Harmonisation of Digital Privacy Law and Practice: The Jersey Workplace Case Study

Ali Ahmed1† and David Booth2††,

1† Cairo University Egypt, 2† University of Liverpool/ Laureate Education

Summary
This paper thoroughly investigates the digital privacy provisions in the island of Jersey. This is mainly done by examining the two key pieces of legislation with which any workplace must comply with. Those legislations are: The Employment (Jersey) Law 2003, and the Data Protection (Jersey) Law 2005. Neither law has digital privacy provisions per se, but these are the two prevalent pieces of legislation governing employer-employee relations in the island of Jersey at present. The study relates the local legislation in the island of Jersey to its UK and European counterparts identifying the missing parts. To realise that purpose, the work introduces a case study of the Lysaght's workplace and investigates its compliance of with the Law. The study highlights the areas of concerns and provides recommendations for both employers and government. This work updates employees with regard to their rights and entitlements in the Island of Jersey. It can be used as the basis for steering the future judicial review of this area, to ensure the island of Jersey remains in compliance with its peers both domestically and internationally. It also can be used to assist IT professionals and employers in ensuring their approach to the digital privacy of their staff is handled entirely with compliance with the expectations and requirements of all key stakeholders.

Key words:
Digital Privacy, Island of Jersey, jurisdictions, Employee Rights.

1. Introduction

The notion of an individual's right to digital privacy in a workplace is something that must, logically, be considered from multiple perspectives. It is logical to appreciate those perspectives may vary in objectives. The notion of 'privacy' is multi-fold and can be categorized into a number of headings including, but not limited to, those indicated in Table 1.

Table 1: Examples of the 'privacy' concept

Type	Example of method of protection
Physical	Article 8 of the European Convention on Human Rights cites "[e]veryone has the right to respect for his private and family life, his home and his correspondence" [1]
Medical	The Hippocratic Oath [2] has a confidentiality clause preventing a doctor from breaking a patient's confidence
Political	The notion of a secret ballot [3] conceptually ensures people can vote anonymously
Financial	'Insider dealing' is typically considered an offence (e.g., the Company Securities [4]
Informational	Data Protection is often given statutory footing (e.g., the Data Protection (Jersey) Law 2005 [5]

The issue of digital privacy is becoming increasingly prevalent in a world where more people are connecting to the Internet than ever before [6]; where there is a tendency to access and share information both inside and outside the traditional working environment on popular social networking sites [7], and where employees' access to computer facilities is widely-regarded as being an intrinsic part of being employed in the modern workplace [8]. In many aspects of privacy, studies show that people are prepared, in certain situations, to essentially trade-out aspects of their own privacy for a sense of increased security and safety in their daily activities [9]. while this approach certainly draws criticism [10], it is, for many of us, a reality. A well-known example of this is the increased airport security with invasive search methods as a way of reducing the threat of terror attacks on commercial airlines [11]. While a society in which no information were stored on any citizen would be impossible to administer, it would be appropriate to conclude that a society where no privacy is afforded to citizens would not necessarily be secure [12]. Blanger and Crossler observe that one of the issues with research into any area of information systems privacy is that many of the established research works and surveys undertaken are highly USA-centric and while this does not in any way impede the validity of, or interest in, the research itself, it becomes immediately apparent that the status quo in any one jurisdiction does not indicate the global view on this issue [13].
As Allen et al observe, there is" primary tension between employer interests in surveillance and employee interests

Manuscript received June 5, 2016
Manuscript revised June 20, 2016

in privacy" [14]. In other words, employers and employees approach the topic of workplace privacy, digital and otherwise from, at least initially, fundamentally different perspectives. Businesses rely upon the trustworthiness of their staff to continue functioning optimally, but that sense of trust is both delicate to maintain, and reciprocal in nature. Disgruntled employees who feel unable to trust employers underperform, being at greater risk of leaking sensitive corporate information, and becoming more disruptive to their colleagues [15, 16]. Privacy is of considerable interest to IT professionals, and any other members of staff who are actively engaged in the practice of monitoring the digital activities of their staff, or monitoring their staff digitally as the two are not always the same thing. It is of vital importance that IT professionals are confident, when considering the balance between what is technically possible and what is legally permissible, that their practices and procedures fall on the right side of the law.

The island of Jersey is a world-renowned offshore finance centre, attracting significant business annually as a result of its geographical location, independent legal framework, low taxation rates, and well-developed financial services industry [17]. The island is ranked as the world's highest-rated offshore finance centre [18] by an international survey, on a number of occasions [19]. While there are differences in the interpretation and application of workplace digital privacy practices between jurisdictions, often based on their respective legal frameworks [20], there are commonalities shared between most jurisdictions. This is of interest from a Jersey-perspective as, while being situated geographically in-between England and France, Jersey as a member of the Channel Islands is not a part of the European Union. It simply means it faces a number of somewhat unusual issues when investigating digital privacy from a legal perspective.

2. Background and Literature Review

In order to provide a sense of perspective on this study, there is a need to examine the legal framework within which the notion of digital privacy in the Jersey workplace finds itself. Jersey is, as shall be discovered soon, subject to a number of unusual considerations, which set it apart from larger jurisdictions such as the United Kingdom.

2.1 Employee Rights in the island of Jersey

The island of Jersey is unique in a number of contexts. It is the largest of the Channel Islands that is a Crown dependency, which affords the island autonomy in its own administration, while retaining strong links with the government of the United Kingdom over a small number of key issues such as military defence in times of war [21, 22]. Residents of Jersey are considered British citizens. while the United Kingdom actively represents the Channel Islands' collective interests internationally [23], Jersey is both self-governing, and judicially independent from the United Kingdom. Furthermore, it is not a part of the European Union in its own right, beyond having a free trade relationship with the EU under the provisions of Protocol No 3 of the UK's Treaty of Accession to the European Economic Community of 1972 [24]. This makes it, in the eyes of the EU, a" third country" [25]. In practice this means that laws, conventions, treaties, directives, regulations and other legislative acts of both the UK and the EU must generally be ratified under local law for them to have legally-binding effect within the island [26]. Where there is a lack of local legal precedent, judgments and legal positions of the other Channel Islands, the UK and the EU may be considered persuasive, but are not binding on Jersey courts [27].

Prior to 2005, Jersey had little in the way of statutory protection for the rights of employees in the workplace. The few issues that were addressed were generally covered under one of the following five pieces of legislation [28]: -

1. The Health and Safety at Work [29];
2. The Industrial Disputes [30];
3. The Payment of Wages [31];
4. The Termination of Employment - Minimum Periods of Notice [32]; and
5. The Terms of Employment (Jersey) Regulation [33]

There was considerable gaping in-between this coverage, with issues such as unfair dismissal and a minimum wage not being addressed at all. In fact, the system as it then was, was indeed in need of review that it was cited as being" out of date, fragmented and ineffective" [28].

After a reasonably comprehensive review process, which involved polling the island's workforce to gauge their opinion and garner feedback about key issues that needed to be addressed, together with a review of employment legislation and practice in various other jurisdictions including the United Kingdom, the Isle of Man, Bermuda and New Zealand, the" Draft Employment (Jersey) Law 200-" was submitted by the Employment and Social Security Committee for consideration, on 08 October 2002 [34]. The main driver behind this draft piece of legislation was the lack of a minimum wage system in the island, and the Draft Employment (Jersey) Law 200- was essentially built as a construct to frame and support the introduction of a minimum wage system in Jersey. As with many such constructs, additional

suggestions were contributed during the process and, ultimately, this piece of draft legislation matured into the Employment (Jersey) Law 2003 [35], which came into force with effect from 01 July 2005. It addressed,

consolidated and updated the island's position on a number of topical issues including minimum wage, unfair dismissal, minimum rest periods, annual leave entitlement, termination of employment, and holiday pay for temporary staff [36].

2.2 Rise of Workplace Disputes

Another major initiative introduced as a result of the Employment (Jersey) Law 2003 [35] was the creation of a tribunal (the" Jersey Employment Tribunal" [37], who would have responsibility for hearing claims in respect of both statutory and contractual employment-related matters [38]. It should be noted that recourse to the Jersey Employment Tribunal is not the only avenue through which an aggrieved party may seek satisfaction. There are, additionally, the Petty Debts Court [39], the Magistrate's Court, and the Royal Court [40], and JACS offers independent, free legal advice to interested parties, often resulting in conflict resolution prior to legal action or a tribunal hearing. Figure 1, shows an analysis of the number of cases that have been heard by the Jersey Employment Tribunal, per year, since its inauguration in 2005.

