Investigating the Tension Between Cloud-Related Actors and Individual Privacy Rights

Bob Duncan
Business School,
Aberdeen University, Scotland
robert.duncan@abdn.ac.uk

Karen Renaud
Division of Cyber Security,
Abertay University, Scotland
k.renaud@abertay.ac.uk

Beverley Mackenzie
Division of Cyber Security
Abertay University, Scotland
1705191@abertay.ac.uk

***Abstract*—Historically, little more than lip service has been paid to the rights of individuals to act to preserve their own privacy. Personal information is frequently exploited for commercial gain, often without the person's knowledge or permission. New legislation, such as the EU General Data Protection Regulation Act, has acknowledged the need for legislative protection. This Act places the onus on service providers to preserve the confidentiality of their users' and customers' personal information, on pain of punitive fines for lapses. It accords special privileges to users, such as the right to be forgotten. This regulation has global jurisdiction covering the rights of any EU resident, worldwide. Assuring this legislated privacy protection presents a serious challenge, which is exacerbated in the cloud environment. A considerable number of actors are stakeholders in cloud ecosystems. Each has their own agenda and these are not necessarily well aligned. Cloud service providers, especially those offering social media services, are interested in growing their businesses and maximising revenue. There is a strong incentive for them to capitalise on their users' personal information and usage information. Privacy is often the first victim. Here, we examine the tensions between the various cloud actors and propose a framework that could be used to ensure that privacy is preserved and respected in cloud systems.**

***Index Terms*—Cloud, Cloud actors, Privacy, Confidentiality**

I. Introduction

In the decade since the introduction of the cloud computing paradigm, we have seen a significant shift in cloud capabilities. In 2011, NIST [1, p.2] provided an updated definition of what cloud computing is, explaining that the essential characteristics of the cloud are (1) on-demand self service, (2) broad network access, (3) resource pooling, (4) rapid elasticity, and (5) measured service

Since this definition was formulated, the capabilities of cloud, and the uses to which it can be put, have evolved considerably. It is perhaps inevitable that hackers have turned their attention to cloud as well, with some success as recent attacks demonstrate [2]. Successful hacks leak data, and privacy violations become a huge concern. We have to take a close look at the parameters of this problem, to consider how to formalise better mechanisms for preserving the privacy of everyone using the cloud.

Of interest, here, is the number of different actors involved in the cloud ecosystem. This has rendered the environment far more complex than traditional distributed network systems. The number of actors has increased considerably, to include both programmatic and human actors. The number of bad actors carrying out attacks has increased exponentially [3], [4], [5], [6], [7]. We can see that the time between breach and discovery has been steadily falling between 2012 and 2016. This can be attributed in some way to the impact of efforts of companies to improve security in light of the need to comply with the General Data Protection Regulation (GDPR). This momentum was rather lost when some serious lobbying resulted in a change from the requirement to report a breach within 72 hours of occurrence to *within 72 hours of discovery*, as evidenced by the 2017 breach report [8], where the time between breach and discovery returned to near 2012 levels in the space of a year. Of significance throughout this period is the alarming increase in attack volume throughout, yearly.

While cloud users have been quick to exploit the opportunities offered by cloud, so too have bad actors been keen to exploit its inherent vulnerabilities. Hackers are now specifically targetting the cloud [9] so all stakeholders really cannot afford to neglect cloud security. This is not a simple task, as [10] points out. He refers to the "The Inevitability of Combinatorial Risk" due to technical interdependencies and the multiple actors involved in the system.

In addition, we have seen a significant change in the way governments approach security and privacy concerns. Of particular interest is the new EU GDPR [11], which brings to bear very significant penalties for non-compliance in the event of a security breach. Furthermore, jurisdiction is now global, instead of EU-wide only. This is likely to encourage other jurisdictions to strengthen their own security and privacy legislation, which, to date, have been rather poorly framed.

In Section II, we present the core principles of privacy. In Section III, we consider the range of vulnerabilities in cloud ecosystems that must be addressed in order to ensure a high level of security and privacy can be achieved. Then, in Section IV, we look at how the actors involved in cloud ecosystems have evolved during the past decade. In Section V, we develop a framework to address how to defend against such vulnerabilities. In Section VI, we consider the anticipated manner in which the framework might be deployed, and in Section VII, we discuss our conclusions.

 ISBN: 978-1-61208-703-0

II. Privacy and the Cloud

Privacy researchers have expressed concerns about computer users divulging too much information [12], not appreciating or valuing their personal information and giving it away unthinkingly, unwittingly sacrificing their privacy [13]. As governments move to put all their citizens' details online [14], utilizing cloud services to do so, the potential for privacy invasion increases the consequences disastrous [15].

Privacy is undoubtedly a complicated concept [16]. Solove explains that privacy is "*an umbrella term, referring to a wide and disparate group of related things*" [17, p.485]. Privacy, according to Privacy International, who are more specific, is a multidimensional concept, which is related to four components: (1) body, (2) communications, (3) territory, and (4) information. When it comes to the cloud, our interest is in the second and fourth of these.

