# Cyberspace Challenges and Law Limitations

Aadil Al-Mahrouqi
School of Computer Science and Informatics
University College Dublin
Dublin, Ireland

Cormac O Cianain
School of Computer Science and Informatics
University College Dublin
Dublin, Ireland

Tahar Kechadi
School of Computer Science and Informatics
University College Dublin
Dublin, Ireland

***Abstract*—Privacy and Data security are heating topic in the modern technologically advanced economy. Technological Innovations have created new forms of electronic data which are more vulnerable to theft or loss when compared to traditional data storage. Moreover, the recent advances in internet technologies have exacerbated the risk of security threats. The Internet brings a whole new set of challenges in terms of data protection. Considering the complexities of modern technological advancements and its impact on data security, this study examines the Irish laws and EU directives for privacy and data security, its effectiveness in managing large scale data breaches and limitations. This paper also simulates attack scenarios that can be done by anonymous users in a complex cyberspace environment and explains how a digital evidence related to the attack scenario can be tracked down.**

***Keywords*—Internet anonymous; pseudonymous internet users, electronic discovery; large-scale data breaches***

## I. Introduction

Cyberspace has become a vital part of individuals and communities worldwide. Many key sectors of the global economy including banking and finance, health sector, communication and the defence relies heavily on cyberspace (United States Department of Defence, 2011). According to Deibert and Rohozinski [1] cyberspace has become an indispensable part of the social, political and economic power worldwide. Cyberspace security threat is a key challenge for the modern society. Many critical infrastructures of the society rely heavily on cyberspace that makes it vulnerable to disruption and exploitation. It represents one of the most serious threat to national security and public security [2]. Any risks from cyberspace are severe since it undermines the safety and security of citizens and cause disruption in social and political life. The constant innovation and advancements in cyberspace technologies continuously generate new forms of security challenges. Users who conform the basic protocol to internet connectivity increases the participation of people from all backgrounds creating a constant flux based on ingenuity [3].

The rise in security threats generated from the development of cyberspace has increased the need for tighter laws and regulations. However, the constant transformation and high degree of complexity of cyberspace creates a major barrier for its regulation. Cyberspace is characterized as a network of interconnected electronic communication channel [4]. The transnational organization of the cyberspace networks makesthe states be fully in control of the entire activities in the cyberspace. This lack of physical proximity and control is a major barrier to states regulations to manage increasing data security breaches. All these special properties and complexities of cyberspace allow cybercrime to elude state control [1]. This paper specifically examines the cyberspace security threats from anonymous and pseudonymous Internet users, electronic discovery challenges, law responses to the problem to these security threats and large-scale data breaches and finally evaluates the current limitations in Irish laws and regulations.

Aadil

August 27, 2015

## II. Literature Review

The purpose of this literature review is to provide an overview of the most relevant, previous research done on the legal laws that focus in anonymous and pseudonymous internet users, electronic discovery challenges, law responses to the problem to these security threats and large-scale data breaches and finally to evaluate the current limitations in Irish laws and regulations.

### A. Anonymity and Pseudonymous Internet

The Internet provides all the users across the globe the freedom and the choice to remain anonymous or pseudonymous. Anonymity has become the cornerstone of Internet communication that promote free speech. Many people prefer to remain anonymous or pseudonymous on the Internet for several reasons which may not always be with criminal intent. For example some people use pseudonymous ID for fun or share information for the benefit of society without revealing their identity. Although not all people misuse the choice of Internet anonymity, people with criminal intent use Internet anonymity techniques to perpetrate cybercrime [5]. Anonymity in blogging is very popular these days. When some bloggers prefer to use their real names some prefer to be pseudonymous to communicate and share their messages and thoughts on blogs. Organizations also use blogs to keep in touch with their customers to obtain feedback about their products and services. It also allows employees to share new ideas which can be used by companies to develop new strategies. Anonymous blogging without any harm to others is permitted among Internet users.

The protection of identities of anonymous and pseudonymous people in Internet varies between countries and depends on the nature of the activities. For example when anonymous