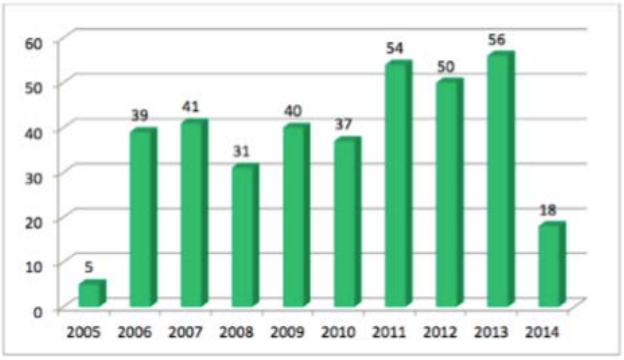

Fig. 1 Employment Tribunal Cases per Year [41].

Given Figure 1, the Employment Tribunal issued fifty-six judgements 2013. With an estimated working population of 56,290 as at June 2013 [42], that suggests an average of one judgement per thousand employees. while this figure may appear insubstantial, if the same ratio were applied to a larger jurisdiction such as the United Kingdom, it is believed to rise to a" serious" concern.

Figure 2 shows a summary of new employment claims raised during 2013, as produced by JACS in their 2013 annual report [43]. The disparity between the statistics shown in figures 1 and 2 indicates that the vast
majority of the judgements issued by the Employment Tribunal in 2013 were not in respect of new matters, but rather cases that had started in previous calendar yearsa.

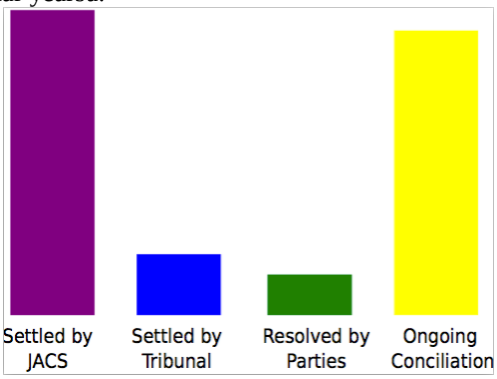

Fig. 2 Number of Claims in 2013.

2.3 Prevalent Legislation

While the Employment (Jersey) Law 2003 was generally well-received and is still the most prominent piece of employment legislation in the island, it does not adequately address all scenarios [44]. That is why there have been a number of recommendations put forward by local bodies, such as the Employment Forum in subsequent years, suggesting codes of practice be implemented to add further clarification to those scenarios [44].

As a self-regulating territory, Jersey needs to keep abreast of developments in Europe and other key global jurisdictions, in order to ensure its policies and practices are both current, and well-regarded by its peers in the international community. A good example of this in operation is the formal incorporation of the European Convention on Human Rights (ECHR) [1] into a piece of domestic legislation. while the ECHR has had a measure of effect in the island since 1954, discussions in years gone by which centred around Jersey formally ratifying the ECHR via a piece of domestic legislation were met with disapproval by the Home Office in London. It was felt that Jersey acting ahead of the UK in ratifying an international convention would be inappropriate [45] bearing in mind the UK's historical responsibility for Jersey's international relations. Since the enactment of the Human Rights Act 1998 [46] in the UK, however, Jersey received approval from the Home Office to move forward with its own version of that legislation, and the Human Rights (Jersey) Law 2000, which cites as its main object" [giving] further effect to rights and freedoms guaranteed under the European Convention on Human Rights" [47], was brought into force, in the island of Jersey, with effect from 10 December 2006.

[a] This is actually supported by additional figures in the aforementioned JACS report.

In addition to the two aforementioned pieces of legislation, JACS identify a number of additional laws which are of relevance to employment in the island [48]. However, the majority relate to very specific areas of concern, such as the Rehabilitation of Offenders (Jersey) Law 2001[49], and the Control of Housing and Work (Jersey) Law 2012 [50]. The only other live piece of legislation which is of significance to our study is the Data Protection (Jersey) Law 2005. Data protection, that is," the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information" [5], is a matter of considerable significance in most developed countries, and Jersey is no exception.

The ubiquity of Internet access nowadays in developed countries such as Jersey [51] means that not only is there an abundance of personal data published to, and consumed on, the Internet, but that our attitudes towards the dissemination of that data are changing globally, from a societal perspective [52]. As Dillon opines," [w]ith every passing age ... there is more information, and this information is cheaper and easier to get to, [with] less need for a single authority to control it" [53]. While we concur with Dillon's view, the purpose of data protection legislation is not to control the data in and of itself, but rather to offer protection to the individual who is the subject of the data ("data subjects", as defined in the law). This is to ensure a degree of control over the data rests with them, over those who would ultimately seek to process that data ("data controllers", again, as defined in the law). Unusually, both the islands of Jersey and Guernsey have their combined data protection policies administered by a single Data Protection Commissioner, currently Mrs Emma Martins [54], who practices from Jersey. Mrs Martins was interviewed in her capacity as Data Protection Commissioner in support of this research, and shall discuss her considerable input in the following sections.

2.4 Digital Privacy Provisions in Existing Framework

There are no provisions within the Employment (Jersey) Law 2003 [35] which overtly relate to digital privacy in the Jersey workplace. This position is confirmed by JACS [55]. The researchers were, instead, referred to the offices of the Data Protection Commissioner, as JACS felt this area would fall under the remit of Data Protection law, which they make a point of not advising on [55]. This latter point accounts for the distinct lack of documentary best practice guidance on JACS website relating to data protection, or specifically to digital privacy in the Jersey workplace. It is the considered opinion of the professionals who contributed to this work during their respective interviews that there is no form of legal protection currently afforded to digital privacy within the Jersey workplace [56, 57].

2.5 Works in Development

Currently, there are two significant developments related to this research. Firstly, the Freedom of Information (Jersey) Law 2011 [58], which has already been approved, but is not due to come into force locally until the end of 2015[McIntosh, 2011]. Secondly, the forthcoming Pan-European data protection law [56, 57]. While it may sound, at first instance, like the Freedom of Information law has direct bearing upon this research, unfortunately it cites as its remit" the supply of information held by public authorities" [58]. Thus, it is considered by legal professionals as having little to no bearing on the general state of workplace digital privacy in the island [56]. The Freedom of Information (Jersey) Law 2011 [58] makes provision for individuals possessed of a general right to the information they seek, to apply for disclosure of that information from public officesb. Such requests can only be withheld in certain restricted situations, such as where the public office considers the request vexatious c , or where the information is readily available to the applicant by other meansd. In practice, this means that civil servants in the island of Jersey will need to operate in a clean manner, as previously non-disclosable information may legitimately come to light under this act [56].

Significant changes are also taking place with regard to the data protection standards as established within the EU [57]. Specifically, the EU is looking to consolidate and replace its inconsistently-implemented and applied data protection standards to cover all member states equally [59]. From Jersey's perspective this creates a number of interesting issues. While not part of the EU, Jersey is presently entitled to engage in the free

trade of data with EU member states following a comprehensive review of its data protection legislation by the European Commission. A 'comitology procedure', which culminates in the issuance of an 'adequacy decision' if the jurisdiction being reviewed meets EU data protection standards [60]. While changes to the EU data protection provisions would therefore not have direct applicability to Jersey with immediate effect, nor would they fundamentally compel Jersey to follow suit, it would almost certainly be the case that Jersey would ultimately lose its adequacy status in case local legislation is not revised to reflect the changes by EU [57]. It remains to be seen whether this would involve a full comitology

[b] section 8

[c] section 21

[d] section 23

procedure being called for, or whether satisfaction of the incorporation of the key points would suffice.

2.6 Corporate Data Storage

The value of data to the business world as a whole is incalculable. Data represents the major building block upon which business functions. Not only is there an understandable need to retain that data in order to run a business effectively, but in many instances there is a legal requirement to retain certain types of data for given periods of time. There are plenty of readily available examples of poor data management practices leading to costly outcomes for business [61] and the need for better practices [62]. While the recommended and required periods of data retention are generally well-documented under the various laws to which they relate. In Jersey, the Data Protection (Jersey) Law 2005 stipulates as its fifth principle that" [p]ersonal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes" [63]. Table 2 outlines a number of these types of data, their required or recommended periods of retention, and the body or law which stipulates this to be the case.

