A speedy balance needs to be struck between the need for a successful apprehension of the culprits and the rights of potential victims to protect themselves.

The rationale for not prosecuting or for reducing a penalty where an organisation has voluntarily reported a breach is because early notification gives an opportunity to preempt any financial harm. Stolen data can be used in a matter of hours and there may not be much time for a prolonged consideration of the matter if notification is to be of use.

Any proposed regulation would need to be calibrated to impose a greater cost on non-reported breaches which subsequently come to light to help organisations to balance the reputational damage of being found out (if you have lost data but haven't owned up) against the reluctance to self-incriminate.

It would also be necessary for any proposed legislation, involving penalties, to address whether there was any relationship between the level of security in place and the damage done or whether any penalties imposed would be related to malpractice by the holding organisation. In the UK penalties are being introduced from next year but not for breaches specifically:

"Under the Data Protection Act (DPA) the ICO cannot issue fines for breaches of the eight data protection principles at the heart of the law. From next April that will change and it will be able to issue fines for knowing or reckless breaches of the Act's principles.

"The ICO has pressed strongly for monetary penalties where the Data Protection Act has been knowingly or recklessly breached. Penalties are being introduced next April, but are not yet in force," said an ICO statement.

A spokesman for the ICO said that it did not yet know how much it would be allowed to fine people and organisations, and that there was "some work still being done" on the fines.

The fines can be levied by the ICO when one of the eight principles have been seriously breached, but only if the ICO is convinced that the breach was deliberate or that the data controller knew, or ought to have known, of the contravention risk, and that the contravention would be likely to cause substantial damage or substantial distress and that

the controller failed to take action to stop it. ."
http://www.theregister.co.uk/2009/07/23/ico_fines/

Given the difference in rationale between data holdings by Public Service and Private sector organisations should there be a different response for each sector?

It may broadly seem that you are compelled to give your data to the Public Service but chose to give it to private sector organisations this is not really the case. Existing law does not distinguish between private and public sectors and it is unlikely that breach reporting legislation could or should.

What are the consequences of increased regulation in terms of cost of compliance?

The costs which may arise as a result of a breach (apart from reputational cost) include cost of notification, cost of indemnifying against damage done to clients, legal costs should civil actions or prosecutions ensue and cost of a fine if provided for in legislation. These costs would arise directly to organisations should they cause or suffer a breach. Indirect costs would arise for tax payers in any increased cost of administration and enforcement which would arise. Indirect costs might also arise if organisations enforcing a tighter information security regime tried to pass the cost on to clients. However the costs would be difficult to isolate and it would be difficult to justify a cost incurred for doing something the client is entitled to in any case – keeping personal information safe.

Regulation or legislation which would provide for mandatory disclosure , however it is brought in (pre or post EU directive, directly to the data subject or via the Data Protection Commissioner) will certainly add some cost to the activities of those who comply. Given the variety in scale and scope of data holdings and potential mechanisms for breach it is not possible to make calculations of costs of compliance with various options in a useful way. Organisations who are adhering to the Data Protection principle of holding data securely will, in any case also be incurring a data security cost.

This cost is incurred whether breaches occur or not. It is broadly equivalent to having an adequate insurance policy. Some organisations offer Data Loss insurance policies and as awareness of the risks to organisations of data loss is raised these policies are likely to become more prevalent. They would presumably only be paid out where the relevant data loss prevention practices were verifiably in place. A media report on data

breach protection insurance is available at:
http://www.americanbanker.com/btn_article.html?id=20070525TLBOP8OV

The cost of data loss prevention is likely to be the same in any economy, the cost of a data breach notification is also likely to be broadly the same. The elements under the control of the state are the costs of administering any regulatory infrastructure and the levels of any penalties.

If the core concern is to reduce the potential for harm to be done to individuals by lost data, is the expectation that large organisations should incur the cost of tighter information security controls but that smaller companies, clubs or individuals are exempt, valid? Is this expectation capable of being expressed in legislation? Once harm or apprehension of harm, due to unauthorized or careless release of data, is conceived as a core issue how can the relevance of who has released the data or how it was released be taken into account in legislation?

Laws, Policies and how they are implemented.

While it is straightforward to state a policy that an organisation does not allow use of devices such as USB drives there is a technical knowledge and cost threshold for organisations who decide to actually lock down access to enforce the policy. There is little value in having a policy without putting in place the capacity to enforce it. Those stating the policy may not have a full understanding of what is needed to comply. They may be relying on people to implement the policy who may not have a full understanding of the legal and reputational issues involved. Although working in a technical environment they may lack adequate information or skills to address all the challenges they face. Where companies do come to report breaches it is clear that there is a variation in understanding within the companies concerned of the technical issues or their capacity to address them. In an attempt to bridge this gap in the UK, the Information Commissioners Office promotes a CEO level promise:

"The ICO is urging heads of organisations and government departments to sign up to the Personal Information Promise. The Promise lists a number of key commitments that senior figures will make on behalf of their organisation to protect the personal information they are entrusted with."

A data-loss prevention policy requires people to actively do complex things as well as refrain from doing things which can seem harmless. A powerful behavioral change may be needed to bring this about to overcome the

natural self-protective first response to a discovered breach. The organisation and the individuals working for it need to really comprehend that the full economic cost (direct financial costs, reputational costs including lost customers, potentially fines) of data loss is greater than the benefits to be derived from the perception that data is there to be mined and used to their individual and organisational advantage, before there is a sustained behavioral change.

Fines and reputational damage at corporate level do not necessarily permeate the culture of an organisation unless consequences are seen to flow to responsible individuals. To reduce the prospect of harm being done needs an organisation, its employees and contractors to have a mainstream understanding of the problem linked in to other organisation policies.

A significant feature in the recent history of computing and networks can be said to be founded on individuals inside organisations and self educated enthusiasts using the invention of the PC to circumvent the rigorous controls which existed in the earlier mainframe and midrange environments. There is a continuing dichotomy between corporations wishing to centralise and control data and individuals wanting to use new tools to personalise their work experience.

Companies face increasing economic drivers to gather and hold more information to give them a business edge and access to a cheaply gathered, easily harvested resource. There are many examples where data is collected completely unknown to the data subject or known to them but where they may have no understanding of the uses to which it is being put. (CCTV footage, material gathered from disadvantaged such as functionally illiterate people). Organisations are also driven to join up the disparate data they have on individuals to give them an overview of their clients. Organisations may also need to gather, hold and share data for regulatory purposes. This is augmented by how easy it is now to gather data and how willing people are to hand it over. Within organisations there can be the simple human curiosity factor at play which can cause chunks of organisational data to be broken off and used in (potentially malicious) ways unforeseen by the hierarchy. As the internet evolves towards the more collaborative Web 2.0 there is a further push towards removing boundaries and connecting previously unrelated holdings to give a "whole of customer" view. These behaviors aren't particularly new but the supporting technology is and there is certainly a powerful challenge to the successful protection of privacy. Information is easier to lose than to hold, easier to share than to keep private.

Organisations need to understand not only the importance of not losing their clients data but how to make sure, using whatever mix of encouragement and sanction they use for other policies, that their employees and agents understand and carry out their obligations. In challenging times data security can be seen as a cost which does not contribute to income.

Communicating Risk: Data equals Money

It is unlikely that statistics and risk analyses will challenge either corporate or individual behaviour on their own as repeated publication of factual information is unlikely to influence the levels of fears about any given risk. Improved regulation, whether by transposed directive, new primary legislation or codes of practice will support behavioural change but the real challenge is likely to be a communications one.

To change behaviours it is necessary to change feelings rather than purely addressing the conscious mind (Slovic, Gazzaniga quoted in "Risk, the Science and Politics of Fear" by Dan Gardner). Research is showing that people don't analyze risk in a conscious thoughtful way but analyse risk and benefit as if they were the relevant alternatives. (http://en.wikipedia.org/wiki/Affect_heuristic). In our current context both data holders and data subjects may well be underestimating the risks of providing data to be held (or trusting the IT people to look after it) as they have a general view of the good that comes from handing over the data.