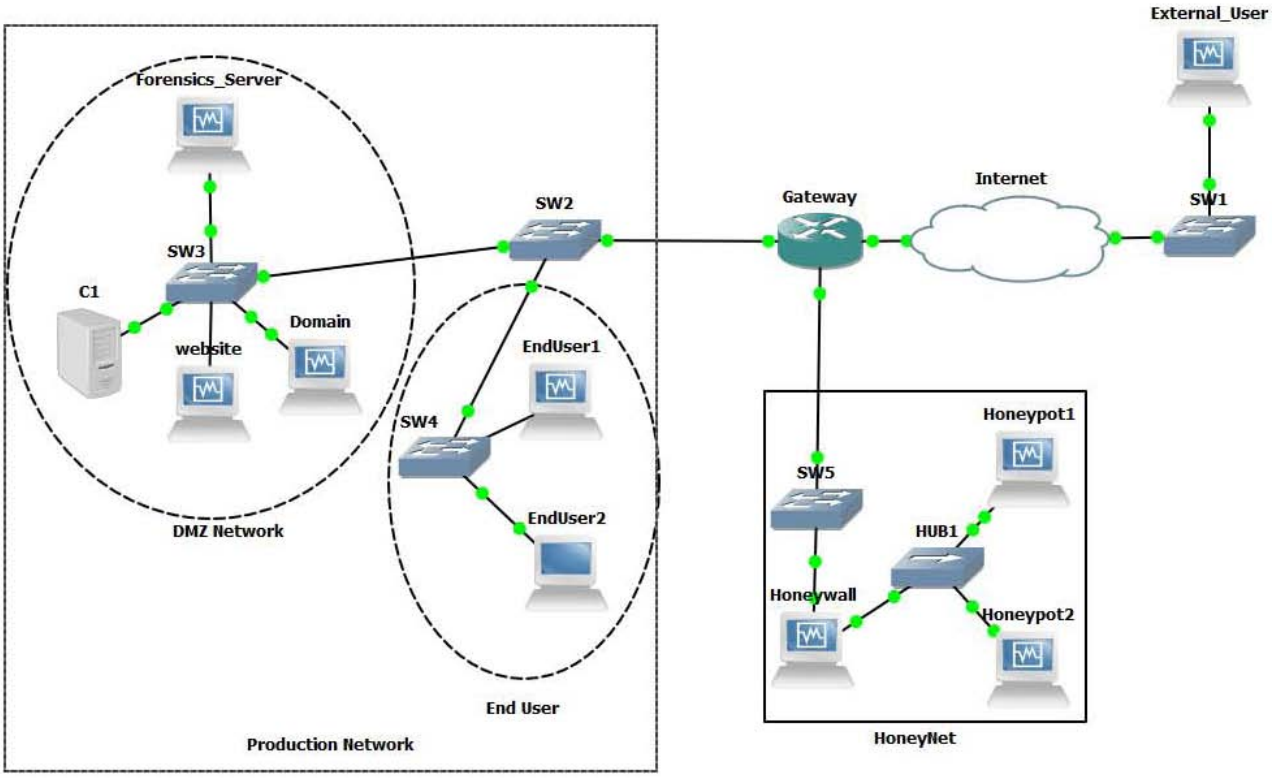


Fig. 1: Simulation Honeynet Network in GNS3

blogging affects the reputation of individuals and organisations, there are laws to reveal the identities of the anonymous person. Although there are exceptions to this law. There are many cases where organisations reacted to anonymous bloggers which when affected their reputation. One such case was when an employee was sacked by her employer for writing an Internet diary under the pseudonym Petite Anglaise which resulted in reputational issues for her employer. The woman was awarded 30,000 for wrongful dismissal [6]. However, blogging can become bullying when the privacy of others are harmed by sharing secrets that affect the reputation of individuals and organisations. Ryanair appealed to the high court of Ireland seeking the disclosure of identities of anonymous individuals using code names such as ihateryanair and cantfly wontfly who made intimidating posts about their pilots [7]. However, a high court in Ireland dismissed the application. A similar case in US, Totalise plc v. Motley Fool was successful where the court ordered to identify the pseudonymous user using the Zeddust ID, under the data protection act and section 10 of the contempt of court act for posting negative comment. [8].

Anonymous downloading has resulted in the illegal downloading of music and film from online website. The first case in Ireland relating to anonymous downloading was brought to the high court in 2008 by EMI and three other major record companies to compel Eircom to prevent its broadband and customers downloading music illegally through file sharing website [9]. In the context of Article 2 and 8 of the Data protection act 1988-2003 [10], Eircom ensured the confidentiality of the users who illegally downloaded music from file sharing to the plaintiff until the courts order released. There has been similar cases in Beijing, China where the ISPs were forced to block the P2P download [11], [12].

### B. Electronic Discovery Challenge

Technological changes and development in the information processing are becoming increasingly complex and incredible throughout the history. We have gone through an era of paper based society which is now transformed to a completely electronic based society with the technological advancements. These advances in information processing has brought major changes to the form of record keeping and information processing. The transformation from paper to digital information processing and record keeping has opened out a new set of challenges and complexities to the society. The digital record keeping and information processing has created an explosion of information which is the fundamental reason for the e-discovery problem. E-discovery is the process of identifying, preserving and collecting electronic documents that may be considered relevant to a matter. Electronic information sources are becoming an increasing source of evidence for modern disputes and court can order expensive electronic discovery to form evidences. E-discovery in Ireland is currently governed by the Rules of the Superior Court (Discovery) 2009 S.I. 93 2009 [13]. McCarth v.OFlynn [1979 I.R.127 (x-ray) and Clifford v Minister of justice [2005] IEHC 2008 are examples of cases in Ireland which explained that data discovered in a court can be any item that gives an information as opposed to an item on which writing can be inscribed.

Electronic discovery has been a significant issue in Irish

court over the past decade. Based on the significant commercial disputes on electronic discovery, the litigation committee of the law society of Ireland issued a report with recommended changes to the 1999 electronic discovery rules of the superior court of Ireland. The whole recommendations of the litigation committee was accepted and adopted by the rules committee to the superior court of Ireland in 2009. This provided Irish courts with a wider scope and offered significant flexibility in terms of electronic discovery applications. Courts began to consider several complex electronic discovery issues including application concerning Meta data and reasonableness of processes employed. The superior court in a telecom case has stated that the data mining application can be granted as court has the right to order the disclosure of documents or creation of new documents under electronic data discovery.

Organisation has the obligation to preserve document under the new discovery rule. The law society of Ireland has stated clearly that the party seeking discovery to provide a letter to the party against whom the discovery sought specifying the specific category of documents required and the reasons for which the specific category of documents is sought. Failure to discover all the data sought based on the necessary could be a breach of party's obligation to discovery [14]. When a discovery is made, the party against whom the discovery is sought is required to prepare an affidavit that report the statements of the documents. The law society makes it clear that there is not any regulation on the documents that are lost or spoiled. When there is a discovery requirement by Irish law and the documents are lost or spoiled, then there is an obligation to prepare an affidavit that states that I formally had but no longer have the documents required. It should also include an obligation that specify what happened to those document when you last had them and where they are now and obviously an adverse influence can be drawn against you if you lie in this regard or you had these document but recently you have destroyed them or lost them or they went up in the fire.

There are several issues associated with the discovery of documents in the present legal system mainly due to the differences in the traditional rules on document discovery and the increased use of electronic documents by individuals and organisations. The first problem is what constitutes the documents that have to be discovered. This includes the doubts regarding the type of electronic documents whether it includes electronic data that might or might not constitute the content of the document itself, does it include the Meta data and so on. The second problem is that the traditional rules that have been developed for paper documents is not suitable for the discovery of electronic documents.

There are several other challenges relating to the electronic discovery. Once such challenge is the expense incurred by organisations for electronic discovery. The expense of electronic discovery can even exceed the amount discovered. In a case where eircom was asked to produce a report based on the information in its database the expense was higher than the amount discovered. Based on the EMI v Eircom case of electronic discovery where Internet users have been illegally downloading music, the barrister Ronan Lupton reported in the Electronic Discovery Ireland conference in Dublin that the amount spent on electronic discovery was 700,000 EUR while the amount recovered was only 70,000 EUR. The electronic documents stored by an organisation are mostly in proprietary format which means that the data needed to be interpreted. An organisation might need a software to interpret this information which might be expensive. Moreover, rarely the lawyer has IT knowledge necessary to interpret the electronic documents using software making legal proceeding complex and therefore is a major barrier to legal system. Confidentiality of the electronic documents discovered is a major concern. To ensure the confidentiality of the electronic documents, courts have the authority to limit the sight of the documents as in Koger v ODonnell [2009].

Social media sites such as Facebook, twitter, and LinkedIn has been used by people with criminal intent to perpetuate crimes. The electronic communications in social media sites create an extensive electronic information that have become evidences in many litigations. A recent case was where a woman in Ireland was dismissed from her job for insulting her boss on Facebook. Further examination of the Facebook page revealed more critical comments some containing expletives, about her employer. The employment appeals tribunal ruled that the dismissal of the employee was not unfair. Thus social media communications is a major source of evidence that impact the ethical consideration for lawyers. Disrespectful and defamatory comments or message posted on Facebook or other social media site is highly relevant in modern environment and can create adverse consequences.