Given Jersey's reputation as a top-tier offshore finance centre, many Jersey-based businesses, particularly those in the finance industry, are keen to identify and preserve the geographical location of the data itself, once moved into cloud storage. This is predominantly because many jurisdictions actively comply with, inter alia, the United States' Foreign Account Tax Compliance Act (FATCA) legislation (encompassed within the U.S. Hiring Incentives to Restore Employment (HIRE) Act, 2010), and Jersey's reputation would be substantially tainted if it were unable to guarantee the confidentiality of the data it holds within the cloud structures. Being able to restrict the storage of cloud data to desirable jurisdictions has enabled local cloud solution providers such as Calligo [64] to establish their niche and, interestingly, the issue of U.S. access to cloud data stored on foreign soil is being hotly debated through an open court case at present. Microsoft are engaged in an on-going legal battle to have a search warrant issued by the United States District Court for the Southern District of New York overturned, as this warrant demands Microsoft relinquish data stored on a cloud server in Dublin, Ireland, to a court in the U.S. Microsoft object on the basis that they feel the U.S. warrant should not apply, as the data is held outside the remit of U.S. law [65]. As should be readily apparent, this case could potentially have far-reaching implications for many cloud providers, and is being heralded by many as a landmark case both in terms of cloud security, and the seemingly fast-approaching global reach of certain U.S. legal motions [66].

Table 2: Recommended and required periods of data retention

Type		Example of method of protection
Financial	Due Diligence	Five years from the end of the relationship with the client (Article 20(3) of the Money Laundering (Jersey) Order 2008) [67]
	Transactional	Six years [68]
	Governance	Ten years [68]
	Pay As You Earn (PAYE)	Three years, plus the current year [69]
Legal	Wills/Probate	As long as possible, but at a minimum for the life of the client [70]
	Trust Deeds	Six years from the determination of the trust in the UK [71]; three years from the determination of the trust in Jersey
	Contracts	Ten years [68, 73]

2.7 Conflict and Overlap with Current Framework

Merabet [74] illustrates how goodwill in the workplace can be shattered when employees resort to the use of social media to criticise their employer. In certain industries such as the medical profession, goodwill takes on a much more serious and potentially even life-and-death nature, as nurses are often called upon to work in quite stressful and demanding conditions, where their goodwill is regularly tested. Clover [75] and Gordon [76] both published interesting works in testimony of this fact. There is a perceived threat to the goodwill between employer and employee where an employer is seen to take steps which the employee translates into an assumption that the latter is untrustworthy, or in need of monitoring to bolster their productivity. In fact, this is where a significant number of workplace disputes arise. Milner [56] suggests that a court will generally consider whether an employer has been reasonable in their chosen use of surveillance, monitoring and logging solutions, and this is backed-up by Martins [57], who confirms that her role as Data Protection Commissioner involves advising employers, who may have undertaken surveillance steps without first checking to make sure they are justifiable. Focusing on this issue from a Jersey-centric perspective, there is no form of statutory protection for an individual's right to digital privacy in the Jersey workplace. Furthermore, the provisions of Article 8 of the ECHR, as ratified by the Human Rights (Jersey) Law 2000 [47], only extend to a working relationship with the State. While the States of Jersey are a major employer in the island, accounting for approximately 12% of all jobs on the island in their non-trading departments [42], they are by no means the sole employer in Jersey. In fact, the

States of Jersey Statistics Unit's report for 2013 shows that, of the 56,290 people working in the island as at June 2013, 49,360 of those worked in the private sector, so the private sector accounts for approximately 88% of all jobs in the island [42].

The greatest measure of protection afforded to the Jersey individual in relation to their data comes from the Data Protection (Jersey) Law 2005 [5], yet this law is not a privacy law [57]. Its provisions do not extend beyond the manner in which data is handled, to the moral and social issues underpinning why that data is being collected in the first place. Specifically, the Data Protection (Jersey) Law 2005 oversees how data controllers (i.e. employers for our present purposes) maintain, control, and use data on behalf of data subjects (i.e. employees in our present example), and ensures that data subjects are able to have access to the sum of all the data that is held by a data controller in relation to the data subject, upon payment of a nominal fee. Breaches of the Data Protection (Jersey) Law 2005 as, for example, where a data controller has taken data on a data subject and passed it to a third party without the express consent of the data subject, are actionable, and enforceable at law.

3. Case Study

3.1 Methodology

Digital privacy becomes an issue when:

1. an employer offers the use of corporate facilities for private purposes
2. an employee brings their own device into the corporate environment
3. logging of media used for work and private correspondence takes place
4. undisclosed members of staff have access to employees' personal data (although this is also a data protection issue)

There is a need to validate the compliance of the work practices in a typical workplace in the island of Jersey against the multiple jurisdictions the island is operating on. This is a qualitative positivist study that attempts to increase the understanding of how typical workplaces in the island of Jersey operate regarding privacy provisioning. Since this research addresses the description question of" how workplaces in the island are operating especially when multiple jurisdictions are to be followed?", there is a pertinent need for a case study that closely observes, investigates, and collects data in natural settings [77]. "Clearly, the case study research method is particularly well-suited to IS research, since the object of our discipline is the study of information systems in organizations" [78]. The case study has to investigate what an international business in the island lacks to comply with the privacy legislations. The data collection is done through interviews and workplace observations. In order to authoritatively examine the current state of affairs, interviews will be conducted with a well-known Jersey employment Advocate [56], and the chief of the local Government's Data Protection Commission [57]. Once the data is collected from interviewee, a comparative Analysis of current Law provision in the island to what is actually a typical workplace in the island is operating on will be conducted. One of the predicted limitations of this research methodology is the inability to generalise the research findings into some best practice guidelines. While the case study selection, as will be shown, is appropriate, further research is needed for such a generalisation.

A case study was undertaken at the sponsor's [79] work premises between April and June 2014, analysing all methods of data collection and archiving across both live and backup environments, and documentation in support of such practices. Of the thirty-one members of staff, twenty-eight have their own dedicated workstations, which comprise a telephone with direct dial extension, and a networked, windows-based computer workstation. The remaining three members of staff represent a common filing and mail team, who work at three different locations on the premises, across six windows-based computer workstations, responding to the demands of staff, and external courier services. The sponsor's office is spread across two floors in one building, and building security comprises a set of motion detectors at various locations around the office premises, tied to a centralised system which records activity 24/7 and sends notifications of suspected break-ins to an offshore data centre for processing. A suite of seven servers (i.e. more precisely six physical and one virtual) represent the backbone of the firm's IT infrastructure. There is an eighth server (i.e. the oldest of a legacy batch of servers), which the sponsor retains off-site, for Disaster Recovery (DR) purposes. This server has not been tested in a simulated DR scenario for over four years, and is due to be replaced shortly. Given the complete lack of use of this server in recent years, and to avoid going off-tangent with the focus of this research, it is being discounted from further analysis. The sponsor's current telephone system was installed when they moved into their new premises in 2000, and does not support the recording of conversations, beyond regular voice-mail functionality. It is for this reason that a virtual call logger has been deployed, to log key data regarding telephone calls made to, and from each employee's extension. Contrary to the stipulations in the sponsor's office handbook, it has become convention for staff to store data they wish to keep, but which is not so sensitive as to

warrant backing-up on a nightly-basis, on the local hard drives of their respective workstations. Access to the servers is restricted to two individuals: the managing director, and the IT department head. Access is periodically delegated to third parties as may be required for the completion of their respective works. However, any such work is undertaken on-site, and under the direct supervision of either of the aforementioned individuals. Such access is typically given to two external companies, one of whom services the sponsor's UPS (Un-interruptible Power Supply), and the second of whom services and updates the sponsor's leased MFPs (multi-function printers). User-name and password data is never shared with these third parties.