The growth in volumes of information being held is outside the scope of anything in history and is difficult to get a comprehension of the quantities involved and for our brains' internal risk assessment calculations to adjust.

("At 487 billion gigabytes, if the world's rapidly-expanding digital content were printed and bound into books it would form a stack that would stretch from Earth to Pluto 10 times. As more people join the digital tribe – increasingly through internet-enabled mobile phones – the world's digital output is increasing at such a rate that those stacks of books are rising quicker than Nasa's fastest rocket… The digital universe is expected to double in size over the next 18 months"
http://www.irishtimes.com/newspaper/frontpage/2009/0519/1224246881481.html).

It seems that this particular topic is one where there is a degree of disconnect between fears expressed about breaches and the day to day behaviour of handing over personal information to data holders. There is also some disconnect between organisations' statements of policy and practice on the ground.

One line of approach would be to actively promote the equation of sensitive personal information records with money. From the individual's perspective they should be reluctant to hand personal information over to strangers unless they know what they are handing it over for and whether and how it will be stored and used and how and when they can have it back.

From the organisations' perspective the narrative equating money with sensitive personal information would be different. What happens if a substantial six figure bank draft belonging to the organisation is left openly on a desktop, in the boot of a car, on a park bench, on a train, in the pub? The consequences would be clear in most organisations: for the individual and for whatever governance arrangements left the individual in possession of the draft.

Less clear and more defensible from the organisations' perspective would be the situation where well resourced and intelligent raiders defeat your reasonable defences. In this case the individual employee may be in the clear but the higher levels of the organisation may still be culpable if they haven't been keeping up to date with what constitutes a reasonable defence.

In either case the money is gone. The analogy breaks down when you attempt to work out in what way the harm done to the individual owner of the lost data (and to the company) is different.

As things are now, the consequences are well communicated in the money example (the money has been lost either directly by the individual or by the company's shareholders and they will be consulting their insurance policy. All problems and costs accrue to the company). It is much less clear in the data loss example (data belongs to the subjects and problems and costs accrue both to the organisation and to the individual). In the money example, it is also accepted that regardless of the legislation and organisational protections being in place, both organised and opportunistic thefts will happen. However, tighter regulation can be shown to have reduced the incidence of, for example, cash in transit robberies.

Regardless of what improved regulatory regime is in place, the volume and value of data being held guarantees that there will continue to be data losses and data thefts. What is the best mix of regulatory responses to reduce the risk and encourage the best response when things do go wrong?

In cases where breaches have occurred, in Ireland or elsewhere, it is not clear whether, notwithstanding organisations' policy or training programmes, the people who have been primarily responsible have been aware of their obligations, or any penalties. There is some evidence that within organisations, just as where access to money is concerned, those with privileged access are sometimes prone to temptation and in more recent times there are reports that people leaving employment are taking corporate information with them. http://www.ponemon.org/blog/post/more-employees-ignoring-data-security-policies

Threshold of Harm

In certain contexts, a single record going astray can cause substantial harm. Harm can be objective (financial) or subjective. As an example, bullying is generally accepted to have happened if a person feels bullied. An equivalent situation may be individuals feeling themselves to have been damaged by a data breach even if the data never gets to individuals it shouldn't or if no objective harm has occurred. These sorts of harms can be addressed by tort legislation but there are few relevant cases.

In establishing a reporting obligation and potentially giving a decision making authority to the DPC on whether a particular breach is serious enough to be reported, how can the threshold of harm be established to allow a rational decision to be taken? In this context the decision needs to be rapid and the frequency of reporting should not be such as to overwhelm the resource of the DPC or to put that office in the position of being a bottleneck on timely reporting. Is there an identifiable minimum data set, which if lost, would trigger a report? Is there any way to establish a number of records which would trigger a report? Perhaps formal guidance under existing legislation could be issued. In a recent example, a small number of sensitive health records were lost on an unencrypted HSE laptop which would have fallen under any suggested numerical threshold but where notification was required. In making these calculations what objective mechanism can be used to assess whether the disclosure of the loss by the data holder to its clients may itself cause distress?

Options

Broadly there are a range of regulatory options available as set out in the table below. Two aspects worth particular attention are how a threshold would be determined and the level of penalty, if any, where penalty refers to a fine imposed by either a court or the DPC over and above any costs incurred arising from mandatory reporting. No fine, or too small a fine, runs the risk of changing the existing relationship but being ignored in the calculation on whether or not to disclose. Much more substantial fines will certainly focus attention but would need to be proportionate to the severity of the breaches.

Regulatory Option	Pro	Con
1. No further development of the existing DPC Guidelines pending new EU directive.	De facto many organisations who lose data are now contacting DPC/Gardai No recent example of organisation advised by DPC to report loss to customers refusing to do so Organisations making reports incur costs which are directly related to the scale of their breach Does not add any new regulatory burden Allows for emergence of EU level directive and avoids double legislation Keeps existing encouragement, educative approach	Reporting is not mandatory and has no statutory basis In principle, breaches of duty should attract penalty EU directive may not emerge in timely fashion
2. Further Develop Code of Conduct and awareness campaign under existing legislation (e.g. commission risk based audit of organisations' devices and publish results; increased levels of information on costs of data loss,	Keeps focus on fundamental Data Protection principles rather than on specifics Treats visible symptom (lost data) as indicator of underlying poor practice Increase awareness of existing legislation	Focussing on only one symptom Does not introduce penalties for offenders No specific penalty apart from reputational cost to organisation of failing an audit and cost of subsequent more detailed audit

develop guidance on thresholds)	Limited additional regulation cost Flexible and in line with emerging National regulatory approach – serious breaches could, in risk based evaluation flag up attention of other regulatory bodies Allows for emergence of EU level directive and avoids double legislation	Additional cost of increased audit activity may need to be offset by reduced activity in other areas. Cost of awareness raising activities
3. Legislate for penalties for very serious contraventions of the Data Protection Acts, with failure to report significant data breaches to the DPC and to data subjects being considered as aggravating factors in a contravention of the data security provisions of the Acts	Model being implemented in the UK, following consideration of different options Keeps the focus on overall compliance with the DPA rather than focusing on only one aspect Responds to a more general demand that serious contraventions of the DPA should attract penalties and that failure to have such penalties can lead to a relative neglect of data protection within an organization Would encourage DPC to only use penalty	Penalty provisions could encourage a less cooperative approach between data controllers and the DPC Danger that DPC could be pressurised into using penalty provisions in inappropriate cases e.g. in response to manufactured media outrage Relies on organisations to decide on reporting thresholds More legal costs

	powers for the most serious breaches Would eliminate the anomaly of penalties for relatively minor breaches of the *e*Privacy Regulations but no penalties for even the most serious breaches of the DPA	

4. Legislate for mandatory reporting to DPC for data breaches with penalties for serious breaches or failure to report or both. DPC decides on whether and how to notify	Would introduce penalties into Data Protection legislation and improve levels of protection Place stronger onus on data holders controllers to comply with Data Protection Principles Would improve general levels of data security Would cover all potential breaches equally – without threshold every incident would call for a report. DPC role would allow for consistency of decision making and help avoid overreporting to data subjects Provides more direct legislative support for DPC guidelines	Changes legislation from cooperative, educative to penalising. Difficult to have penalties for one aspect of data protection failure but not for any other. Introduces additional business cost (but only for those who breach – the cost of any penalty.) Potential for overreporting if people are in receipt of multiple notifications Penalties would require prosecutions where convictions may be difficult to secure unless a system of administrative penalties imposed by the DPC were introduced. May not be in line with new EU directive Could overwhelm resources of DPC and result in reduced timeliness of notification to data subjects
5. Legislate for	As for 4 but would	As for 4.