International transfer of data in a multinational corporation as per the data request from a different country is a major issues in the cross border data protection. For example, when a multinational corporation with operations in US and Europe received a court order to produce personal data stored in its European affiliate, it created an ethical dilemma for the privacy officer. The privacy officer faced the dilemma of whether to satisfy the compulsory US discovery obligations or to comply with the European data protection law which restricts data disclosures for litigation purposes. This has become a complex problem that not only affects the European affiliates of multinational corporations but also the lawyer who deal with the cross border electronic discovery process. Thus there is a need to reconcile the requirement of the US litigation rules and EU data protection laws to provide a precise guidance for businesses on how to manage such conflicting situations. Pre-trial discovery for cross border civil litigation adopted by the Article 29 Data protection working paper (Art.29 DPWP) is a working paper that aims to manage the conflict between the US litigation rules and EU data protection laws [15]. The articles covers the nature of the problem, the legal issues in the EU data protection laws governing the electronic discovery requests and the working paper guidance and further practical steps that can be used by organisations to tackle the issues.

Electronic discovery approach in Irish jurisdiction is less developed especially in the commercial court proceedings which deal with large number of commercial litigations. The admissibility of the electronic evidence was a major problem in Irish courts before the legislative interventions in the Section 22 of the E-Commerce Acts 2000. One major problem with the computer generated evidence is the difficulty to identify the original evidence. This is because the computer generated evidence can be produced multiple times in the same format

which is different from the traditional evidence in the paper. In traditional evidence in the paper, there is a single original and the rest can be called copies. Section 22 of the E-Commerce Acts 2000 permits the use of material which is not in its original form provided that it is the best evidence that could be obtained. However, Irish law does not allow the use of material obtained illegally or unconstitutionally since it is considered inadmissible.

### C. Law responses to large scale data breaches

Large scale data breaches has become a common in Irish news headlines. There are quite few cases on public and private bodies losing data from their server, laptops and USB keys. One high profile example is of Bank of Ireland losing the personal information of their customers without prior notification. The financial regulator and Billy Hawkes, the Irish Data Protection Commissioner who examined the case identified and examined the security arrangements in place and the exact circumstances that resulted in the delay in reporting to the appropriate personnel for taking further actions. The only justification provided by the Bank of Ireland for its defense was that it "monitored all of these customer accounts and can confirm that there has been no evidence of fraudulent or suspicious activity" which itself was insufficient and does not justify the fact that the customer information was not protected.

Another famous example was the security breach is by Health Service Executive (HSE). From 2010-2013, there has been over 69 shocking large and small data breaches by HSE in the form of stolen or lost laptop, USB sticks and smartphones. 61 of the electronic records were stolen, with 51 having unspecified sensitive information and 20 without encryption codes [16]. In security breach in 2008 left thousands of HSE staff open to identity theft when an unencrypted laptop containing the personal details had been stolen from the HSE offices at the Carnegie Centre in Dublin's Lord Edward Street. The staff were not told about the theft of the unencrypted laptop until after 13 days [17]. Similarly in 2010, hundreds of patient records were seriously compromised by a major security breach at the HSE [18]. In 2011 HSE reported another breach of data when documents including sensitive information of over 100 patients including names, addresses and date of births were discovered in a bin outside Roscommon hospital. More recently, June this year, HSE has breached the rights of its employee by disclosing his salary details to his ex-wife [19].

### D. Duties under the Data Protection Act

The continuing high profile data breaches has demanded the need for greater accountability by organisations like Bank of Ireland and HSE that holds personal information. Now the major issue is about what can be done to increase the accountability of these organisations and what steps should be taken to prevent such incidents happening in the future. Organisations are not taking the necessary steps to systematically organise and secure personal data. The problem is that the data belongs to different people and not the organisation that hold the data due to which the organisation lack incentive to secure the data appropriately. There is a need to incentivise the holder of the data. The cost associated with the data breach is for the individuals whose information is lost and the cost of securing the data against the breach is held by the organisation holding the data. One method to incentivise the organisation holding the data is to internalise the cost of data loss. There are currently different data security obligations and duties for data controller to secure data under data protection act which is discussed in the following section.

All the business incorporated in Ireland that gather or processes personal data is required to comply with the data protection acts. The data protection acts makes the data controller accountable for the security of the personal data. Data controller has a duty to keep and secure the data. Section 2(1)(d) of the data protection act 1988 and 2003 states that Appropriate security measures shall be taken against unauthorized access to, or unauthorized alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Thus securing data is to prevent unauthorised access and unauthorised disclosure of data to third parties. A data controller is responsible to prevent both internal and external security breach of personal data. In order to ensure effective data security the data protection commissioner issues a code of practice and guidelines on the responsibilities of data controller and actions to take when personal data is exposed to risk of exposure [20].

Section 2 C of the data protection act prescribes the appropriate security measures by the data controllers which includes the measure to ensure the level of security appropriate to prevent the harm that might result from unauthorised or unlawful data processing or accidental or unlawful destruction of the data concerned. There are cases where the data protection commissioner identified inadequate security measures and took necessary steps. One such example was when the data protection commissioner identified inadequate security measures in 2008 when the Credit Union transmitted the personal data of its customers including username and passwords via unsecure mail. The excuse by the credit union for lesser security mesures for usernames and passwords was because they were afraid that the users might not remember their user details at a later date was unjustifiable by the data protection commissioner.

*1) Sanctions for Failure to Provide Adequate Data Security:* In Ireland, the Data protection commissioner neither have the power to impose a fine for inadequate data security nor for criminal prosecution for data breaches. This allows large data breaches by public and private organisation escape easily. Moreover this is also one main reason why there is continued data breaches in public organisations like HSE. The data stolen from Bank of Ireland in 2008 was only reported to the data protection commissioner only after a year and the actual cost of data lost is not yet notified. UK has much stricter sanctions for failure of adequate data security, For example, the financial services authority UK fined the Nationwide Building Society (UK) 980,000 for the poor data security which resulted in the loss of a laptop containing sensitive information of millions of its customers [21]. The EU directive (95/46/EC) necessitates having an adequate control for data protection in member states and in case of failure to comply with the national data protection law and the person who suffered the damage is entitled to receive compensation from the relevant data protection controller (Article 23).

*2) Data Breach Notification and Department of Justice Review Group:* Data breach notification in Irish law requires the organisation to voluntarily disclose any data breaches to data protection commissioner. To ensure data breach notification the data protection commissioner approved a code of practise in July 2010 which states that All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident. In case of doubt in particular any doubt related to the adequacy of technological risk-mitigation measures the data controller should report the incident to the Office of the Data Protection Commissioner. [22].