One of the paramount aspects in designing/selecting a case study is its significance. The selection of the sponsor's workplace to undergo the case study is simply because the employer employs a total of thirty-one staff at its physical premises in the island of Jersey, and represents the interests of an international client-base in over 160 jurisdictions around the world. In spite of the scope of its international operations, the sponsor is bound entirely by Jersey's law, making it an ideal candidate for the study. While the case study may not be sufficient to generalise the findings, it serves well understanding how workplaces within the Island of Jersey operate. Another reason for selecting the sponsor's workplace is simply given the ubiquity of computer technology in the modern work environment, employers may find themselves accumulating more data on their staff than might have been the case in years gone by. The sponsor's workplace is an appropriate one to investigate that since staff members are allowed to use company telephone and e-mail facilities for personal matters. They are also permitted to bring their own devices in from home to use on work premises. In such a setting, the privacy provisioning interestingly may need to address many concerns.

3.2 Current Practices: Observations and Data Collection

The sponsor is keen on logging and archiving as much data as is practically possible, for two main reasons. Firstly, for the purposes of business continuity in the event of a significant disaster recovery scenario. The majority of case files are paper-based, and digital data archiving wherever possible is seen as a measure of damage mitigation, as well as sensible business practice. Secondly, to maximise data available for subsequent investigation purposes. The following discussion compartmentalises the sponsor's current digital privacy practices into the key areas of:

1. E-mail correspondence
2. Telephone calls
3. Internet Activity
4. Data archiving/Backup
5. Remote access and Support
6. Cover and Timekeeping
7. Documentary basis for activity logging

Every member of staff with a dedicated terminal has their own bespoke e-mail address. The sponsor's policy regarding the use of e-mail for corporate and personal use is set-out in the office handbook. The sponsor's e-mail system is administered via a combination of Microsoft Exchange Server 2003 on the mail server; MailMarshal Console and Configurator on both the mail server, and a limited number of workstations; Outlook for Office 2010 Standard on every workstation; Outlook for Office 2003 Professional on the mail server; and MailStore Home on a limited number of workstations. Outlook handles the day-to-day administrator of e-mail correspondence for each staff member, and a 2GB mailbox size limit has been placed on each exchange mailbox by the sponsor's IT Department, at server level. Once an individual mailbox exceeds 2GB in size, the mail server sends a daily warning to the staff member concerned, requesting them to reduce the size of their mailbox immediately, but does not otherwise curtail e-mail activity. The employee in question will then typically run a MailStore Home archive operation, to extract old e-mails from their exchange mailbox, and archive them to their local hard drive (i.e. contrary to stipulations in the office handbook). All inbound and outbound e-mails are logged within MailMarshal Console at the server level, and the sponsor uses MailMarshal Console to retrieve any business e-mail it may wish to action (i.e. typically for sending reminders, or analysing complex or problematic transactions, as and when same come to light). The mail retention period has been disabled, meaning the sponsor is able to retrieve any e-mail sent or received from their office dating back as far as 2004. This system does not log internal e-mails, and these are only present in each staff member's exchange mailboxes.

All calls are logged courtesy of the call logging virtual machine, to keep track of the extension dialled to or from; the number called (where this is available); the duration of the call; and the call cost to the company. Unlike call centres and other businesses which engage in the practice of full call logging[e], the content of telephone calls made by the sponsor's staff are not logged. One of the reasons for this is that the telephone system itself is too old to support such a functionality. However, regular reports are generated for the Accounts & HR department, showing staff members who spend more than a given threshold of time on the telephone, for subsequent investigation. The

[e] By which we mean the complete recording of a transcript of the conversation taking place, traditionally for training and quality control purposes

researchers of this study made enquiries of the sponsor as to whether they would seek to log the content of telephone calls should it be functionally possible to do so. They said it would not be their intention, unless they felt they had due cause to do so, predominantly because they insist on written instructions from their clients before taking action.

All employees are given unrestricted Internet access. This means there is no content filtering in place on the network, nor restrictions on which web-sites employees can, or cannot, visit. Obviously this raises a number of security concerns, and the increased risk of exposure to third party viruses, malware and other nefarious programs. The sponsor understands such risk though.

Unfettered Internet access is considered a perk of working at the sponsor's organisation, and functions essentially on an honour system. Employees who are found to be abusing the privilege have it curtailed or removed from their respective workstations. This duty being fulfilled by the IT department head on instruction from the managing director. In such a case, the Internet browsing is redirected to a splash screen by the configuration of a proxy to a specific IP address. The confirmation of this practice is outlined in the office handbook[f]. In spite of the stipulation in the office handbook that all Internet site visits are logged, this practice is not presently in operation. This functionality exists but has not been enabled on the router, thus the threat of logging is used essentially as a deterrent, rather than an actionable policy.

The sponsor uses two systems for data archiving. Firstly, a backup job runs on a nightly basis courtesy of Symantec Backup Exec. This backup routine writes data to one of a series of DLT-3 tapes, which the managing director replaces each morning. The preceding evening's backup tape is retained by the managing director, and taken off-site for security and DR purposes. The second backup method is a more basic set of scripts which runs each evening, and backs up various specific flat files and folders from each of the seven servers, as well as undertaking backups of each SQL database, and an ExMerge operation to extract each staff member's mailbox to an individual'.pst' file [80], which is subsequently backed-up via script. These backup scripts xcopy [81] data to one of a set of 1TB external USB hard drives which, again, the managing director replaces each morning. The preceding evening's backup USB hard drive is retained by the managing director, and taken off-site for security and DR purposes. In order to ensure the 1TB USB hard drives do not fill-up too quickly, the backups are arranged to take place on an incremental basis, meaning only data which has been updated or added will be xcopied to the external hard drive. The USB hard drives are periodically reformatted, to ensure data is kept fresh.

Terminal Services access is restricted to the seven members of the sponsor's management team (i.e. managing director, managing director two co-directors, a consultant, the Accounts/HR department head, the deputy-head of the firm's largest fee-earning department, and the IT department head). In practice only the managing director, one of his co-directors, the Accounts/HR department head, and the IT department head use terminal services.

The sponsor's IT department is keen to use remote support wherever possible to speedup its response time on support calls. A broad range of software is used for this function, which includes two versions of Remote Administrator; LogMeIn[g]; TeamViewer 9; and Remote Access Viewer. This is indicative of the IT department's view that it is better to offer multiple solutions than a single solution, for redundancy purposes (i.e. in case there is some type of service stall which prevents a single remote-access solution being deployable in a given support
scenario). The IT department does not operate a support call docketing system, and staff at the sponsor's work premises simply pick up the telephone, or e-mail the IT department, and receive support on the fly.

Staff members are typically assigned to work in pairs for cover purposes. Specifically, each member of staff is responsible for a given range of jurisdictions, and oversees the sponsor's core work in those jurisdictions. If they are indisposed, however, (typically on annual leave, absent through sickness or in a meeting), their partner covers their workload for them. To facilitate this, each staff member in a pair is given unrestricted access to the mailbox of the other, via Active Directory, at the server level. As with the notion of unrestricted Internet access, this concept of unfettered access to a colleague's mailbox raises a number of security and data privacy concerns that will be discussed later.

There is no automatic method of timekeeping at the sponsor's work premises. Similar to their Internet logging practices, the system works on an honour basis. Each member of staff has a customised spreedsheet workbook into which they enter their attendance times each day. These are submitted at the end of each week via a visual basic macro operation, and are reviewed each Monday morning by department heads, and the Accounts/HR department head.

Passwords are controlled by, and known only to, the IT department, and the person using the password on a regular basis, for security purposes. This procedure again being outlined in the office handbook. While there may be understandable security and data privacy concerns on the part of the staff at this practice, each staff member gives

[f] Under the section "Use of Electronic Mail and the Internet" in the sponsor's office handbook

[g] now disabled on all workstations owing to the decommissioning of LogMeIn Free by the developers

their express consent for this practice to take place, by signing and returning a copy of the office handbook to the Accounts/HR department head. The staff appreciate that a failure to comply with this policy may leave the IT staff with no alternative but to reset passwords to their default values, in the event that accounts need to be accessed in a given staff member's absence. Building security is handled via a system of motion-detection cameras, tied to a centralised system. Access to the building itself is controlled via key and fob, with each staff member having a unique four-digit PIN code to deactivate the alarm system. The Accounts/HR department head controls the list of fobs. Those fobs misplaced are immediately deactivated. There is no policy for locking down USB ports, and/or CD/DVD-ROM drives on any workstation on the premises.