mandatory reporting to DPC above defined threshold with penalties for serious breaches or failure to report or both	focus on large scale breaches, either in terms of numbers of records, severity of breach or range of information lost, Reduce danger of over reporting and associated report fatigue Legislative support for existing ad hoc arrangement where organisations are increasingly approaching the DPC and being advised to notify data subjects.	Objective threshold difficult to establish. Judgement and complex decision required in a very short space of time Additional resources needed for DPC to allow timely discharge of function
6. Mandatory simultaneous reporting to DPC and to data subjects all breaches.	As for 4. Eliminates any time delay in DPC reaching a decision to report or not report and improves chance of data subject to effectively take precautions. Affirms primary relationship is between data subject and data holder. Leaves the client the choice of how to react. DPC can subsequently follow through seeking penalties for breach	As for 4. "Crying wolf" danger of overreporting Potentially heavy cost on business disproportionate to businesses operating in other EU jurisdictions Primary decision on what constitutes a breach remains with data controller

7. Mandatory simultaneous notification to DPC and to data subjects all breaches above threshold	As for 5. Helps reduce overrreporting if threshold is consistently defined and applied Guidance could be given from DPC on how thresholds would apply. Organisations could rely on having complied with these guidelines if challenged. Follows new German model	Difficulty of defining objective threshold. Introduces a potential delay while organisation considers whether notification is necessary
8. Mandatory reporting directly to data subjects all breaches, penalties for failure to report	Most closely follow US model Affirms primacy of data subject's role Low administrative cost for the state Organisations may be tempted to weigh likely penalty against known cost of report	Danger of overreporting Reduces educative, guidance role of DPC Moves away from current EU mainstream Relies on organisations alone to decide on thresholds More legal costs

Submissions

The options and questions as set out are intended to assist in shaping discussion and feedback. Comments need no be limited to these specific options and questions.

Submissions can be emailed to:

dataprotectionreview@justice.ie

or posted to:

The Secretary

Data Protection Review Group

Department of Justice Equality and Law Reform

Pinebrook House

71-74 Harcourt Street

Dublin 2

Appendix 1

Submissions Received by September 2009

Pricewaterhousecoopers

Irish Banking Federation

BH Consulting - Brian Honan

Digital Rights Ireland

Sam Johnston, Certified Information Systems Security Professional

Trust Ireland

4 Private Citizens

1 Legal References

Irish Legislation

Material extracted from Data Protection Commissioners site:

LAW ON DATA PROTECTION

Data Protection Acts
The main Irish law dealing with data protection is the Data Protection Act 1988. The 1988 Act was amended by the Data Protection (Amendment) Act 2003. An informal consolidated version of the two Acts is available.

The 2003 Amendment Act brought our law into line with the EU Data Protection Directive 95/46/EC.

All Sections of the Acts are in force, except Section 4 (13) (enforced subject access).

Electronic Privacy Regulations
The ePrivacy Regulations 2003 (S.I. 535) deal with data protection for phone, e-mail, SMS and Internet use. They give effect to the EU e Privacy Directive 2002/58/EC. These regulations have been amended by SI 526 of 2008.
SI 192 of 2002 – which has been replaced by SI 535 – is available for reference.

Regulations under the Data Protection Acts
Fees
S.I. 658 of 2007 - The fee you must pay for Registration and for Prior Checking
S.I. 347 of 1988 - The fee that an organisation may charge you for an Access Request(€6.35) and the fee for a certified copy of a Register entry (€2.54)

Registration
S.I. 657 of 2007 - Who must register
S.I. 351 of 1988 - Registration Forms
S.I. 350 of 1988 - Period of Registration (1 year)

Restrictions on Right of Access
S.I. 82 of 1989 - Health data
S.I. 83 of 1989 - Social Work data
S.I. 95 of 1993 - Functions of the Financial Regulator and of the Consumer Agency. Various functions performed by auditors etc under the Companies Acts

S.I. 81 of 1989 - Information on adopted children and information the Public Service Ombudsman gets during an investigation

Prior Checking of Processing

S.I. 687 of 2007 - Processing of genetic data in connection with employment

Other Laws
Cross-Border Bodies
British-Irish Agreement Act, 1999, Section 51 - Data protection in cross-border bodies

Fine Gael Private Members Bill

http://www.oir.ie/viewdoc.asp?DocID=10087&&CatID=59&StartDate=01%20January%202008&OrderAscending=0

EU developments
Data Breach Notification Laws in Europe Privacy Laws & Business: survey on attitudes of 21 European National Data Protection Authorities
www.privacylaws.com

Current Status of Proposal for ePrivacy Directive
http://www.europarl.europa.eu/oeil/file.jsp?id=5563642

" Security of processing and protection of personal data: the text stipulates that the provisions of this directive particularise and complement Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

Without prejudice to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the measures taken in this area shall at least:

- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure;
- ensure the implementation of a security policy with respect to the processing of personal data.

When the personal data breach is likely to adversely affect the personal data and privacy of a subscriber or an individual, the provider shall also **notify the subscriber or individual of the breach without undue delay**. If the provider

has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and those measures were applied to the data concerned by the security breach.

Providers shall maintain **an inventory** of personal data breaches, comprising the facts surrounding such breaches, their effects and the remedial action taken. "

Second Opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.
http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf

Review of Data Protection Directive By UK Information Commissioner
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf

ePrivacy Directive: Information Note from DPC

During the negotiations on the Telecom Reform package, the European Parliament and the Council had achieved a compromise on all three elements of the package: the Better Regulation Directive, the Citizen's Rights Directive (which includes the amendments to the ePrivacy Directive) and the regulation establishing the Body of European regulators for electronic communications (BEREC). On 6 May, the European Parliament plenary voted on the compromise texts. The texts on the Citizens' Rights Directive and on BEREC were accepted as agreed with the Council; however, on the Better Regulation Directive the EP plenary deviated from the negotiation result and accepted one amendment which was not agreed with the Council.

As a consequence, the intended agreement in second reading has not been reached, and the Council has now to decide on its reaction to the EP vote. If the Council does not accept the EP position as it stands, the Treaty provides for a conciliation procedure during which the institutions may negotiate on a sustainable compromise. This conciliation procedure is executed under strict time limits, which start from the point in time when

the EP formally submits its approved text to the Council. This has not happened yet.

On 11 June, the Council held an informal discussion on the state of play of the Telecom Package. In its subsequent press release, the Presidency announced the Council's intention to adopt the three proposals of the package as soon as possible. It further said that "The Council is ready to work towards a solution of this last outstanding problem and looks forward to working with the newly appointed European Parliament during conciliation."

It is expected that negotiations will start in September.

The text adopted by the EP for the Citizens' Rights Directive can be consulted at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN&language=EN#BKMD-14

Commission of the European Communities, Review of the EU Regulatory Framework for electronic communications networks and services', June 2006, p30, available at http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf

Extract from European Data Protection Supervisors views on development on ePrivacy directive.

On 13 November 2007, the European Commission adopted a Proposal amending, among others, the Directive on privacy and electronic communications, usually referred to as the ePrivacy Directive[1] (hereinafter "**Proposal**" or "**Commission's Proposal**"). On 10 April 2008, the EDPS adopted an Opinion on the Commission's Proposal where he provided recommendations to improve the Proposal in an attempt to help ensure that the proposed changes resulted in the best possible protection of the privacy and personal data of individuals ("**EDPS First Opinion**")[2].

2. The EDPS welcomed the Commission's proposed creation of a mandatory security breach notification system requiring companies to notify individuals when their personal data have been compromised. Furthermore, he also praised the new provision enabling legal persons (*e.g.* consumer associations and Internet service providers) to take action against spammers to further supplement existing tools to fight spam.

3. During the Parliamentary discussions that preceded the European Parliament's first reading, the EDPS provided further advice by issuing comments on selected issues that arose in the reports drafted by the European Parliament committees competent for reviewing the Universal Service[3] and ePrivacy Directives ("**Comments**")[4]. The Comments primarily addressed issues related to the processing of traffic data and the protection of intellectual property rights.