Privacy is a human right in Europe, and the United Kingdom is a signatory of the European Convention of Human Rights. Article 8 of the Convention [18] states that EU citizens have the right to respect for private and family life. In particular, the State may only interfere with this right proportionally, in accordance with law and in the interests of national security, public safety, and for the prevention of crime. Yet the public at large seems to accept widespread privacy violations, seemingly without protesting [19], [20], [21].

Yet the UK government itself does not seem to respect their citizens' privacy rights. The UK government recently passed the Investigatory Powers Act (IPA). Part 4 of the Act requires web and phone companies to retain all data logs pertaining to their customers' activities for two years. They are required, upon request, to provide these to official bodies without judicial oversight, not respecting privacy.

Privacy and confidentiality are aligned yet conceptually different terms, which are often conflated. For example, Meriam Webster defines privacy as "freedom from unauthorized intrusion", "seclusion" and "secrecy". Confidentiality is defined as "private, secret". Yet these concepts are very different. The ISO/IEC 29100 [22] provides a more specific definition of the privacy principle: "*specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose*". The ISO/IEC 27001 [23] definition of confidentiality is: "*that information is not made available or disclosed to unauthorized individuals, entities, or processes*". This distinction is important when we start considering privacy and the cloud.

The introduction of the GDPR is said to be *"the most important change in data privacy regulation in 20 years"* [11]. The legislation came into force on the 25th May 2018, and replaced the existing Data Protection Directive 95/46/EC. Organisations that fail to comply will be subject to significant fines. GDPR is essentially linked to confidentiality; the requirement for cloud service providers is to ensure that personal data provided, or stored, by their users is secured and not leaked.

This means that cloud providers have to start taking confidentiality seriously, but little advice is offered to cloud providers in this respect. The Information Commissioner's website offers advice to the man and woman in the street, but not to cloud service providers [24]. In this paper, we propose a framework that will fill this gap.

III. Range of Vulnerabilities in Cloud Ecosystems

Due to the nature of the cloud ecosystem, and the various actors involved in the provision of cloud services, cloud users are at risk from cloud-specific threats and vulnerabilities. A cloud-based attack can have huge economic ramifications, comparable to that of a major natural disaster [25]. The range of vulnerabilities can be demonstrated by looking at the OWASP Top 10 risk tables for 2017. The first one addresses Web based weaknesses:

- A1:2017 — Injection
- A2:2017 — Broken Authentication
- A3:2017 — Sensitive Data Exposure
- A4:2017 — XML External Entities (XXE)
- A5:2017 — Broken Access Control
- A6:2017 — Security Misconfiguration
- A7:2017 — Cross-Site Scripting (XSS)
- A8:2017 — Insecure Deserialization
- A9:2017 — Using Components with Known Vulnerabilities
- A10:2017 — Insufficient Logging & Monitoring

The next Top 10 list considers Cloud specific risks:

- Accountability & Data Risk;
- User Identity Federation;
- Legal & Regulatory Compliance;
- Business Continuity & Resiliency;
- User Privacy & Secondary Usage of Data;
- Service & Data Integration;
- Multi-tenancy & Physical Security;
- Incidence Analysis & Forensics;
- Infrastructure Security;
- Non-production Environment Exposure.

We should also consider potential IoT weaknesses, since many cloud systems have enabled IoT use, and therefore are exposed to IoT vulnerabilities:

- Insecure Web Interface;
- Insufficient Authentication/Authorization;
- Insecure Network Services;
- Lack of Transport Encryption;
- Privacy Concerns;
- Insecure Cloud Interface;
- Insecure Mobile Interface;
- Insufficient Security Configurability;
- Insecure Software Firmware;
- Poor Physical Security.

Since mobile communication also forms an intrinsic part of the Cloud and IoT — we should also take account of the potential impact of Mobile vulnerabilities. To this end, we consider the OWASP top 10 of Mobile Vulnerabilities:

- M1 — Improper Platform Usage;
- M2 — Insecure Data Storage;

 ISBN: 978-1-61208-703-0

- M3 — Insecure Communication;
- M4 — Insecure Authentication;
- M5 — Insufficient Cryptography;
- M6 — Insecure Authorisation;
- M7 — Client Code Quality;
- M8 — Code Tampering;
- M9 — Reverse Engineering;
- M10 — Extraneous Functionality.

In the UK, the Information Commission Office (ICO) is the body that is responsible for the provision of individual rights with respect to data privacy. But, over the last decade cloud computing has been afforded little attention from this body. Yet, in 2015, the ICO's 'Annual Track Report' reported that it was established that out of a survey sample of 2,465 respondents, 60% stated that they had some apprehension with respect to cloud computing [26]. Such apprehension is well grounded, as demonstrated by some recent attacks [2]. Insurance companies like Lloyds are warning of the possibility of huge losses related to cloud attacks [27].