Documentary support for all the sponsor's monitoring and logging practices is outlined in a combination of the contract of employment, and the office handbook. The typical wording of the sponsor's contracts of employment serves to headline the most important piece/s of information on a given topic, and to direct staff to the relevant portion of the most up-to-date iteration of the office handbook, for further information. In the case of digital privacy and monitoring practices at the sponsor's workplace, the template contract of employment states" Policy for the use of e-mail, web, and telephone is set out in the Office Handbook. It must be understood that e-mail, web sites visited, and use of the telephone will be monitored at the management's discretion for the protection of the company. By signing this document, you are agreeing to these conditions."

The sponsor's office handbook clearly states," Use of Electronic Mail and the Internet" that lists of web-sites visited by employees, as well as every e-mail sent and received are logged, and monitored by management. The staff therefore have an overt, explicit understanding by virtue of signing their contracts of employment that logging of their Internet activity, e-mail correspondence and telephone activity takes place, and can be monitored at management's discretion.

3.3 Comparative Data Analysis: Legislative Perspective

The two key pieces of legislation with which the sponsor must be seen to comply are the Employment (Jersey) Law 2003, and the Data Protection (Jersey) Law 2005. Neither law has digital privacy provisions per se, but these are the two prevalent pieces of legislation governing employer-employee relations in the island of Jersey at present. The sponsor's practices are compliant with both pieces of legislation and, as such, there is no immediately pressing need for the sponsor to take any kind of drastic action with regard to its existing practices. However, there are concerns in the current practices.

As has been mentioned previously, the sponsor uses one main shared folder, mapped to commonly-accessible drive to store the bulk of its data, and to share same amongst its staff. This folder is sub-divided into a small number of core folders for items such as debit notes, template letters and precedent forms; and one folder per member of staff. The sum of all sensitive information is stored within that folder structure and, while sensitive files are password-protected. The sponsor is concerned that they may need to improve their network security processes, no information leakage is materialised especially for employees leaving the sponsor's organisation. As was identified previously, the sponsor does not presently use any form of policy editing software to lock down access to USB ports and CD/DVD-ROM drives. This is a risky policy indeed that needs to be reconsidered. The most sensitive areas of the business (i.e. accounts folder) have restricted permissions on folders. Thus, only members of a given privileged group are able to physically access. From our investigation, although the sponsor's office is entirely open-plan, the staff are not in the habit of locking their workstations when unattended. This is a serious problem as identified by the Jersey Data Protection Commisioner [54] that makes information available to unauthorised requesters. The latter concern falls beyond the scope of this research though.

One of the major findings of this case study is the inconsistency identified in the office handbook. For example, the data protection legislation cited in the office handbook is incorrect. That section should be updated to reflect that it is the Data Protection (Jersey) Law 2005, with which the sponsor's practices are compliant. The Data Protection (Jersey) Law 2005 repealed the Data Protection (Jersey) Law 1987 when it came into force[h]. Thus, the 1987 legislation needs to be cited only where it still has a direct bearing upon the data controller in question. In other words, where the data controller was registered under the 1987 law. A search of the on-line data protection register shows that the sponsor was not registered until 05 February 2007 [5]. That simply means it must comply with the Data Protection (Jersey) Law 2005, and not the Data Protection (Jersey) Law 1987 [82]. Another inconsistency exists in the policy of storing data on hard drives. Storing data on the local hard drives of the available machines running MailStore Home runs contrary to the practices outlined in the office handbook. The practice states," [i]ndividual C drives are not to be used for storing data" [79]. Either the handbook should be changed or, preferably, the server version of the product should be deployed. The latter suggestion enables the saving of MailStore archives to networked locations that would, in turn, increase the

[h] Article 71, Data Protection (Jersey) Law 2005

sponsor's backup resilience as the archives could be incorporated into the sponsor's nightly backup scripts.

The sponsor's policy of logging all inbound and outbound e-mail is considered a sensible matter of business continuity. This would, however, raises concerns whether there is a legal obligation for them to retain their e-mail correspondence for such a long period of time. This practice runs the risk of violating the fifth principle of the Data Protection (Jersey) Law 2005. If a generous ten-year retention period were enforced, which is in-line with that afforded to legal contracts as we outlined before, and would therefore presumably extend to instructions received by the sponsor from its client base then, starting in 2015, the 2004 e-mails can be dispensed with. This will help the sponsor keep their archive to a manageable threshold. This, in turn, would be regarded favourably by the Data Protection Commissioner, as it complies with the fifth principle of the Data Protection (Jersey) Law 2005. We do not perceive there being any digital privacy concerns in relation to the concept of e-mail logging and archiving, many businesses either needing to engage in such practices to comply with their legal obligations as outlined before. In addition, there is a need to insulate their respective businesses, in the event of a disaster recovery scenario [83].

The process of archiving telephone activity logs is another common practice in many businesses, and we do not perceive there being a digital privacy issue with this. As Milner [56] observes, the employee is using the employer's facilities for a combination of legitimate business, and personal use, and should therefore have an appreciation that the employer has the perceived right to monitor the use of its own equipment, for a variety of purposes. Given that actual telephone conversations are not logged; the sponsor's use of call logging is at an acceptable level for its business operations.

While the allocation of unrestricted Internet access represents an obvious security concern,

we appreciate the sponsor's willingness to trust its staff. Content filtering is perceived negatively amongst employees and, sometimes, affect the performance either psychologically or physically in case of poor Internet connection. That would, however, create a security concern since employees may potentially visit infected websites (i.e. viruses, malware, etc.). There is one section of the office handbook which relates to this process," ... use of the internet for personal matters must be restricted to the individual's own time, i.e. during their lunch break, or before or after their normal working hours." [79]. Given that section, the recommendation here is that a logging system be enabled. Thus appropriate actions can be taken in case of breaches. We perceive there being a potential digital privacy issue here, whereby if, for example, an employee was to use their dedicated terminal to browse the Internet during their" own time" with their" own devices" (e.g. during their lunch hour - and were to engage in a legitimate activity which the sponsor may not approve of during that time). A prime example would be sending their curriculum vitae to a rival employer with a request for consideration for a prospective job elsewhere, then the sponsor's options may be limited if they come to learn of this, by virtue of the sponsor having held-out that it is acceptable for the staff to use the Internet for their own purposes during their" own time". A simple caveat such as" ... but the firm retains the right to audit the use of any specific workstation at any time, for any reason" would likely suffice [56]. It is arguably excessive, and broad in its implications, but given the rather restrictive legal framework in place in the island at present, it would give the employer additional leverage should they feel the need to take action. Similarly, as most local workplace digital privacy concerns are addressed as matters of contract law at present, this would flow through into the existing framework for such disputes.

Data archiving and backup functionalities are of critical importance in the modern age, and it is important that these decisions are not solely made by IT personnel, but by the most senior management in an organisation as well [84]. A robust DR plan will include data archiving, as well as the storage of those data archives (i.e. typically in some type of off-site facility). It is our view that the sponsor is well within its rights to back-up the sum of the data on its network, for DR and business continuity purposes. While we have concerns over the security of the sponsor's off-site data archives, this falls beyond the scope of this research.

While we find the sponsor's IT department's notion of deploying multiple remote-access solutions to be reasonable, we would suggest that the more third party remote-access solutions deployed, the less secure the network becomes, particularly if the passwords used are simple to guess. There is an additional area of concern with the use of remote-access software from a digital privacy perspective, which is that the person using the remote-access software can see exactly what the target user is doing on their workstation and, While this monitoring is often overt (as is the case with TeamViewer, where a dialogue box pops-up on the remote terminal to indicate a remote session is underway), older software such as Famatech's Remote Administration v2.1 do not have any such obvious interaction with an end-user. In the case of Remote Administrator v2.1, for example, the only indication that a remote monitoring session is underway is by virtue of the system tray icon changing colour, and this would fall outside the notice of many end-users. There is, therefore, scope for the misuse of this type of technology in an office setting, such as where a department head may direct IT staff to monitor an employee's activities, and report back. While we are assured that the sponsor does not use this type of technology to that end, we are

nevertheless concerned that the potential exists for it to be misused, and would recommend that a suitable clause be included in the office handbook to explain the specific uses of this type of solution, to allay any concerns staff may have.