4. On 24 September 2008, the European Parliament ("**EP**") adopted a legislative resolution on the ePrivacy Directive ("**first reading**")[5]. The EDPS viewed positively several of the EP amendments that were adopted following the EDPS Opinion and Comments mentioned above. Among the important changes was the inclusion of information society service providers *(i.e.* companies operating on the Internet) under the scope of the obligation to notify security breaches. The EDPS also welcomed the amendment enabling legal and natural persons to file actions for infringement of any provision of the ePrivacy Directive (not only for violation of the spam provisions as initially proposed by the Commission's Proposal). The Parliament's first reading was followed by the Commission's adoption of an amended proposal on the ePrivacy Directive .

FREQUENTLY ASKED QUESTIONS RELATING TO
TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES
http://ec.europa.eu/justice_home/fsj/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

House of Lords Report: www.official-documents.gov.uk/document/cm72/7234/7234.pdf

Australia

http://www.privacy.gov.au/publications/submissions/alrc/c11.html#L24947 "Office generally supports consideration of the addition of provisions to the Privacy Act to require agencies and organisations to advise affected individuals of a breach to their personal information in certain circumstances. Notification in a timely manner would enable individuals to take any necessary steps to protect their personal information.

128. Such a change to the Privacy Act to require the reporting of information security breaches would provide a strong market incentive to organisations to adequately secure databases and information repositories to avoid the potential brand damage arising from negative publicity….. that 'mandatory reporting' legislation remains a new and evolving concept that requires further research. "

New Zealand

http://www.caslon.com.au/privacyguide5.htm

http://privacy.org.nz/assets/Files/Privacy-Breach-Guidelines/Privacy-breach-guidance.DOC

"Notification can be an important mitigation strategy that has the potential to benefit both the agency and the individuals affected by the breach. If a privacy breach creates a risk of harm to the individual, those affected should be notified. Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves."

Canada

Approaches to Security Breach Notification: A White Paper, 9 January 2007 available at http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-print.pdf

http://www.theregister.co.uk/2009/07/21/canada_castigates_facebook/ "Facebook does not protect personal information well enough to comply with Canadian data protection law, the Canadian Privacy Commissioner has said."

USA

Congressional report on Breach notification laws http://opencrs.com/document/RL34120

2 Technical references

As computation continues to move into the cloud, the computing platform of interest no longer resembles a pizza box or a refrigerator, but a warehouse full of computers. These new large datacenters are quite different from traditional hosting facilities of earlier times and cannot be viewed simply as a collection of co-located servers. Large portions of the hardware and software resources in these facilities must work in concert to efficiently deliver good levels of Internet service performance, something that can only be achieved by a holistic approach to their design and deployment. In other words, we must treat the datacenter itself as one massive warehouse-scale computer (WSC).
http://www.morganclaypool.com/doi/abs/10.2200/S00193ED1V01Y200905CAC006

The IT environment has changed significantly in a few short years, as several factors have dictated the need for a more robust approach to corporate security policies, including:

1. A trend towards mobility of information,
2. Theft of IT assets arising from a proliferation of mobile devices,
3. Increasing data privacy and data security concerns, and
4. Regulatory compliance mandated by recent legislation.

These factors have made it necessary for network administrators to design and implement comprehensive security policies to keep pace with the changing IT landscape. Effective solutions for these multifaceted problems require a layered approach comprised of products, policies and procedures that can work in concert to provide organizations with the broadest security blanket available.

There is a strong relationship between the issues of compliance, data protection and theft recovery. Organizations must take this into account when defining security policies. It is no longer enough to attempt to address compliance issues without addressing data protection. Protection of data on mobile and remote computers requires an understanding of the issues surrounding computer theft
http://www.webbuyersguide.com/resource/white-paper/11429/Laptop-Security-Compliance-Protection-and-Recovery

Is your system infected with a backdoor trojan, or remote access trojan? Maybe you received a warning from your antivirus, antispyware application, or someone helping you? What is a backdoor trojan, and why should you be concerned?
http://www.geekstogo.com/2007/10/03/what-is-a-backdoor-trojan/

US Federal Government skill shortage

http://www.theregister.co.uk/2009/07/22/federal_cybersecurity_shortage/

Internet Security Threat Report

The Symantec Internet Security Threat Report offers analysis and discussion of threat activity over a one-year period. It covers Internet threat activities, vulnerabilities, malicious code, phishing, spam and security risks as well as future trends. The fourteenth version of the report, released April 14, 2009, is now available.
http://www.symantec.com/business/theme.jsp?themeid=threatreport

http://www.guardian.co.uk/technology/2009/jul/15/hacking-usa "A recent wave of cyber attacks that crippled thousands of computers and websites in the United States and South Korea could have originated from inside Britain, experts have warned.

According to security researchers in Vietnam, the source of last week's string of attacks by the Mydoom virus - which overwhelmed systems belonging to the US Treasury and the office of the South Korean president Lee Myung-Bak - can be traced to the UK.

"We have analysed the malware pattern that we received" said Nguyen Minh Duc, a director of Vietnamese security company BKIS, in a post on the company's blog. "We found a master server located in the UK."

Investigators said they had discovered new details on how the strikes took place by investigating and tracing back the attacks.

According to BKIS, infected computers had tried to contact one of eight so-called command and control servers every three minutes. These machines then gave instructions to the hacked PC - generally ordering them to direct traffic straight at victim websites, in attempt to overload them and force them to crash.

But these eight servers were themselves being controlled by a single source, which evidence indicated was located somewhere in Britain."

http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf "Your Botnet is My Botnet: Analysis of a Botnet Takeover .....Once infected with a bot, the victim host will join a botnet, which is a network of compromised machines that are under the control of a malicious entity, typically referred to as the botmaster. Botnets are the primary means for cyber criminals to carry out their nefarious tasks, such as sending spam mails [30], launching denial-of-service attacks [24], or stealing personal data such as mail accounts or bank credentials [14,32]. This reflects the shift from an environment in which malware was developed for fun to the current situation, where malware is spread for financial profit.

http://www.wired.com/science/discoveries/magazine/16-07/pb_theory "The Petabyte Age is different because more is different. Kilobytes were stored on floppy disks. Megabytes were stored on hard disks. Terabytes were stored in disk arrays. Petabytes are stored

in the cloud. As we moved along that progression, we went from the folder analogy to the file cabinet analogy to the library analogy to — well, at petabytes we ran out of organizational analogies."

http://www.theregister.co.uk/2008/11/10/sys_man_virt_cash/ "In some ways, virtual server sprawl is much worse than the physical server sprawl from the turn of the last millennium. At least with real servers, there is some physical limit - the size of the data center and the power delivered to it - that puts a limit on the number of machines system administrators create.

http://secunia.com/blog/58/ "Adobe Insecure / Unpatched Version From Official Site"

http://whitepapers.windowsecurity.com/whitepaper3127/ overview : As attitudes to work and information continue to evolve away from those of the past, organizations are become more aware of the acute need to control the information that flows into, through and out of their networks. This paper demonstrates the need for a high-profile acceptable use policy to prevent data leakage, gives practical guidance on how to use current investments in IT security technologies at the gateway and endpoint to support this policy, and describes where new investment should realistically be made

Extract from sales material from one security solution vendor:

" Attacks are typically targeting internal user systems within the corporate network, using invisible "Web-borne" techniques to take control.
With the necessary tools readily available on the Internet, gaining remote access to an internal workstation only requires determination from the cybercriminal. It only takes a few hours for the criminal to stealthily gain access and take control of the critical internal business systems and data of a company and use them for profit.