The code allows departure from the data breach notification when all the following three conditions are met. They are a) $<$ 100 data subjects affected; b) all data subjects affected have been notified without delay; and c) the incident did not involve sensitive personal data or financial data. In all other cases, the data controllers reporting to the data protection commissioner as per the code of practice should contact the data protection commissioners office within two working days of becoming aware of the incident about all the details of the incident include the circumstances surrounding the incident. Based on the details outlined about the incident of data breach the office of the data protection commissioner determine the need for detailed report and/ or subsequent investigation based on the nature of the incident and the appropriate physical and technological security measure to protect the data.

The department of justice commissioned a review group on data protection law. The justice review group on data protection law recommended two necessary changes for effective enforcement of data protection and to avoid any future breach. The recommendation states that The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the DPC, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the DPC.

### *E. Comparison with The US*

Data protection issues have become a growing problem in the modern world with the increased use of Internet anonymity. Thus the Internet has become an easy planet to conduct crimes. Governments all over the world are moving towards regulating crimes over the Internet through laws and regulations. However several crimes escape the law due to the complex nature of Internet anonymity techniques. This section examines the laws and regulations in the US compared to the EU directive and Irish laws and regulations throughout history to regulate anonymous and pseudonymous Internet communications to prevent Internet based crimes [23]. However, the 1997 decision by the federal district court of Georgia in the US invalidated a state law that criminalized anonymous and pseudonymous Internet communications, since Pseudonymous and anonymous communications have been part of American tradition and jurisprudence. Pseudonymous and anonymous communication has been a part of US history with many having made rich contributions to political discourse. Thus the issue was consistent with age-old practices in America. Internet anonymity is treated similarly to anonymity in a leaflet or book, treating it as another form of communication media [24].

Decriminalising anonymous and pseudonymous Internet communication has provided new hope to anonymous and pseudonymous Internet users to continue with criminal activities on the Internet. One main difference between the anonymous communication over the Internet and any other media is the ability of anonymous communication through Internet to reach the population all over the world as opposed to reach in a small region. Wider reach of Internet anonymous activities can have a much larger impact than anonymous communication through any other media. The Irish data protection act 2a 1988-2003 does not allow organisations to disclose any personal information without individuals permission, even when there is a physical and security threat. Thus the terms and conditions of many organisations include a clause that allows an organisation to share the personal information of individual when there is a suspected illegal activity or to prevent physical harm or financial loss. One such examples is the privacy policy statement of PayPal that We may share your personal information with Law enforcement, government officials, or other third parties when we are compelled to do so by a subpoena, court order or similar legal procedure. We need to do so to comply with law or credit card rules. We believe in good faith that the disclosure of personal information is necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate violations of our User Agreement. Other third parties with your consent or direction to do so [25].

The privacy law in the US is much different when compared to the EU directives. When the EU established board standards ensure individual privacy protection [26], the Patriots act in the US allows the US government to search for personal information without users knowledge [27]. Thus the privacy laws in EU and the US are entirely different. The priorities of the EU approach to privacy and data protection law is entirely different from the US privacy and data protection law. The priority of US privacy and data protection law is to ensure justice and security within the country with less priority over the protection of individual priority. However in EU, the privacy and protection of individuals is the main priority. This is evident in the two cases, one in the the US and one in Ireland where the plaintiffs approached the court to reveal the identities of anonymous individuals passing defamatory information over the Internet. The case in US Totalise plc v. Motley Fool was successful and the identities of the anonymous user was identified, whereas the Ryan air attempt to identify defendants who were claimed to intimidate Ryan air pilots was rejected by The High Court, Dublin.

Lawyers in America can preserve and produce electronically stored information without a sanction [28]. However the EU Data Protection and Privacy act (95/46/EC) requires laws to obtain and order to search and preserve evidence. This is because the privacy law in EU is much more comprehensive. The EU privacy act stated that In the EU, privacy is considered a fundamental human right. Therefore, the directive seeks not only to protect E.U citizens privacy generally, but does so within the context of protecting a fundamental right requiring

protection of a high degree, which in the Unions language means the maximum possible. Since the US and EU have different privacy and data protection laws, there have been recently a conflict on the privacy and data protection agreement between the US and EU. There is an US - EU agreement to keep the personal information of the transatlantic passengers from EU for up to 15 years [29].

As per S.11 of the Data protection Acts 1988/2003 there are specific conditions that must be satisfied before personal information of European citizens is transferred to third countries. It is stated that Organizations that transfer personal data from Ireland to third countries i.e. places outside of the European Economic Area (EEA) will need to ensure that the country in question provides an adequate level of data protection. Certain third countries have been approved by EU commission that qualified the condition of adequate data protection. The US safe harbour arrangement has been approved for those US companies that have agreed to be bound by the data protection rules. There are currently no cases where the EU member states requested to disclose information of citizens currently residing outside EU. Countries those do not have adequate data protection standards or that are not approved, the data controller ensures data protection rights of individuals in other ways. The controller may use EU approved model contracts that contain data protection standards that are equivalent to EU data protection standards. To ensure data protection by corporation the data controller use EU approved binding corporate rules for international transfer of data and information within the company [30]. The S11 of Data protection Acts 1988/2003 and the Article 29, has set exception to the transferring of data from EU member states to third countries.

The authors [31], [32] proposed the forensics readiness and awareness framework to reconstruct a cybercrime scenario that was previously observed. The proposed framework that contains fifteen different software and database blocks. These blocks works as a single unit in order to forensically process and normalise the captured events. The blocks summarised in four sections, namely, alert logs normalisation, attack scenario reconstruction, information logs normalisation and security awareness and training.

In [33] the authors presented a simulation study network attack scenario. This is the first step towards validating the proposed model. The figure 1 shows the simulation case study used capturing, normalizing and analysing events. The main point of designing virtual network attack environments is to create a sandbox that allows one to perform such experiments, from real assets and at a low cost. Both the capturing and examination of the events were conducted in the simulated case study. The detection of network artifices changes after the executions of SQL-injection attacks were also recorded. The outcome of this experiment can be used as a recommendation in real cyber infrastructure. The core idea of the case study is to examine the website that has been compromised by an SQL injection attack. To simulate this attack scenario many open source tools were used such as Graphical Network Simulator (GNS3), Oracle VM Virtual Box and VMWare workstation. The Wireshark forensics tool was also used to detect criminal activity from the network layer (Layer 3 in OSI model), in addition, the devices memory of victims and attackers examined by using the Volatility Framework 2.4 were also examined.

In addition, simulation approaches helps to graphically simulate an attack for courts, jury and investigators. The simulation approaches also helps to simplify the incidence (An image = 1000 words). The current study [17] proposes investigation learning methodology based on the proposed case study. The learning methodology consists of two stages; stage one is to build a network topology of the proposed case study and stage two is to create a network union matrix.