The issue of cover in the workplace is a problem for any employer, and there appears to be little guidance offered to Jersey businesses in relation to how best to establish cover in a given organisation. It is of concern to us that cover at the sponsor's workplace sees staff pairings having complete, unrestricted access to one another's exchange mailboxes, as it is not difficult to envisage one member of staff reading correspondence that is private to the other, and vice-versa. Milner [56] and Martins [57] are both quite vocal about the individual's grasp of the use of technology in the modern workplace, and how unprincipled many staff members are when it comes to their individual use of these communal forms of communication. For example, even knowing e-mail correspondence is logged automatically, staff members will often still send inappropriate content to friends at other firms. Milner observes that the forthcoming Freedom of Information legislation will mean States departments in particular will have to become considerably more diligent in their use of such facilities, lest apparent misuse thereof come to light rather publicly [56]. While we do not have an improved solution to present to the sponsor, we draw to their attention the potential significance of this unrestricted access over time.

We have touched upon the sponsor's policy of retaining data archives off-site above, and we find their existing building security provisions to be adequate. We have no digital privacy concerns about these measures, as they are in place to comply with legal and insurance requirements, as well as an understandable desire to keep the building secure, out of hours. We find the sponsor's level of Internet-based security to be lacking but, again, this falls outside the remit of this study, and is further mitigated by the presence of Sophos anti-virus on each workstation and server.

Table 3 summarises the concerns and potential legislation violations in the current practices of the sponsor's workplace.

Table 3: Work Practice Vs Legislation

Work Practice	Possible Legislation Violation	Action(s)
Data Access	Unauthorised access. The Jersey Data Protection Commisioner [54]	Outside the research scope
Data Protection Legislation	Office Handbook: The data protection legislation cited is incorrect (i.e. Data Protection (Jersey) Law 1987)	The Handbook has to be updated to reflect that it is the Data Protection (Jersey) Law 2005
Data Backup Policy	Office Handbook: Storing data on the local hard drives of the available machines running MailStore Home runs contrary to the practices outlined in the office handbook	Either the handbook should be changed or, preferably, the server version of the product should be deployed.
Email Logging Policy	Too long retention period violates the fifth principle of the Data Protection (Jersey) Law 2005.	A 6-10 years' retention period has to be specified [68]. This might involve a process of email classification.
Archiving Telephone Activities	No violations. The actual call conversations are not logged.	N/A
Internet Activity Logging	No violations based on the terms of use stated in the Handbook. "... use of the internet for personal matters must be restricted to the individual's own time, i.e. during their lunch break, or before or after their normal working hours." [79]	N/A
Remote Access	No violation	N/A
Offsite Data Archive	No violation	N/A

3.4 Recommendations

This research identified some areas of concern, which could be addressed, to ensure any potential misunderstandings are kept to an absolute minimum. The following addresses that in detail:

- Sponsor's Handbook
  There is a need for the handbook to be re-written to outline the following:
  - The legislation with which the sponsor is compliant should be identified as the Data Protection (Jersey) Law 2005, and not the Data Protection (Jersey) Law 1987
  - A global caveat should be introduced in the section referencing Internet access, along the lines of" the firm retains the right to audit the use of any specific workstation at any time, for any reason". This would increase the authority of the sponsor to police the use of its own equipment

    - The explicit use of remote-support solutions such as TeamViewer and Remote Administrator should be outlined, in order to avoid any misunderstanding as to the intended purpose of that software (i.e. it is for remote-support, not remote-surveillance)
- Workstations
  The sponsor should upgrade those workstations using MailStore as a product from MailStore Home to MailStore Server. MailStore Home archives can only be stored on local hard drives, and this violates the general provision of not storing data locally as stipulated in the sponsor's handbook. Furthermore, it is not possible at present to screen an employee's interaction with the hard drive of their own PC, as there is no restriction placed on the use of USB ports, or CD/DVD-ROM drives. Finally, being able to save archives onto the network with MailStore Server facilitates easier backup, DR, and business continuity
- Retention Period
  A firm retention period should be established for e-mail archiving. If ten years is the threshold, then the sponsor can begin, from 2015, to dispose of its oldest-archived e-mails.

There is an area of interest, which came to light during our interview with Advocate Milner, which is the increasing trend for staff members at many organisations to bring in their own devices (i.e. Bring Your Own Device (BYOD)), and attach them to the corporate network [56]. While heralded by some as the next major movement in the evolution of the modern workplace [85], BYOD raises a number of interesting predicaments from a digital privacy perspective, in the main because the ownership of the device being used is sometimes not clear-cut. In the instance, for example, of a device that is owned outright by an employee, but in respect of which the employer pays for all monthly costs, to what degree does the employer have the right, whether explicit or implied, to monitor the use of that device? Given the ubiquity of mobile technology in the modern age [86], it is not surprising that industry pioneers such as Microsoft, Apple and Google have extensive involvement in the BYOD arena. Microsoft, for example, offers a detailed set of guidelines as to how best to implement their product line in conjunction with BYOD initiatives in your own business [87]. Apple presents a number of business cases illustrating the suitability of its own product line for BYOD consideration [88]; and in May 2014 Google purchased Divide manufacturers of an Android app designed to create a secure working environment in BYOD scenarios [89, 90], which can be taken as a tentative endorsement of their interest in this area. The position at law in Jersey is unclear, yet this does not appear to affect the sponsor as the terms of their office handbook clearly state," I.T. equipment and related devices, or storage media containing data or software may not be introduced to or removed from the Company's premises without the specific authority of the Managing Director or her delegates as cited above." [79]. Authority to administer BYOD scenarios is therefore restricted to two individuals - the man- aging director and the IT department head. Should the sponsor consider implementing a more open BYOD policy in the future, we would suggest a review of the legal position in Jersey be undertaken at that time, and that due consideration of both the benefits and the drawbacks of BYOD as a business concept be considered [91].

It is at this point that it behoves us to return to our original hypothesis, being" formal recognition for digital privacy would prevent potential privacy breach in the Jersey workplace". As seen throughout the course of this paper, there is a distinct lack of recognition at law, in the island of Jersey, for the notion of digital privacy in the workplace. The Data Protection (Jersey) Law 2005 is not a privacy law, and has no provision which expressly caters to digital privacy. This silence is echoed in the Employment (Jersey) Law 2003 and, while we are given to understand that the concept of digital privacy is something which data protection commissioners are discussing across Europe [57], there is no overt indication that the forthcoming EU data protection regulation will have an express provision relating thereto when it comes into force.

We have seen how, even in a well-documented office environment, where all policies are compliant with the law as it presently stands, there are areas which can be tightened-up, to avoid potential conflict of interests between staff and employer, or scope for legal action by disgruntled staff in the event of a fundamental breakdown in communications. A simple example of this would be where IT staff were to use remote-support software to engage in remote surveillance of staff activities. While morally questionable, this is not an unlawful practice under Jersey law at present, and it is doubtful whether an employee would have any grounds at law for taking action were they to become aware of this actually taking place. It is, therefore, our recommendation that local government consider introducing legal provisions for the concept of digital privacy in the Jersey workplace.

4. Conclusion and Future Work

This research is conducted in the island of Jersey, examining Jersey-specific legislation; conducting interviews with a leading local employment lawyer, and our local data protection commissioner; researching

forthcoming changes owing to the new EU data protection regulation; and investigating the working practices and documentary support therefor, of a local employer who is the sponsor of this research [79]. As such, this research is of a direct applicability to employers, employees and local government within the island of Jersey itself.

The research touches upon the forthcoming EU data protection regulation, but focus thereon from a Jersey-centric perspective and are, as a result, of less benefit to those studying the aforementioned regulation from a European perspective. That being said, this research may still be of benefit to those who have an interest in jurisdictions in respect of which the EU has issued an adequacy decision.