Organized crime cells are especially focused on infiltrating businesses and personal computers, using the services of highly-skilled professional Crimeware writers.
These crime pros need little time to access the personal information and data of the end-user. This of course significantly increases the security risk and thus places a huge burden on security experts. They use the Web as their main vector for malicious code propagation, since they understand that signature-based solutions were not designed to counter code obfuscation, Web 2.0 platforms and technologies, and other dynamic attack vectors in today's web scenario. "
http://www.wickhill.com/products/finjan/solutions/uk_index.php

Ebook- How to Secure Windows and Your Privacy. This open source ebook tells Windows users how to secure their computer and their privacy.
http://downloads.zdnet.com/abstract.aspx?docid=832667

IT managers are "grossly underestimating" the explosion of unstructured data in the enterprise, according to Hewlett Packard. HP published new research carried out by Coleman Parkes Research, which surveyed more than 1,020 CIOs and department heads of large enterprise organisations across the UK and Europe. It found that on average, European companies believe than only 25 percent of their data is currently unstructured (ie emails, Word documents, third-party files). UK companies estimated that 29.4 percent of their data is in an unstructured format. This, says HP, is in stark contrast to research from industry analysts that indicate more than 70 percent of information is actually unstructured data. "Unstructured data is the 'dark matter' (ie the missing factor) of enterprise information http://www.pcworld.com/businesscenter/article/153558/unstructured_data_grows_unchecked_study_says.html

Sales material from vendor of cloud data holding: "Access all your backed-up data anytime from any Internet connection anywhere… Wherever there's an internet connection, you're a click away from any of your backed-up data. Just think of the convenience. " And the risk?
http://www.datadepositbox.com/index.php/data-backup-features

"Software restore forgotten user login password reveal asterisks ** character"**
Brothersoft Editor: Data doctor hidden password unmask utility decode any typed key board character in asterisks form **** of password text box. Recovery software is easy to use, free of cost, user friendly password reveal utility

http://www.pebbleandavalanche.com/weblog?-quiet=1;page=45 **"**A devoted corps of companies pursues your data wherever you go, and they care nothing about your privacy. To coin a phrase, let's call them the *datarazzi*."

Vendor white paper on strategies to prevent Data Loss.
http://i.zdnet.com/whitepapers/Varonis_WhitePaper_10_Imperatives_for_Preventing_Data_Loss.pdf

http://www.lloyds.com/News_Centre/Features_from_Lloyds/Industry_wakes_up_to_data_loss_risk_07122007.htm *:* "specialist insurance products can mitigate the financial cost of any loss. E&O insurance provides cover for data loss as a result of negligence and is available from various Lloyd's syndicates, according to Cooper. Companies can also take out a 'cyber liability'

policy to cover defence costs and class actions from customers following a deliberate attack and these are also available from Lloyd's, he says.

Lloyd's broker Safeonline also arranges cover for small businesses and large corporations relating to data loss as a result of hacking, a virus attack or the theft of physical media.

"Awareness of the risks associated with holding customers' data has grown tremendously as a result of incidents like those at Nationwide and TJX," says Chris Cotterell, Safeonline partner.

Policies brokered by Safeonline include coverage for costs relating to reconstituting lost data and also the costs relating to third party claims following a breach of security. Policies also provide cover for the cost of notifying people about the incident and the legal costs involved in regulatory proceedings resulting from an incident.

Lloyd's insurers ACE, Novae and Beazley all write data loss related cover. A medium sized corporation can typically arrange cover with a limit of £25 million, though a programme of between £50 million and £100 million is possible in certain circumstances, Mr Cotterell says."

http://www.lctjournal.washington.edu/Vol1/a006Bodden.html : "the business will look to its liability insurance for protection. <2> However, businesses that are expecting coverage under their Commercial General Liability ("CGL") policy may be in for a rude surprise. "

http://www.ponemon.org/blog/post/more-employees-ignoring-data-security-policies Employees routinely engage in activities that put sensitive data at risk. They are downloading data onto unsecured mobile devices (61%), sharing passwords (47%), losing data-bearing devices (43%), and turning off their mobile devices' security tools (21%). And, reflective of the blurring of the lines between personal and professional lives, they are using web-based personal email in the office (52%), downloading Internet software onto an employer's devices (53%), and engaging in online social networking while in the workplace (31%).

http://news.sky.com/skynews/Home/UK-News/Sky-News-Undercover-Laptop-Investigation-Repair-Shops-Caught-Hacking-Into-Personal-Files/Article/200907315343387?lpos=UK_News_News_Your_Way_Region_5&lid=NewsYourWay_ARTICLE_15343387_Sky_News_Undercover_Laptop_Inve Some computer repair shops are illegally accessing personal data on customers' hard drives - and even trying to hack their bank accounts, a Sky News investigation has found.

http://europeanjournal.typepad.com/my_weblog/2009/07/the-edps-raises-privacy-concerns-over-the-intelligent-transport-systems.html "The EDPS raises privacy concerns over the intelligent transport systems… The Commission believes that the deployment of ITS in Europe will serve different Community objectives such as cleaner transport, transport efficiency, improving safety and security. ….However, according to the EDPS, the Commission's proposal is "***too broad and general to adequately address the privacy and data protection concerns"***

3 Regulatory references

Better Regulation Website. Welcome to Better Regulation

The aim of this website is to provide information on Better Regulation - an important part of the Government's drive for greater economic competitiveness and modernisation of the Public Service. **http://www.betterregulation.ie/eng/**

Revised Regulatory Impact Analysis (RIA) Guidelines have now been published. These revised Guidelines take into account the recommendations from the Report on the Review of the Operation of RIA which was published in July 2008.

Risk Based Enforcement

Summary of work of High Level Group on Business Regulation:

"One of the five Action Areas in the Government's strategy for economic recovery, *Building Ireland's Smart Economy*, is Efficient and Effective Public Services and Smart Regulation. The strategy states that "A consolidated inspections programme will be developed to reduce the number of inspection visits to business"; also that "Enforcement should be based on risk so as to minimise the burden on citizens and businesses."

The High Level Group on Business Regulation is seeking ways to reduce administrative costs on business. The European Commission has found that cooperation with audits & inspection by public authorities, including maintenance of appropriate records accounts for more than half of all administrative costs, as measured in their cross-Community measurement exercise. In the UK, the Hampton Review of 2005[1] argues that pursuing a strictly risk-based approach to inspection and enforcement has the potential both to reduce administrative burdens on business and result in efficiency improvements in the Government sector."

Key Points about Risk Based Enforcement

The principle is that enforcement should aim to increase regulatory compliance in the most efficient and effective manner possible, given the limited resources available. Also that this should be done in such a way as to eliminate unnecessary administrative burdens in the economy.

In order to achieve this, enforcement should be based on an assessment of risk. "The fundamental principle of risk assessment is that scarce resources should not be used to inspect or require data from businesses that are low-risk, either because the work they do is inherently safe, or because their systems for managing the regulatory risk are good."[6]

Risk assessment should use all available good quality data. Resulting enforcement activity should follow directly from this assessment. This means that inspections should be targeted where risk is greatest. In cases of low risk, advice and support may be sufficient to ensure compliance. In cases of persistent non-compliance, however, sanctions currently in place may not be sufficient to deter this behaviour, and may need to be reviewed.

The cost to businesses of providing information and undergoing inspections should be weighed against the benefits deriving from this activity. In particular, the administrative burden imposed by regulators should be proportional to the risk associated with non-compliance. In practice, this may mean requiring less risky businesses to provide less information, for example.

Enforcement should always include a small element of random inspection. It should also be dynamic in the sense that it responds to the best information available to regulators. The enforcement activities of different bodies should not overlap in a potentially confusing or duplicative manner.

The **Financial Services Authority** has fined HSBC £3m for failing to properly look after its customers' information and private data.

These failures to follow proper processes led to at least two losses of customer data.

The FSA investigated the bank and found unencrypted customer details on open shelves and unlocked cabinets. Customer details were also sent via the post or couriers to third parties
http://www.theregister.co.uk/2009/07/22/fsa_hsbc_data_loss/

http://www.ico.gov.uk/upload/documents/pressreleases/2009/amicus_legal_undertaking_press_release.pdf : "The Information Commissioner's Office (ICO) has found Amicus Legal

[6] Reducing Administrative Burdens: effective inspection and enforcement, Philip Hampton, HM Treasury, March 2005

Ltd in breach of the Data Protection Act after reporting a laptop computer containing personal information relating to 100,000 customers was stolen. The laptop, privately owned by a contracted consultant, was not encrypted.

Amicus Legal has signed a formal Undertaking outlining that it will take reasonable measures to keep personal information secure in future. The Undertaking has been signed on behalf of Amicus Legal Ltd by the Chief Executive, Andy Tomkins."