An in-depth survey for events admissibility in the Irish court of law is carried out in [34]. Overall, the legal review is mainly focused on different primary areas: the admissibility and authentication of digital evidence and focuses mainly on Irish law. Admissibility refers to a set of lawful tests carried out by a judge for forensic assessment of the finding evidence. Trustworthy means that an accurate copy of digital evidence was acquired, and that it has continued to be unchanged since it was recovered. Authentication is a process to check the reliability of digital evidence. The judge summarises five issues that must be considered when evaluating whether evidence will be admitted, namely; not unduly prejudicial, best evidence, not hearsay or admissible hearsay, authenticity and relevance.

The authors also presented an investigation learning methodology based on the proposed case study presented in [34]. The learning methodology consists into stages, stage one is build a network topology of the proposed case study and stage two is to create a network union matrix. Using this setup the authors were then able to simulate specific network devices configuration, perform SQL injection attacks against victim machines and collect network logs. The main motivation of the work is to finally define an attack pathway prediction methodology that makes it possible to examine the network artefacts collected in case network attacks.

Based on this case study the authors proposed a new network forensics model [34] that can makes network events admissible in the court of law. The proposed model presented used to collect available logs from connected network devices, applies decision tree algorithm in order to filter anomaly intrusion, then re-route the logs to a central repository where events management functions are applied.

## III. Case study of cyberspace risks and resolutions

The case study scenario is selected based on the issues and problems that are faced in cyber space forensics. In this research, the scenarios have been developed to demonstrate the results and to assist organisations and investigators in dealing with such attacks. There are two attack scenarios that the authors can investigate, the authors have made certain assumptions about the attack strategies used in order to simplify and summarise an attack. One is an internal attack committed by a trusted person within the company, and the other is an external attack committed by an entity whose credentials are unknown to the company. These two scenarios present very different concerns for a company and support, to a point, two differing attack topologies. A third attack type is a hybrid of both of these attack types and can be described as a fuzzy attack. This is one where the attacker is external to the network

but establishes a presence within it by compromising a node, gaining a certain degree of control of a node from where he can launch an attack.

### A. Incident Summary

Law enforcement received a report that Great International Banks (http://10.55.3.101/) website has been compromised by an unknown attacker. Based on the initial investigation on the website the attacker used different techniques and tools to compromise the victims website such as SQL injection, XSS, broken caching, directory traversal and breaking the local authentication login to the server. Please see the (Figure 1 depicts the Network topology).

Using various tools and methods against the experimental website, an attacker is able to garner lots of information regarding the sites setup, the applications and services running on the device hosting it and back end data meant only for the web application. The system displays many of the vulnerabilities which arise due to poor system administration. The very nature of the Internet is communication. Adding checks, authentication and security can slow down the development of a site and restrict services. Implementing these takes skill and an in-depth knowledge of system, network and application systems. Its often easier to leave a site less secure and use default values for speeding up implementation. Once new features or services are added to an application the site needs to be retested for vulnerabilities. These new features often introduce more security vulnerabilities due to poor error handling and gaining elevated privilege access due to poor authentication and trust between services hosted on the device running the application.

Issues encountered testing this system reveal issues with poor error handling, invalidated user input, cookie poisoning, SQL Injection, XSS broken authentication, cryptography issues, broken caching, directory traversal and a poorly implemented mail relay service. The authors have based the severity on the level of access the authors were able to gain from each of the issues, hear the authors will list the most of the issues which the authors observed in the penetration test as well as a recommendation how to fix these issues.

### B. Examples of cyberspace risks

*a) Poor error handling (Severity-Medium):* Poor error handling is demonstrated by provoking the system into telling you more about the underlying infrastructure. Error messages can be provoked by entering unexpected or unusual input in the application. Using this method against the login page showed that the application was running on IIS (Microsoft Internet Information Services).

HTTP normally runs over port 80, telnetting to "telnet 10.55.3.101 80" generated the 400 error (HTTP/1.1 400 bad request, server: Microsoft-IIS/5.0). This tells the attacker that the system is probably subject to many of the vulnerabilities with IIS/5.0. It narrows the search of the attacker to this specific application and the attacker can then be tailored towards IIS 5.0. Without this information, an attacker wouldn't be able to leave out attacks for other web servers such as different version of IIS and Apache.

By inserting values via the branch locator page of the application, the authors were able to get the application to accept a value it was not expecting. By using a "Man in the middle" attack by intercepting traffic to be sent to the application via the browser, the authors were able to insert "zip= <script >alert(document.cookie) </script >&searchtype=zip" instead of "zip=1225215&searchtype=zip" which the application was not expecting. This resulted in the application displaying:

Microsoft VBScript runtime error '800a000d'
Type mismatch: 'clng'
/locator.asp, line 19
<script >alert(document.cookie) </script >
Line 19 of the code in locator.asp

Telling the attacker the name of the file used to interact with the database "locator.asp". That the back end database is most likely a version of Microsoft's SQL server, its caused by line 19 in the code for locator.asp and it's been trying is assigned a value that should be an integer.

*b) Directory traversal (Severity-Very High):* normally a web application would only have access to files in the webroot/<site>directory or shortcuts to cgi/asp directories where the files can only run as a specific web user thus reducing the access to the overall system. From information garnered the site, it was most likely running from a Windows device and seeing a posting in one of the forums "$http : //10.55.3.101 \setminus disclosures.asp?content = .. \setminus .. \setminus winnt \setminus System32 \setminus cmd.exe$", the authors decided to try simple attack and attacker could run. Using Nmap against the site to find it there were any readable directories. The authors mounted a separate image of the web server so the IP address changed as the authors were then able to load a backtrack image and use Nmap. Showing that there were 3 shares, Admin, C$ and IPC" Using the virtual server the authors were then able to navigate to these by running:

$10.55.3.101 \setminus Admin\$$

$10.55.3.101 \setminus C\$$

But both of these required a username and password. The authors were able to find this by using the mounted image and running Nmap again. To reveal that the username "administrator" and password "password" would give be accessed. This is a very high vulnerability as it gives the attacker full access to the systems infrastructure and resources. By using this authentication the authors were able to access server files.

*c) Default or easily guessable paths:* Using Burp and some research into the ISS setup, the authors were able to determine the location of directory readable folders:

$http : //10.55.3.101/Images/$
$http : //10.55.3.101/css/$
$http : //10.55.3.101/html/$
$http : //10.55.3.101/includes/$
$http : //10.55.3.101/js/$

A sample list in the:

$http://10.55.3.101/js/$

Friday, July 26, 2002 7:12 PM 2514 rollovers.js
Wednesday, December 25, 2002 10:32 PM 23 test.txt
Wednesday, July 31, 2002 4:05 PM 1807 validate.js

$http://10.55.3.101/images/$

$Friday, July 26, 200211:06PM2548eycu.gif$
$Friday, July 26, 20027:19PM644forum_off.gif$
$Friday, July 26, 20027:17PM644forum_on.gif$
$Tuesday, July 03, 20017:48AM1101icon_browser_ie.gif$
$ResultsTruncated..$

Most of the folders don't hold sensitive information, primarily used for cascading style sheet, images used in the rendering of the web application but access to the js folder and includes would give the attackers a chance to trick the script to accept values from the user and are executable on the server.