The following summarises the research findings throughout this project:

- There is no legal provision for a right to digital privacy in the Jersey workplace at present, under any piece of prevalent legislation;
- Employers and IT practitioners who are compliant with the Employment (Jersey) Law 2003, and the Data Protection (Jersey) Law 2005 are therefore unlikely to need to make any drastic changes to their practices in the short term;
- Employers should ensure they refer to the correct piece of data protection legislation when citing their compliance. In the vast majority of cases, this is the Data Protection (Jersey) Law 2005, and not the Data Protection (Jersey) Law 1987, which has been repealed;
- Employers should ensure they retain a blanket provision in their support documentation, office handbooks and similar, to audit the use of any aspect of their IT infrastructure, for legitimate business purposes. This ensures they retain a strong degree of control over the use of their facilities, and can take appropriate action for implied breaches thereof, within reason;
- Where there is a perceived ambiguity relating to the purpose of specific software (e.g. remote-access software), the intended purpose of that software should be communicated to staff, for the sake of clarity;
- A firm data retention period should be established, to ensure compliance with the fifth principle of the data protection law ("[p]ersonal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes" [5];
- If employers encourage the BYOD model of computing, where staff are invited to bring their own devices into the corporate environment, appropriate security reviews and data protection initiatives should be undertaken, and there are various industry leader-promoted guides to help employers realise the potential trouble spots in these areas [87]. As with digital privacy in the Jersey workplace, there is no provision relating to BYOD technology in prevalent legislation within the island. That being said, the BYOD model falls more under the remit of data protection than the central concept of digital privacy, as the storage of sensitive personal data is one of the fundamental areas the Data Protection (Jersey) Law 2005 focuses upon;
- The topic of digital privacy in the workplace is something which is being discussed among data protection commissioners across Europe [57], and While there is no indication that an overt digital privacy provision will be introduced in Jersey with the coming into force of the new Pan-European Data Protection Regulation, that such a topic is being discussed is encouraging for the future;
- It is our considered view that digital privacy in the workplace exceeds the remit of traditional contract law, and needs its own unique set of provisions, to ensure it is given the consideration it deserves. While we acknowledge this is a very difficult area within which to legislate, we feel this study demonstrates that there is sufficient need for there to be greater clarity in this area of law and practice, than presently exists.

The future direction of this research will wait for confirmation of the full changes brought into force by the forthcoming EU data protection regulation with considerable interest and, thereafter, to seeing how Jersey's adequacy status will be reviewed in the wake of those changes coming into force in the EU. To be able to do that liaising with local government (i.e. JACS and the office of the data protection commissioner) is required. This is mainly to discuss the dissemination of our recommendations to employers and employees in the island of Jersey in light of this paper and to keep abreast of developments regarding the EU, as well as any future digital privacy discussions held between data protection commissioners across the EU and other adequacy-approved jurisdictions, to see what comes of those discussions.

References

[1] T. C. of Europe, Convention for the protection of human rights and fundamental freedoms as amended by protocols no. 11 and no. 4. Rome, Online (June 2010).

[2] E. Holmboe, E. Bernabeo, The 'special obligations' of the modern Hippocratic oath for 21st century medicine, Medical Education 48 (1) (2013) 87–94.

[3] Jersey, Public elections (jersey) law 2002: Elizabeth ii, Jersey: The Judicial Greffe (2002).
[4] Jersey, Company securities (insider dealing) (jersey) law, 1988: Elizabeth ii., Jersey: The Judicial Greffe (1988).
[5] D. P. Register, Data protection (jersey) law 2005 - register of data controllers, Online (2005). URL https://www.dataprotection.gov.je/cms/Notification/Controller.aspx?id=16382
[6] W. B. Group, Internet users (per 100 people), Online (2014).
[7] M. M. Skeels, J. Grudin, When social networks cross boundaries: A case study of workplace use of facebook and linkedin, in: Proceedings of the ACM 2009 International Conference on Supporting 860 Group Work, GROUP '09, ACM, New York, NY, USA, 2009, pp. 95–104.
[8] W. Netter, W. Koslow, Introduction: Privacy in the workplace, Online (2002). URL URL https://cyber.law.harvard.edu/privacy/Module3_Intronew.html
[9] R. van den Hoven van Genderen, Trading privacy for security, Amsterdam Law Forum 1 (4) (2009) 95–102.
[10] E. Chemerinsky, Post 9/11 civil rights: Are Americans sacrificing freedom for security, Denver University Law Review 81 (4) (2004) 759–773.
[11] E. Holbrook, Airport security: Privacy vs. safety, Risk Management 57 (2) (2010) 12–14.
[12] C. Fuchs, Privacy and security in Europe, in: S. . C. Centre for Science (Ed.), ACTs Work Package 7 Dissemination and Coordination, 2013.
[13] F. Belanger, R. E. Crossler, Privacy in the digital age: A review of information privacy research in information systems, Management Information Systems Quarterly 35 (2011) 1017–1041
[14] M. W. Allen, S. J. Coopman, J. L. Hart, K. L. Walker, Workplace surveillance and managing privacy boundaries, Management Communication Quarterly 2007 21 (2007) 172–200.
[15] C. Holton, Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem, Decision Support Systems 64 (4) (2009) 853–864.
[16] P. M. d. H. Federica Pazzaglia, Karan Sonpar, S. Flynn, The dangers of disgruntled ex-employees, Online (June 2013). URL http://sloanreview.mit.edu/article/the-dangers-of-disgruntled-ex-employees/
[17] M. Hampton, The offshore interface: Tax havens in the global economy', Online (1996). URL http://www.academia.edu/190557/The_Offshore_Interface.Tax_Havens_in_the_Global_Economy
[18] M. Mainelli, M. Yeandle, Gibraltar as an overall international finance centre, in: Gibraltar Global Investor's Guils 2012 Milestone GRP, 2012, pp. 36–39
[19] C. G. Foreword, The Global Financial Centres Index 14, Cole v Jersey Post [2003]. JLR 460 (September 2013).
[20] L. Friedman, B.A. & Reed, Workplace privacy: Employee relations and legal implications of monitoring employee e-mail use, Employee Responsibilities & Rights Journal 19 (2) (2007) 75–83.
[21] S. of Jersey, Jerseys relationship with the uk and eu., Online (2014). URL http://www.gov.je/Government/JerseyWorld/InternationalAffairs/Pages/RelationshipEUandUK.aspx
[22] T. B. Monarchy, Channel islands, Online (2014). URL http://www.royal.gov.uk/MonarchUK/QueenandCrowndependencies/ChannelIslands.aspx
[23] Ministry of justice, background briefing on the crown dependencies: Jersey, 910 guernsey and the isle of man, Online, http://www.justice.gov.uk/downloads/about/moj/our-responsibilities/Background_Briefing_on_the_Crown_Dependencies2.pdf (2014).
[24] G. Thorn, Documents concerning the accession to the European communities of the kingdom of Denmark, Ireland, the kingdom of Norway, and the united kingdom of great Britain and northern 915 Ireland, Official Journal of the European Communities 15 (L73) (1972) 164.
[25] E. Commission, Countries outside the eu (third countries), Online (2013). URL http://ec.europa.eu/justice/data-protection/bodies/authorities/third-countries/index_en.htm#h2-9
[26] P. Johnson, Jersey legal system & constitutional law, Online (2013). URL http://www.lawinstitute.ac.je/wp-content/uploads/2013/12/2013.08.15_JLS-Study-Guide-2013-FINAL.pdf
[27] C. Michel, Hamon, Ta picot (ci) ltd v Michel, Crill and Hamon (Crills), JLR N-3 (1995).
[28] M. Cavey, Fair play in the workplace, The Jersey Law Review 3 (2). URL https://www.jerseylaw.je/Publications/jerseylawreview/June99/fairplay_in_the_work_place.aspx
[29] Jersey, Health and safety at work (jersey) law 1989: Elizabeth ii, Jersey: The Judicial Greffe (1989).
[30] Jersey, Industrial disputes (jersey) law 1956: Elizabeth ii, Jersey: The Judicial Greffe (1956).
[31] Jersey, Payment of wages (jersey) law 1962: Elizabeth ii, Jersey: The Judicial Greffe (1962).
[32] Jersey, Termination of employment - minimum periods of notice (jersey) 935 law 1974: Elizabeth ii, Jersey: The Judicial Greffe (1974).
[33] Jersey, Terms of employment (jersey) regulation 1998: Elizabeth ii, Jersey: The Judicial Greffe (1998).
[34] S. Assembly, Draft employment (jersey) law 200-, Online (October 2002). URL http://www.statesassembly.gov.je/AssemblyPropositions/2002/28672-7426.pdf
[35] Jersey, Employment (jersey) law 2003: Elizabeth ii, Jersey: The Judicial Greffe (2003).
[36] JACS, Employment (jersey) law 2003., Online (July 2005). URL http://www.jacs.org.je/legislation/employment-%28jersey%29-law-2003/
[37] J. E. Tribunal, Jersey employment tribunal, Online (2012). URL http://www.jerseyemploymenttribunal.org/
[38] W. Malorey, Some employee protection at last, . The Jersey Law Review 8 (1).
[39] S. of Jersey, Petty debts court, Online (2014). URL http://www.gov.je/CrimeJustice/Court/Pages/PettyDebtsCourt.aspx
[40] R. C. of Jersey, Magistrates court and youth court, Online (2014). URL http://www.jerseycourts.je/about/magistrates-court-and-youth-court/