The Federal Trade Commission today released a survey showing that 8.3 million American adults, or 3.7 percent of all American adults, were victims of identity theft in 2005. Of the victims, 3.2 million, or 1.4 percent of all adults, experienced misuse of their existing credit card accounts; 3.3 million, or 1.5 percent, experienced misuse of non-credit card accounts; and 1.8 million victims, or 0.8 percent, found that new accounts were opened or other frauds were committed using their personal identifying information.

http://www.ftc.gov/opa/2007/11/idtheft.shtm

US Government Accountability Office: Information Security. Agencies Report Progress but Sensitive Data Remain at Risk .
http://www.gao.gov/new.items/d07935t.pdf
KPMG Survey on prevalence in UK :
http://www.kpmg.ie/Succeeding/publications/DataLossBarometer.pdf

HSBC have had three parts of their group fined a total of £3million for insufficient data security. Various parts of the huge banking and financial services group lost data and they were found not to have controlled data with sufficient care. http://superquote.wordpress.com/2009/07/22/hsbc-data-loss-3m-fine/

Laptop Data Breaches: Mitigating Risks through Encryption and Liability Insurance Machal- Fulks & Scott
http://www.scottandscottllp.com/main/uploadedFiles/resources/Articles/Article-Laptop_Data_Breaches.pdf

The President's Identity Theft Taks Force. Combatting Identity Theft A Strategic Plan 2007. http://www.idtheft.gov/reports/StrategicPlan.pdf

The influential Article 29 Working Party, an independent European advisory body on data protection and privacy to the EC, has argued that social networks like Facebook, Twitter and MySpace need more regulation to ensure that personal data of their respective users is not put at risk. Even though the majority of sites that the report mentions are based in the United States, the group states their large presence in Europe means that they should be subject to European Union privacy and data protection legislation http://www.scribd.com/doc/16736099/ARTICLE-29-DATA-PROTECTION-WORKING-PARTY-Opinion-52009-on-online-social-networking

4 Indicative Data Breach Incidents and responses

Chronology of Data Breaches

What does the Chronology of Data Breaches contain?

The data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. Some breaches that do NOT expose such sensitive information have been included in order to underscore the variety and frequency of data breaches.

Is the Chronology of Data Breaches a complete listing of all breaches?

No, it is not a complete listing of breaches. The list is a useful indication of the types of breaches that occur, the categories of entities that experience breaches, and the size of such breaches. But the list is not a comprehensive listing. Most of the information is derived from the Open Security Foundation list-serve (see below) which is in turn derived from verifiable media stories, government web sites/pages, or blog posts with information pertinent to the breach in question. Many breaches (particularly smaller ones) may not be reported. If a breached entity has failed to notify its customers or a government agency of a breach, then it is unlikely that the breach will be reported anywhere

http://www.privacyrights.org/ar/ChronDataBreaches.htm

Sample extract from January 09

2009 NAME
(Location) TYPE OF BREACH NUMBER OF RECORDS Jan. 2, 2009 Merrill Lynch
(New York, NY) A third-party consulting services firm working on behalf of Merrill Lynch reported, one of their employees was burglarized. The burglars took various items, including a computer, which had on it the names and Social Security numbers of current and former Financial Advisors and some applicants for employment. Unknown Jan. 2, 2009 Pepsi Bottling Group
(Somers, NY)
For More Info Contact:
David Yawman
David.Yawman@pepsi.com
(914) 767-7620 or (866) 578-5410 A portable data storage device, which contained personal information, including the names and Social Security numbers of employees in the US is missing or stolen. Unknown Jan. 5, 2009 Library of Congress

(Washington, DC) An employee in the human resources department of the Library of Congress was charged with conspiring to commit wire fraud in which he stole information on at least 10 employees from library databases. He passed the information to a relative, who used it to open the accounts. Together, the two are alleged to have bought $38,000 worth of goods through the accounts. 10 Jan. 6, 2009 CheckFree Corp.
(Atlanta, GA) CheckFree Corp. and some of the banks that use its electronic bill payment service say that criminals took control of several of the company's Internet domains and redirected customer traffic to a malicious Web site hosted in the Ukraine. The company believes that about 160,000 consumers were exposed to the Ukrainian attack site. However, because the company lost control of its Web domains, it doesn't know exactly who was hit. And so it must warn a much larger number of customers. This breach was reported back in Dec. 3 08. 5,000,000 Jan. 7, 2009 Genica/Geeks.com
(Oceanside, CA)
(888) 529-6261
http://www1.ftc.gov/opa/2009/02/compgeeks.shtm Genica dba Geeks.com ("Genica") recently discovered that customer information, including Visa credit card information, may have been compromised. In particular, it is possible that an unauthorized person may be in possession of your names, addresses, telephone numbers, email addresses, credit card numbers, expiration dates, and card verification numbers. They are still investigating the details of this incident, but it appears that an unauthorized individual may have accessed this information by hacking our eCommerce website. Unknown Jan. 11, 2009 University of Rochester
(Rochester, NY) Personal information including Social Security numbers of about 450 current and former University of Rochester students was stolen by hackers this week from a UR database. The information was taken from a non-academic student database and copied illegally to an off-campus IP address. 450 Jan. 12, 2009 Columbus City Schools
(Columbus, OH) Columbus City Schools experienced a security breach, resulting in employees' Social Security numbers being at risk. CPD officers went to serve drug and auto-theft felony warrants. During the arrest officers learned there might be stolen personal information in the house and found personal information on district employees.It is believed the suspects either stole or intercepted part of a mailing from the payroll division that was en route to annuity companies. 100 Jan. 13, 2009 University of Oregon
(Eugene, OR)
(541) 346-2510 A laptop computer containing data files for Youth Transition Program (YTP) participants was stolen. Those files contained names and social security numbers. Unknown Jan. 13, 2009 Innodata Isogen, Inc.
(Hackensack, NJ) Laptop stolen from an employee's car contained names, addresses, Social Security numbers of current and former employees. Unknown Jan. 13, 2009 Seventh-Day Adventist Church
(Silver Spring, MD) A Laptop stolen and recovered contained names and Social Security numbers. 292 Jan. 13, 2009 Continental Airlines

(Newark, NJ) A laptop containing fingerprints, Social Security numbers, names, addresses, was stolen from a locked Newark office. 230 Jan. 13, 2009 Blue Ridge Community Action
(Morganton, NC) Social Security numbers were on an external computer hard drive that is missing or stolen. The hard drive contained information on clients from four counties who have used the organization's services in the past four or five years. The external hard drive was used to back up information on clients. 300 Jan. 14, 2009 Occidental Petroleum Corporation
(Dallas, TX)
(800) 733-0085 A former employee emails himself (to personal email account)a spreadsheet of employee names, addresses, employee identification numbers, birth dates, starting dates, retirement dates and Social Security numbers. Unknown Jan. 16, 2009 Southwestern Oregon Community College
(Coos Bay, OR) A laptop computer was stolen from the campus putting former and current students at risk. 200 Jan. 19, 2009 Forcht Bank
(Lexington, KY) Customer debit cards were disabled this week after learning they could have potentially been hacked into by persons creating duplicate cards. The cards were comprised when a retail merchant's computer system was hacked. Which merchant is unknown at this time. The breach affected customers of multiple banks and multiple debit and ATM networks. 8,500 Jan. 20, 2009 Kanawha-Charleston Health Department
(Charleston, WV) People who received flu shots from the agency since October, are being warned that their personal information may have been stolen by a former department temporary worker. Information included their names, social security numbers, addresses and other personal information. 11,000 Jan. 20, 2009 Heartland Payment Systems
(Princeton, NJ)
http://www.2008breach.com After being alerted by Visa and MasterCard of suspicious activity surrounding processed card transactions, the company last week found evidence of malicious software that compromised card data that crossed Heartland's network. This incident may be the result of a global cyberfraud operation.
UPDATE (1/26/09):
Heartland Payment Systems has been sued. The lawsuit seeks damages and relief for the "inexplicable delay, questionable timing, and inaccuracies concerning the disclosures" with regard to the data breach, which is believed to be the largest in U.S. history.
UPDATE (2/12/09):
According to BankInfoSecurity.com, the number of financial institutions that have come forward to say they have been contacted by their credit card companies Visa and MasterCard in relation to the breach has jumped from fewer than 50 to more than 200.
UPDATE (6/4/09):
While it's hard to get a handle on just how many consumers were affected by the Heartland Payment Systems (HPY) data breach, the total number of institutions now reporting card compromises is at 656.