*d) SQL injection (Severity-High):* These vulnerabilities are found in the area of the website that accepts input from the user and then uses this in the underlying database. By looking around the website, the authors were able to determine the variables accepted by looking at the client side form checks validate.js. The customer number had to be numeric with no letters or special characters:

$functionCheckNumbers(TheNumber)$
$varvalid = true$
$varGoodChars =$ "1234567890"
$vari = 0$
$if(TheNumber ==$ "")
$valid = false;$
$for(i = 0; i <= TheNumber.length - 1; i++)$
$if(GoodChars.indexOf(TheNumber.charAt(i))$
$== -1)valid = false;$

The password side accepted the following combination of collection of characters:
$(varGoodChars = 1234567890qwertyuioplkjhg$
$fdsazxcvbnmQWERTYUIOPLKJHGFDS$
$AZXCVBNM!@\#() -_; : |? >< ,.)$

Using Burp again as the Man in the Middle attack, the attacker is able to bypass the validate.js and replace:
$acctnum = 123123\&txtPassword = sdfsf12\&action = login$; with: $acctnum =' or'1' =' 1\&txtPassword =' or'1' =' 1\&action = login$

This will allowed us to successfully access to the personal account of first record in the database customer accounts. In summary, been able to manipulate the data held within the database itself, using basic enumeration and SQL code. Constrain input by listing acceptable characters. The use of parameterised SQL for data access. Using an account with the minimum level of access which has restricted access to the database. The use of stored procedures with parameterised SQL. Good coding practice would suggest, never concatenate user input with application SQL for form the SQL been sent to the database. Constant vigilance and checking logs for any suspect attacks. Its rare that an attacker would be able to compromise a system on their first attempt. This may give you time to realise potential errors in your code and fix them before they are exploited.

*e) Column enumeration (Severity-High):* Once the attacker has this level of access, its much easier to gain more access and reveal more information using column enumeration. Using the branch locator page, as a starting point, the authors were able to get the application to reveal the next column by adding 1=1 to the URL giving the response ($http://10.55.3.101/locator.asp?searchtype = state\&state = z'having1 = 1-$) Giving the attacker the next column in the table. Therefore, the next column name is locator and then branch number. Using column enumeration after every column revealed allowed us as an attacker to from the following ($http://10.55.3.101/locator.asp?searchtype = state\&state = z'groupbylocator.branchnohaving1 = 1$) Building from this and using the output from the back end database an attacker would get all of the columns available (Branch, Address, City, State, Zip and Telephone).

*f) Cross Site Scripting:* The authors took information from the forum and tried obvious passwords like admin,password,Aladdin,null, etc against them. One of the accounts (Maria Orlando) had the password for the account 103645516 set to password. Taking the example, and after logging in as Maria Orlando:103645516. This was easy to enumerate in the Burp suite by sending the output to Intruder and building a payload of each password into the account numbers found on the forum. Knowing that the account number was numeric and 9 characters in length made the task easier. The authors were able to gain access using the supplied credentials 103645516:password. The authors then logged into the customer forum as Maria and posted the following java script in the message content:

$< scripttype =$ "$text/javascript$" $>$
$alert($"$BOOM$!!!!"$);< /script >$

So this will producing error message in the forum page once that page refresh.

*g) Cookie poisoning (Severity-Medium/High):* The ability to steal another users identity. Normally used to track a users preferences but can be used once authorisation has been granted to allow the user to login without a password. Very few applications would allow this where financial or medical data is involved, but it has been known to happen. Depending on what the cookie is used to give access to affects the severity. Been able to post messages as someone else, social engineer could allow an attacker to gain an elevated level of access. There is no silver bullet solution but implementing short session timeouts, deleting cookies once a user logs out, setting HTTP only flag and trying to eliminate cross-site scripting from your site will help alleviate issues surrounding cookie poisoning of the stealing of cookies. Hashing the token by using unique features from the client like IP or not unique but the browser been used would make the attackers attempt far more difficult. The authors were able again logged in as Maria but then the authors were able to post into the customer forum as (Michael Nancarrow 10364818), the poisoning code that has been used into the message field of Marias post:

$< script > document.cookie =$
$"custnum = 103646818" < /script >$

However, after executing this attack, the authors had successfully stolen Michaels cookie by using his customer number instead of Marias thus allowing the attacker to post to the forum as Michael. Once the authors clicked back into the customer forum the authors were posting as Michael without having to log out or know Michaels password.

*h) Cryptography issues:* Would the authors log onto a banking application over HTTP? No chance. HTTP is the telnet of SSH. All data would be in plain text and wouldnt offer any challenge to the attacker once this data is intercepted via a sniffer or other device. A key logger would be one of the few way an attacker could retrieve a users passwords but even if the attacker was able to run a TCP dump on either the network port connecting the victims machine or via airsnort, depending on the RSA or SSL key used, there is little risk of the attacker been able to convert this into usable data. This site should be using HTTPS. The lack of any form of cryptography on the site on any of the services provided by the site makes a well-placed attackers objective far easier by been able to read every transaction in plain text.

*i) Broken caching:* Neither cache-control or pragma are set on this website. By default, a response is cached if the requirements of the request method, request header fields, and the response status indicate that it is cached. Any form of expiry reduces the time frame an attacker can exploit a vulnerability. Not allowing for a cookie to expire means that an attacker can lift the cookie from any machine the real user used to authenticate to an application and use that.

*j) Pragma:* Is set on the server to tell the client that its not to cache any of the information locally. Every time the client must request the data required from the server which increases network traffic but ensures the data is the most update. If cookies arent set and stored locally, an attacker cannot use this method to gain access. The server doesnt accept cached information in this case.

*k) Un-validated user input (Severity-Medium/High):* The checks should be performed on the server side at the very least. Implementing them on the client side is useful and would reduce the amount of traffic between the client and the server but as discovered during this assignment, its trivial to bypass client checks. Expecting all the data been sent to you in a particular format is a bad idea. As will be demonstrated later, the authors were able to by the account number validate check and password.

*l) XSS broken authentication (Severity-High):* The most common of all the publicly reported security vulnerabilities.