[41] J. L. I. Board, Search judgments, Online (2014). URL http://www.jerseylaw.je/Search/default.aspx?target=jet#&&Tab=2&WasTextSearch=True&Facets=JETJudgement&Page=1
[42] S. of Jersey Statistics Unit, Jersey in figures 2013, Online (2013).URL http://www.gov.je/SiteCollectionDocuments/Government%20and%20administration/R%20Jersey%20In%20Figures%202013%2020140429%20SU.pdf
[43] JACS, Jersey advisory and conciliation service, Online (2014). URL http://www.jacs.org.je/
[44] E. Forum, Recommendation codes of practice, 965 Online (July 2013). URL http://www.gov.je/SiteCollectionDocuments/Working%20in%20Jersey/ID%20Codes%20of%20Practice%20Recommendation%20July%202013%2020130726%20JJ.pdf
[45] L. B. of Cornhill, Incorporation of the European convention on human 970 rights: legislation.gov.uk, Human rights act 1998, Online (1998). URL http://www.legislation.gov.uk/ukpga/1998/42
[46] Jersey, Human rights (jersey) law 2000: Elizabeth ii, Jersey: The Judicial Greffe (2000).
[47] JACS, Information for employment legislation, Online (2014). URL http://www.jacs.org.je/legislation/
[48] Jersey, Rehabilitation of offenders (jersey) law 2001: Elizabeth ii, Jersey: The Judicial Greffe (2001).
[49] Jersey, Control of housing and work (jersey) law 2012: Elizabeth ii, Jersey: The Judicial Greffe (2012).
[50] M. I. Wilson, K. E. Corey, Approaching ubiquity: Global trends and issues in ict access and use, Journal of Urban Technology 18 (7).
[51] J. Koenigstorfer, A. Groeppel-Klein, Consumer acceptance of the mobile internet, Marketing Letters 23 (4) (2012) 917–928.
[52] D. Dillon, A world infinite and accessible: Digital ubiquity, the adaptable library and the end of information, Journal of Library Administration 48 (1) (2008) 69–83.
[53] D. P. Commissioner, The office of the data protection commissioner, online (2014). URL http://www.dataprotection.gov.je/cms/default.htm
[54] P. Rowan, Re: Digital privacy in the jersey workplace, [E-Mail]. Message to: D. Booth (February 2014).
[55] V. Milner, Interview with d. booth, Interview. Digital recording in possession of author (February 2014).
[56] E. Martins, Interview with d. booth, Interview. [Digital recording in possession of author] (March 2014).
[57] Jersey, Freedom of information (jersey) law 2011: 995 Elizabeth ii, Jersey: The Judicial Greffe (2011).
[58] G. Voss, Looking at European Union data protection law reform through 1000 a different prism: The proposed EU general data protection regulation two years later, Journal of Internet Law 17 (9) (2014) 12–24.
[59] E. D. P. Supervisor, Data protection glossary, Online (2014). URL https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/71
[60] P. Ward, Microsoft sharepoint 2013 disaster recovery guide, eBook (September 2013). URL https://www.packtpub.com/application-development/microsoft-sharepoint-2013-disaster-recovery-guide.
[61] V. Cerullo, M. J. Cerullo, Business continuity planning: A comprehensive 1010 approach, Information Systems Management. June 2004 21 (3) (2004) 70–78.
[62] Jersey, Data protection (jersey) law 2005: Elizabeth ii, Jersey: The Judicial Greffe (2005).
[63] Calligo, The offshore cloud, online (July 2014). URL http://www.calligo.net/.
[64] J. C. FrancisIV, In the matter of a warrant to search a certain e-mail account controlled and maintained by microsoft corporation, Online, http://pdfserver.amlaw.com/nlj/microsoft-warrant-sdny.pdf (April 2014).
[65] B. Borden, A. L. D.Borden, A. L. D'Ambra, E. J. Beale, United states: SDNY significantly broadens reach of warrants under the stored communications act: Forces Microsoft to produce customer email on an extraterritorial server, Online, http://www.mondaq.com/unitedstates/x/312250/ (May 2014).
[66] Jersey, Money laundering (jersey) order 2008: Elizabeth ii, Jersey: The 1015 Judicial Greffe (2008).
[67] J. F. S. Commission, Codes of practice for deposit-taking business, online (2008). URL https://www.jerseyfsc.org/pdf/codes_of_practice_for%20deposit-taking_business_february_2008.pdf.
[68] H. R. . Customs, Keeping records for business- what you need to know, Online (2013). URL http://www.hmrc.gov.uk/factsheet/record-keeping.pdf
[69] T. L. Society, File retention: wills and probate, Online (October 2011). URL https://www.lawsociety.org.uk/advice/practice-notes/fileretention-wills-probate/#ftw4_1
[70] T. L. Society, File retention: trusts, Online (October 2011). URL https://www.lawsociety.org.uk/support-services/advice/practice-notes/file-retention-trusts/#ftt5
[71] W. v Lazard Brothers & Co (Jersey) Ltd, West v Lazard brothers & co (jersey) ltd, unreported (October 1993).
[72] R. v Perrier, Racz v perrier jj 151 at 152 (1979).
[73] S. Merabet, The sword and shield of social networking: Harming employers goodwill through concerted Facebook activity, Suffolk University Law Review 46 (4) (2013) 1161–1186.
[74] B. Clover, Work to rule action will mean nurses 1045 withdraw their goodwill, Nursing Times 106 (29) (2010) 3.
[75] L. Gordon, Lose our goodwill and the health service is finished, Nursing Standard 25 (19) (2011) 32.
[76] Bromley, D. B. (1986). The case-study method in psychology and related disciplines. John Wiley & Sons, p. 23
[77] Myers, M. D. et al. (1997). Qualitative research in information systems. Management Information Systems Quarterly, 21:241–242
[78] Jersey:Lysaght&Co. (2014). Sponsorship of the dissertation - David Booth
[79] Microsoft, Microsoft exchange mailbox merge program (exmerge.exe) information, Online (2014). URL http://support.microsoft.com/kb/174197

[80] Microsoft, Microsoft technet: Xcopy, Online (April 2012). URL http://technet.microsoft.com/en-us/library/cc771254.aspx
[81] Jersey, Data protection (jersey) law 1987: Elizabeth ii, Jersey: The Judicial Greffe (1987).
[82] I. Professional, Law drives demand for email archiving, Information Professional, 2 (1), p. 8 (Feb/Mar 2005).
[83] D. C. C. Steve Hawkins, David C. Yen, Disaster recovery planning: a 1060 strategy for data security, Information Management & Computer Security 8 (5) (2000) 222 – 230.
[84] V. NG, Byod – the inevitable fact of enterprise mobility today, Network-World Asia 10 (3) (2013) 2.
[85] S. Okazaki, F. Mendez, Perceived ubiquity in mobile services, Journal of interactive marketing 27 (2) (2013) Journal of interactive marketing.M. Technet, Bring your own device (BYOD) survival guide for Microsoft technologies, Online, http://social.technet.microsoft.com/wiki/contents/articles/20554.bring-your-own-device-byod-survivalguide-for-microsoft-technologies.aspx (October 2013).
[86] Apple, Bring your own 1070 device, Online (July 2014). URL https://www.apple.com/ipad/business/it/byod.html
[87] Enterproid, Divide is joining google, Online (2014). URL http://www.divide.com/
[88] Reuters, Profile: Google inc (googl.o), Online (2014). URL http://www.reuters.com/finance/stocks/companyProfile?symbol=GOOGL.O
[89] C. Caldwell, S. Zeltmann, K. Griffin, Byod (bring your own device), Competition Forum 2012 10 (2) (2012) 117–121.

Ali ahmed received the B.S. and M.S. degrees in Computer Science from Faculty of Computers and information in 2000 and 2004, respectively. During 2006-2010, he stayed in the Information and Management Group (IMG) at the University of Manchester, UK studying Computer security. He now an assistant professor at Cairo University and an Honorary Lecturer at the University of Liverpool, UK.