UPDATE (6/16/09):
Heartland Lawsuits to be Heard in Texas. The Judicial Panel on Multidistrict Litigation in Louisville, KY issued its decision to consolidate the class action suits. The lawsuits will be heard in the Southern District Court of Texas in Houston. Thirty-one separate lawsuits, on behalf of consumers, investors, banks and credit unions, have been filed against Princeton, N.J.-based Heartland.
UPDATE (7/6/09):
Heartland Payment Systems successfully completed the first phase of an end-to-end encryption pilot project designed to enhance its security.

100 million transactions per month
It is unclear how many account numbers have been compromised, and how many are represented by multiple transactions. The number of records breached is an estimate, subject to revision. Consequently, we have not included this breach in the "Total" below.

Jan. 21, 2009

First Interstate Mortgage Corporation (FIM)/
Nevada One Corporation (Nevada One)
http://www.ftc.gov/opa/2009/01/navone.shtm
(Nevada)

These mortgage brokers have discarding consumers' tax returns, credit reports, and other sensitive personal and financial information in an unsecured dumpster. Approximately 40 boxes containing consumer records were found in a publicly-accessible dumpster. The records included tax returns, mortgage applications, bank statements, photocopies of credit cards, drivers' licenses, and at least 230 credit reports. The defendant, who has owned numerous companies that handle sensitive consumer information, kept the documents in an insecure manner in his garage before improperly disposing of them. Unknown
This breach accrued in Dec. 06 Jan. 21, 2009 Missouri State University (Springfield, MO) Personal information, including Social Security numbers for 565 foreign students at MSU was leaked this month when a university office sent an e-mail message soliciting their help with language tutoring. The email message they got had a spreadsheet attachment that contained names and Social Security numbers for international students. 565
Not included in total -- not known how many students have SSNs. Jan. 23, 2009 Monster.com
(Maynard, MA)
http://help.monster.com/besafe/
http://help.monster.com/besafe/jobseeker/index.asp Their database had been illegally accessed and user IDs, passwords, names, e-mail addresses, birth dates, gender, ethnicity, and in some cases, users' states of residence were stolen. Unknown Jan. 26, 2009 Madison, WI. Human Resources Department (Madison, WI) An oversight by the city of Madison's personnel office is the

reason Social Security numbers of city employees were stored on a laptop computer stolen from a city office. Any official or employee — except those in the police, fire and transit departments — who was issued a new or replacement city identification card from the start of 2004 through 2007 may be at risk. Data on the laptop included photos, names and Social Security numbers. 500 Jan. 26, 2009 U.S. Military
A New Zealand man accesses US military secrets on an MP3 player he bought from an Oklahoma thrift shop for $18. When the 29-year-old hooked up the player he discovered a playlist he could never have imagined - 60 files in total, including the names and personal details of American soldiers. 60 Jan. 27, 2009 U.S. Consulate
Hundreds of files — with Social Security numbers, bank account numbers and other sensitive U.S. government information — were found in a filing cabinet purchased from the U.S. consulate in Jerusalem through a local auction. Unknown Jan. 27, 2009 Beaumont City
(Beaumont, TX) Personal information of current and former Beaumont city workers was accidentally posted online. The information, including birth dates and Social Security numbers. 500 Jan. 27, 2009 Citi Habitat
(New York, NY) During a refurbishing of their office, paper that should have been shredded was improperly placed as trash. Information found blowing in the street included bank statements, 401k statements, credit reports, tax returns, driver's licenses, names, phone numbers and Social Security numbers. Unknown Jan. 28, 2009 CityStage
(Springfield, MA) A computer system might have exposed credit card information of customers on the Internet. The probably occurred in December while the theater's Web contractor was changing servers. Credit card numbers might have been compromised. 60 Jan. 30, 2009 Kansas State University
Manhattan, KS
(785) 532 4441 Students who were enrolled in an agricultural economics class in spring 2001 inadvertently had some personal information exposed on the Internet through a K-State departmental Web site. Names, Social Security numbers and grades of those students have been exposed since 2001. 45 Jan. 30, 2009 Coos Bay Department of Human Services
(Coquille, OR) A scammer made off with Social Security numbers after sending a virus online to a computer at the Department of Human Services office. A application that was installed recorded keystrokes and sent them to an external address. The information was taken from Coos County residents. 45 Jan. 30, 2009 Indiana Department of Administration
(Indianapolis, IN) Social Security numbers of current and former state employees were accidentally posted on a state Web site for about two hours. The Social Security numbers were erroneously included in a contract solicitation file posted on the department's procurement Web site. 8,775 Jan. 31, 2009 HoneyBaked Ham
(Indianapolis, IN) A computer server stocked with credit-card information was stolen from a store. Customers might be at risk. Unknown Jan. 31, 2009 Ball State University

(Muncie, IN) A employee sent out an e-mail, to verify contact information, to 91 special events staff with an excel spreadsheet attachment that, unbeknownst to the employee, included the Social Security number of 19 of the workers. 19”

DataLossDB http://datalossdb.org/about is a research project aimed at documenting known and reported data loss incidents world-wide The Open Security Foundation, as well as our volunteers, feel that there is a distinct need for tools that provide unbiased, high quality data regarding data loss. There are no other open, downloadable, machine parse-able resources out there that facilitate research into this subject matter. By providing this sort of resource, we feel we can help accomplish the following:

- Improve awareness of data security and identity theft threats to consumers.
- Provide accurate statistics to CSO's and CTO's to assist them in decision making.
- Provide governments with reliable statistics to assist with their consumer protection decisions and initiatives.
- Assist legislators and citizens in measuring the effectiveness of breach notification laws.
- Gain a better understanding of the effects of, and effectiveness of "compliance"

Identity Theft Victim Complaint data Federal Trade Commission 2006 report from Identity theft data clearinghouse
http://209.85.229.132/search?q=cache:Xp3yiYju9nsJ:www.ftc.gov/sentinel/reports/idt-annualoverall-figures/idt-cy2006.pdf+Identity+Theft+Victim+Complaint+data&cd=1&hl=en&ct=clnk&gl=ie&client=firefox-a

A laptop containing private details, including bank details, of 30,000 civil servants across Northern Ireland was stolen during a break-in at a government office in Belfast.
http://www.siliconrepublic.com/news/article/13113/cio/30-000-civil-servants-details-on-stolen-laptop

French government probing Sarkozy bank theft(AFP) – Oct 19, 2008 PARIS (AFP) — The French government has launched a probe into withdrawals by thieves from President Nicolas Sarkozy's personal bank account, said a

senior official Sunday.
http://afp.google.com/article/ALeqM5hwrR93MpSzps2leIcVs0arWmiyjg

The computer systems of both the Obama and McCain campaigns were victims of a sophisticated cyberattack by an unknown "foreign entity," prompting a federal investigation, NEWSWEEK reports today……both the FBI and the Secret Service came to the campaign with an ominous warning: "You have a problem way bigger than what you understand," an agent told Obama's team. "You have been compromised, and a serious amount of files have been loaded off your system."
http://www.newsweek.com/id/167581

The Irish Independent **Friday February 08 2008**

HACKERS are targeting state departments for sensitive information. More than 80 government laptops have been stolen or are missing, raising fears about the protection of confidential data.

The Irish Independent has learned the laptops and computers have been lost or stolen over the past five years, triggering concerns sensitive information may be vulnerable.

Four government-controlled websites were also recently the victim of cyber-attacks and telephone hacking incidents.

A garda investigation is under way in the Department of Enterprise, Trade and Employment, which experienced four "noteworthy hacking or cyber-attacks".