*m)Mail relay service (Severity-Medium):* If the VM hosting this platform had Internet access this would have been exploitable. If the site relayed it would become blocked by ISPs and SPAM services. Valid mail would be dropped us less the IP was white-listed. An attacker could spoof mail to an e-mail address, a savvy user would look at the headers of the mail received and reasonably assume it was from the Credit Union.

### C. Security Recommendation

1- Poor Error Handling generic errors should be returned to the client side without references. All errors can still be logged to help the system administrator to troubleshoot any user errors by searching through logs. These, however, shouldnt be displayed to the client. Having generic error pages with Please contact the helpdesk for almost every error can frustrate the client but its a small price to pay for thwarting an attacker from gaining valuable information.

2- Invalidated user input the checks should be performed on the server side as well as the client side. Setting the lengths of variables and what characters can be entered on the server side reduces the risk of an attacker been able to cause a stack overflow or been able to input a script.

3- Cookie poisoning there is no silver bullet solution but implementing short session timeouts, deleting cookies once a user logs out, setting HttpOnly flag and trying to eliminate cross-site scripting from your site will help alleviate issues surrounding Cookie poisoning of the stealing of cookies. Hashing the token by using unique features from the client like IP or not unique but the browser been used would make the attackers attempt far more difficult.

4- XSS broken authentication implement HttpOnly cookies. A set of strong authentication and session management controls.

5- Broken session management restricting the number of attempts a user may try and authenticate. Implementing a time-out period before a user is able to log on again. On the social side, many applications now send an e-mail to a completely separate account informing the real users that another user is trying to authenticate as them. Taking IP location and where a user normally logs on from. If its different, further preset questions should be asked of the user to ensure the right person is gaining access. This may be a small inconvenience on a valid user but will thwart many attackers.

6- Broken access control setting a minimum requirement for passwords. Ensuring that a password must contain upper and lower case, numbers or special characters and have a minimum length of 7 characters. Not allowing easily guessable password like password, ensuring that passwords expire and cannot be reused. Never store passwords in plain text and avoid using the same root password for all systems for Ease of use. If a password is been transmitted it should be over a signed SSL connection. Allowing administrators to only log on from certain IP ranges by implementing ACLs. Use of one-time used passwords like RSA key for Administrator access. Avoid using usernames like admin/root/boh. Avoid trust relationships between components.

7- Cryptography issues the lack of any form of cryptography on the site on any of the services provided by the site makes a well-placed attackers objective far easier by been able to read every transaction in plain text. Network sniffers and Airsnort type applications would give an attacker a very easy method of gaining access that would be difficult for an administrator to differentiate against. It raises the question if the valid user initiated a transaction or an attacker who sniffed/found/hacked the valid users credentials.

8- Broken caching enable cache control and for vital pages like login etc, ensure these arent cached by setting pragma.

9- Directory traversal setting a minimum requirement for passwords. Not allowing directory listing by configuring the .htaccess file and configuring the /etc/conf/httpd.conf . Ensure the Option Indexes is set correctly so an attacked cannot browse every file in the directory. In IIS which this system is running from, directory listing is disabled by default so don't enable it. If for some reason it was enabled, it can be removed by double-clicking on directory browsing from the user interface of ISS, click on Actions, and disable from there.

10- Mail relay service ensures only authenticated users can real messages. Disable anonymous access and allow all only computers which successfully authenticate to the mail service (probably running MS Exchange) to send mail. At the very least basic authentication should be checked but integrated Windows authentication maybe preferred depending on the setup.

## IV. Conclusion

Data breaches are increasingly becoming a major issue with the advances in technologies. Increased storage of electronic data and better technologies to gain access to different forms of data has increased the susceptibility of organisations such as financial services firms and health-care providers who store sensitive information vulnerable to data security breaches. Data breaches are a major cost to the society, and the data protection act aims to protect personal data. The data protection commissioner has developed a code of practice and guidelines to ensure the security of personal data held by the organisation in Ireland. Despite the efforts to ensure data security, the number of data security breaches continues to rise over the years. Statistics shows that the total security breaches in Ireland rose by 47% in two years time. Data security breaches are not just a problem in Ireland but a global issue. The largest data breach of the century was by Heartland payment systems where almost 130 million records were lost [35].

The data security threat is only expected to rise over the coming years with the rise in new technologies such as cloud computing. The modern technology trend of cloud computing that are considered as an effective method for data storage is vulnerable to data theft thereby increase the data security threat. Some countries in EU are already reporting concern on data security with cloud technology. Although, EU directive and Irish data protection law provide more security to individual privacy and data security when compare to the US, there is still a continuous need to review the data security policies and guidelines. The Irish data protection acts are currently developing in line with security requirements, and this trend needs to be continued with the new technological advancements. In time, there might needs to review the data protection act in Irish law and in the EU and can even force to add new data protection and privacy legislation based on the changing data security requirements.

In addition, this paper presents a simulation study network attack scenarios. The main point of designing virtual network attack environments is to create a sandbox that allows the authors to perform such experiments from the real assets and at a low cost. The outcome of this experiment can be used as a recommendation in the real IT infrastructure. The core idea of the case study is to examine the website that has been compromised by various attacks. To simulate this attack scenario, the authors used many open source tools like Graphical Network Simulator (GNS3), Oracle VM Virtual Box and VMWare workstation. The authors used different forensics tools to detect criminal activity from the victim machines, for example, Wireshark, Volatility, Linux dd and HxD.

The future of authentication in the authors opinion is by no means clear. The Internet is about communication. Its primary function is the transmitting, storing and availability of information.

With alternate paths to various destinations, ensuring data transmitted over these paths isnt copied, altered or compromised is against the very protocols designed which established the Internet. The Internet was not designed to be secure, it was designed to be resilient. When the fundamental principals which allowed this were based on open protocols its only a matter of time before any secured connection over it is breached. Users are demanding that authentication methods become to be simpler and more secure. The average end-user doesnt know or care if its via IPv4, IPv6, IPSec, Token ring or 2 tin cans linked together by a taut piece of string. Its just supposed to work. Every form of encryption to date has been broken from ROT13 to SSL. The Enigma code was broken. The latest SSL certs will be compromised. Its the authors opinion that in time anything can be broken.

## Acknowledgment

The authors would like to acknowledge the support of by the Insight Centre for Data Analytics and UCD centre for cyber security and cyber crime Investigation.

## References

[1] R. J. Deibert and R. Rohozinski, "Risking security: Policies and paradoxes of cyberspace security," *International Political Sociology*, vol. 4, no. 1, pp. 15–32, 2010.

[2] U. DoD, "Department of defense strategy for operating in cyberspace," *July. www. defense. gov/news/d20110714cyber. pdf (accessed 14 September 2013)*, 2011.

[3] J. H. Saltzer, D. P. Reed, and D. D. Clark, "End-to-end arguments in system design," *ACM Transactions on Computer Systems (TOCS)*, vol. 2, no. 4, pp. 277–288, 1984.