The Department of Transport was the subject of a "malicious security breach" and is blocking an average of 50 inappropriate attempts to connect to its systems every week.

Controversies

The revelation follows the recent controversies in Britain over the loss of three laptops from the Ministry of Defence and two discs containing personal data of millions of people.

Last night, department officials insisted no sensitive or confidential information was compromised during the catalogue of incidents between 2002 and 2007.

However, Fine Gael said it would be "catastrophic" if criminals got their hands on confidential information stored by government departments.

The incidents also include the loss or theft of 19 Blackberrys and 10 memory keys.

In the Department of Social and Family Affairs -- which has responsibility for social welfare payments -- five laptops were stolen on public transport and in house and car break-ins.

According to the Department of Defence, two desktop computers belonging to the Defence Forces were stolen last year during the UNMIL mission to Liberia and were not recovered.

A non-networked laptop computer went missing during a visit associated with humanitarian relief to countries hit by the December 2005 tsunami.

Another was stolen in 2004 during a mission to Georgia.

Last year, 12 laptops belonging to the Department of the Environment were stolen from the Custom House and another was stolen while in transit. Ten were immediately recovered, nine of which were obsolete and had been prepared for recycling.

The three laptops missing from the Taoiseach's office did not contain sensitive State information, a spokesman said last night. One was used for presentations, while the other two were remote access laptops.

In 2003, 25 new computers belonging to the Department of Foreign Affairs were stolen from temporary offices in Brussels. An individual who had been working on contract in the department later received a four-year suspended sentence for the theft of eight laptops.

While passwords were required to access the devices and emails were later wiped by the departments, computer experts have raised concerns about the loss of information contained on USB keys.

Many departments are examining encryption software to enhance security.

The incidents revealed to Fine Gael in parliamentary questions include cyber-attacks on four Government-controlled websites in recent years.

Last night, the Department of Social and Family Affairs confirmed it was the victim of a telephone hacking incident, while the Department of Finance saw one of its website pages overwritten by a cyber-hack.

A spokeswoman for the Department of Social and Family Affairs said its laptops could be used for remote access to departmental data, but the information is not retained on the device following access.

Investigation

The revelations follow an earlier investigation by the Irish Independent, which revealed staff in the Department of Social Welfare illegally accessed citizens' private information.

Last night, a leading expert on data protection law said the more public servants who can access the data, the more likely something will go wrong.

Professor Robert Clark of UCD said "human error" can account for most data breaches.

Fine Gael's Damien English said because the government is the "guardian" of public information, it must do its utmost to keep apace with ICT security developments worldwide.

"It would be catastrophic if criminals were able to get their hands on confidential information like names, addresses, PPS and dates of births that would lead to massive potential fraud," he said. http://www.independent.ie/national-news/fears-for-our-personal-data-as-80-government-laptops-missing-1284944.html

Article from " The Banker" re data breaches with special reference to banks
http://www.thebanker.com/news/fullstory.php/aid/5930/Plugging_the_leak.html

A contractor to the Home Office, PA Consulting, lost an unencrypted memory stick containing the sensitive personal information of thousands of people last year. The ICO has now made the Home Office sign a formal undertaking to protect citizens' data. http://www.out-law.com/page-9731

The new head of MI6 has been left exposed by a major personal security breach after his wife published intimate photographs and family details on the Facebook website. Sir John Sawers is due to take over as chief of the Secret Intelligence Service in November, putting him in charge of all Britain's spying operations abroad. http://www.mailonsunday.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html

Almost two million PCs globally, including machines inside UK and US government departments, have been taken over by malicious hackers. Security experts Finjan traced the giant network of remotely-controlled PCs, called a botnet, back to a gang of cyber criminals in Ukraine
http://news.bbc.co.uk/2/hi/technology/8010729.stm

The details of bank accounts held by 21 million Germans are for sale on the black market for 12 million euros (15 million dollars), a German magazine reported Saturday. In an investigative report, two reporters for the Wirtschaftswoche magazine met last month with two individuals, arranged through an intermediary, who offered to sell a CD-ROM containing the names, addresses, bank name and account numbers of 21 million people, the magazine said. **http://www.breitbart.com/article.php?id=081206224148.ie9uiizl**

Detailed and sensitive bank information of tens of thousands of German credit card customers have been stolen in what investigators have described as the worst ever case of data theft in the country
http://www.thelocal.de/national/20081213-16107.html

Employees routinely engage in activities that put sensitive data at risk. They are downloading data onto unsecured mobile devices (61%), sharing passwords (47%), losing data-bearing devices (43%), and turning off their mobile devices' security tools (21%). And, reflective of the blurring of the lines between personal and professional lives, they are using web-based personal email in the office (52%), downloading Internet software onto an employer's devices (53%), and engaging in online social networking while in the workplace (31%). http://www.ponemon.org/blog/post/more-employees-ignoring-data-security-policies

Verizon Business 2009 Data Breach Study Finds Significant Rise in Targeted Attacks, Organized Crime Involvement. ***Financial Industry Accounts for 93 Percent of 285 Million Compromised Records; Most Breaches Avoidable if Proper Precautions Taken*** More electronic records were breached in 2008 than the previous four years combined, fueled by a targeting of the financial services industry and a strong involvement of organized crime…… nearly nine out of 10 breaches were considered avoidable if security basics had been followed. Most of the breaches investigated did not require difficult or expensive preventive controls. The 2009 report concluded that mistakes and oversight failures hindered security efforts more than a lack of resources at the time of the breach.

Similar to the first study's findings, the latest study found that highly sophisticated attacks account for only 17 percent of breaches. However, these relatively few cases accounted for 95 percent of the total records breached - proving that motivated hackers know where and what to target.
http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html

Fourth annual *U.S. Cost of a Data Breach Study*. According to the study which examined 43 organizations across 17 different industry sectors, data breach incidents cost U.S. companies $202 per compromised customer record in 2008,

compared to $197 in 2007. Within that number, the largest cost increase in 2008 concerns lost business created by abnormal churn, meaning turnover of customers. Since the study's inception in 2005, this cost component has grown by more than $64 on a per victim basis, nearly a 40% increase.
http://www.pgp.com/insight/newsroom/press_releases/2008_annual_study_cost_of_data_breach

35pc of IT staff admit to snooping10.06.2009 Over a third of IT staff use their administrator rights to have a peek at confidential company information, including customer databases and HR lists, according to a recent survey carried out by security software firm Cyber-Ark on 400 senior IT professionals in mainly enterprise-class firms across the UK and US.
http://www.siliconrepublic.com/news/article/13156/cio/35pc-of-it-staff-admit-to-snooping

Acerno, which has operated for three years with almost no publicity, says it now has files on 140 million people in the United States, nearly all the online shoppers…. Unlike in Europe, where data collection is closely regulated, in the United States, the privacy framework is based on what is called "notice and choice." In other words, it's fine to gather and use information so long as you tell people what you are doing so and give the option to make you stop. On the Internet, however, the way this has worked is based on a complete fallacy: that Web site users read the privacy policy. Here is the bluntest way to put the question: Is a notice really a notice if the vast majority of people who are supposed to be notified don't notice the notice?
http://bits.blogs.nytimes.com/2008/10/24/what-online-stores-sell-data-about-you/

Fewer than half of UK companies use encryption technology to secure their data. Despite the lack of encryption, UK IT managers claim their corporate data is safe and almost two-thirds (65 per cent) said the HM Revenue & Customs (HMRC) data breach will not change their IT spending priorities, according to a survey by Check Point. http://management.silicon.com/itdirector/0,39024673,39169337,00.htm

Veterans Sue VA over Data Loss. The lawsuit, which comes days after the VA reported that the personal information of 26.5 million veterans was stolen from an employees home, seeks damages of $1,000 for every person listed in the missing database files. The suit also asks that the courts prohibit the VA from handling any personal privacy-protected data except under court supervision, and that the court create a set of "consensus minimal security standards" under which the VA can operate. **http://www.eweek.com/c/a/Security/Veterans-Sue-VA-over-Data-Loss/**