[4] G. I. Zekos, "Personal jurisdiction and applicable law in cyberspace transactions," *The Journal of World Intellectual Property*, vol. 3, no. 6, pp. 977–1016, 2000.

[5] H. L. Armstrong and P. J. Forde, "Internet anonymity practices in computer crime," *Information management & computer security*, vol. 11, no. 5, pp. 209–215, 2003.

[6] H. Samuel. (2007) Petite anglaise blogger wins sacking case. [Online]. Available: http://www.telegraph.co.uk/news/1547113/Petite-anglaise-blogger-wins-sacking-case.html

[7] T. McIntyre. (2006) Online anonymity - ryanair edition (continued). [Online]. Available: http://www.tjmcintyre.com/2006/05/online-anonymity-ryanair-edition.html

[8] L. news and guidance from pinsent Masons. (2002) Totalise v motley fool. [Online]. Available: http://www.out-law.com/page-8699

[9] C. J. (2012) Emi records (ireland) limited & ors v the data protection commissioner, [2013] iesc 34 (2013). [Online]. Available: http://www.out-law.com/page-8699

[10] S.-A. Hinfey, "blockingprogress: the irish high court decision in emi v upc," *Journal of Intellectual Property Law & Practice*, vol. 6, no. 7, pp. 494–501, 2011.

[11] J. Delahunty. (2007) Belgium court orders isp to block illegal downloads. [Online]. Available: http://www.afterdawn.com/news/article.cfm/2007/07/04/belgium-court-orders-isp-to-block-illegal-downloads

[12] D. E. Bambauer, R. J. Deibert, J. G. Palfrey, R. Rohozinski, N. Villeneuve, and J. Zittrain, "Internet filtering in china in 2004-2005: A country study," *Berkman Center for Internet & Society at Harvard Law School Research Publication*, no. 2005-10, 2005.

[13] S. Collins, A. Harbison, V. Mee, R. Moore-Vaderaa, C. Murphy, O. OConnor, and D. Moore, "Good practice guide to electronic discovery in ireland," *eDiscovery Group of Ireland*, 2013.

[14] L. S. of Ireland. (2007) Civil litigation discovery in the electronic age: Proposals for change. [Online]. Available: http://www.lawsociety.ie/documents/news/Law%20Society%20Report.pdf

[15] D. P. Commissioner. (2011) Breach notification guidance. [Online]. Available: https://www.dataprotection.ie/docs/Data-Breach-Handling/901.htm

[16] I. Examiner. (2015) Serious hse data breaches risk patient safety. [Online]. Available: http://www.irishexaminer.com/viewpoints/analysis/serious-hse-data-breaches-risk-patient-safety-239828.html

[17] C. Sheehy. (2008) Stolen hse laptop leaves staff open to identity theft. [Online]. Available: http://www.herald.ie/news/stolen-hse-laptop-leaves-staff-open-to-identity-theft-27887535.html

[18] R. Burke. (2010) Hse 'rocked' by security breach on 1,500 patient records. [Online]. Available: http://www.independent.ie/business/irish/hse-rocked-by-security-breach-on-1500-patient-records-26690497.html

[19] E. Edwards. (2015) Hse breached rights of employee by disclosing salary to ex-wife. [Online]. Available: http://www.irishtimes.com/news/ireland/irish-news/hse-breached-rights-of-employee-by-disclosing-salary-to-ex-wife-1.2259714

[20] D. P. Commissioner. (2015) Responsibilities of data controllers. [Online]. Available: https://www.dataprotection.ie/docs/Responsibilities-of-data-controllers/1243.html

[21] P. Williamson. (2007) Nationwide fine for stolen laptop: The nationwide building society has been fined 980,000 by the city watchdog over security breaches. [Online]. Available: http://news.bbc.co.uk/2/hi/business/6360715.stm

[22] D. P. R. Group. (2010) Data protection. [Online]. Available: http://www.justice.ie/en/jelr/dprgfinalwithcover.pdf/Files/dprgfinalwithcover.pdf

[23] D. J. Karl, "State regulation of anonymous internet use after aclu of georgia v. miller," *Ariz. St. LJ*, vol. 30, p. 513, 1998.

[24] J. D. Wallace, *Nameless in cyberspace: Anonymity on the internet*. Cato Institute, 1999.

[25] Paypal. (2013) Privacy policy. [Online]. Available: https://cms.paypal.com/uy/cgi-bin/marketingweb?cmd=-render-content-content-ID=ua/Privacy-popup-locale.x=en-US

[26] J. T. Soma and N. A. Norman, "International take-down policy: a proposal for the wto and wipo to establish international copyright procedural guidelines for internet service providers," *Hastings Comm. & Ent. LJ*, vol. 22, p. 391, 1999.

[27] D. of Justice. (2011) The usa patriot act: Preserving life and liberty (uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism). [Online]. Available: http://www.justice.gov/archive/ll/highlights.htm

[28] K. Gates. (2006) E-discovery amendments to the federal rules of civil procedure go into effect today. [Online]. Available: http://www.ediscoverylaw.com/2006/12/articles/news-updates/e-discovery-amendments-to-the-federal-rules-of-civil-procedure-go-into-effect-today

[29] A. Travis. (2011) Air passenger data plans in us-eu agreement are illegal, say lawyers. [Online]. Available: http://www.theguardian.com/world/2011/jun/20/air-passenger-data-plans-illegal

[30] M. D. Birnhack, "The eu data protection directive: an engine of a global regime," *Computer Law & Security Review*, vol. 24, no. 6, pp. 508–520, 2008.

[31] A. Al-Mahrouqi, S. Abdalla, and T. Kechadi, "Cyberspace forensics readiness and security awareness model," *International Journal of Advanced Computer Science and Applications*, vol. 6, pp. 123–127, 2015.

[32] ——, "Network forensics readiness and security awareness framework," in *International Conference on Embedded Systems in Telecommunications and Instrumentation (ICESTI 2014), Algeria, October 27-29 2014*, 2014.

[33] A. Al-Mahrouqi, P. Tobin, S. Abdalla, and T. Kechadi, "Simulating sql-injection cyber-attacks using gns3," *International Journal of Computer Theory and Engineering*, vol. 8, no. 3, pp. 213–2017, 2016.

[34] A. Al-Mahrouqi, S. Abdalla, and T. Kechadi, "Efficiency of network event logs as admissible digital evidence," in *Science and Information Conference 2015, London, United Kingdom, 28-30 July 2015*, 2015.

[35] N. Yau. (2011) Largest data breaches of all time. [Online]. Available: http://flowingdata.com/2011/06/13/largest-data-breaches-of-all-time