Cloud security issues were also identified by the Cloud Security Alliance (CSA), in their list of the cloud computing notorious nine security risks [28] with the cloud ecosystem being considered susceptible to: data loss, data breach, account hijacking, insecure API's, denial of service, malicious insider, insufficient due diligence, cloud abuse and share technology.

There is also a very important point to take into account here. We have looked at a range of "top 10" vulnerabilities. It is vitally important to realise that there are far more than the ten vulnerabilities in each of these areas. For example, in the case of IoT vulnerabilities, OWASP has identified a total of 94 IoT vulnerabilites that remain to be resolved. Thus, in every single case, it will be vital to not just consider the top 10 vulnerabilities, but to address all potential vulnerabilities to which the company will be exposed.

Due to the nature of cloud, mitigation of these risk is often outside the control of a cloud user. Hence, on occasions when security breaches and security failures do occur, it may be impossible for a client to identify the responsible actor, which, in turn, could lead to tension between actors.

There is a particular issue that must be taken into account with cloud systems, and that is the so called Cloud Forensic Problem [29], [30]. This arises when an attacker gains even a small foothold in a cloud system. Once there, the attacker seeks to escalate privileges to gain access to the forensic logs, which allows them to modify or delete all traces of their incursion into the cloud system. This allows the attacker to become a more permanent intruder, resulting in their capability to access considerably more information over the longer term, while remaining hidden. There is nothing within a cloud system to prevent this from occurring.

We need also to consider the damage insiders can cause from within the company, due to poorly updated processes, poorly configured IT resources and vulnerabilities [31].

Other issues are poorly defined policies, lack of attention to server logs and other aspects that are relatively easy things to police if only the cloud provider takes the time to do so. Finally, there are the malware attacks, such as the Mirai virus attack on cheap Internet of Things (IoT) devices [32]. It subsequently spread to corporate Windows desktops [33], thus facilitating the leveraging of compromised IoT networks into other more valuable corporate systems.

IV. Actors Involved in Cloud Ecosystems

Once cloud started to gain traction just over a decade ago, it offered some interesting opportunities to companies in terms of the ease with which they could provision IT resources. Many assumed it was just the cloud user and the cloud service provider who were the solo actors in the equation, but there were far more than that even 10 years ago. Cloud Service Providers (CSPs) made much of how committed they were to vetting all their staff members properly. However, little was said about the need to hire in temporary staff on an emergency basis, where often such agency companies were much less rigorous in their vetting processes [34].

Similarly, many of the services offered were not actually provided by the CSPs themselves. Often third party providers were used who had much less rigorous approaches to issues of security, privacy and confidentiality. CSPs were often less than transparent about where the data in their cloud offerings would reside, and even less transparent about who access it.

This would give rise to significant issues for European companies who were using cloud, since EU legislative and regulatory recommendations were to only use cloud provided by companies resident within the EU. The European base for Amazon Web Services (AWS) is in Ireland, a European company, so it might be assumed that anyone using such a service would be compliant. However, that would not necessarily be the case, as AWS also have data centres on the East and West coasts of the USA as well as data centres in the Far East[35].

In the interests of availability, AWS frequently would place copies of both software systems and data in other data centres in the interests of resilience, to ensure that recovery from any possible breakdown of services, or a major cyber breach, would be instantaneous. No mention of the possibilities that security standards in each physical location would be of the same high standard. An unwelcome byproduct of this arrangement would be a possible unexpected and unwelcome exposure to foreign legal jurisdiction, even where the company does not trade in that jurisdiction. In US legislation, for example, running software on a US based system automatically extends their jurisdiction over that company and exposes them to the full penalties of the law.

Contractors, consultants and many other parties will also be involved in a cloud ecosystem. Likewise, within a cloud user company, there will also be the need for temporary staff, contractors and consultants, many of whom will, of necessity, have direct access to cloud systems. This introduces a significant degree of complexity to the management of such systems and opens up a huge range of potential exposure and vulnerability to attack.

However, the problem does not end there. Cloud was instrumental in energising the take up of Big Data, and both

 ISBN: 978-1-61208-703-0

have been great enablers for the Internet of Things (IoT). This means that there are now a considerable range of software actors to add to the mix. IoT systems require access to cloud systems where data is stored, processed, analysed and so on. In addition, many of these systems are highly insecure and vulnerable to a range of attacks.

IoT services such as: Domestic and Home Automation, eHealth, Industrial Control, Logistics, Retail, Security and Emergencies, Self Driving Cars and Trucks, Smart Agriculture, Smart Animal Farming, Smart Cities, Smart Environment, Smart Water, Smart Metering, Smart Transport and Smart Utilities have all placed additional stresses on cloud computing. As dumb (and sometimes not so dumb) actors, these can also open up more and more vulnerabilities [36].

This also means that the complexity of handling cloud systems has increased exponentially in the decade since the cloud paradigm really started to gain serious traction. That increase in complexity presents a considerable increase in the risks associated with trying to ensure that a proper and secure environment can be developed to safeguard the security and privacy of customers and enable companies to be compliant with legislation and regulation.

V. Developing a Cloud Security and Privacy Framework

In developing a framework suitable for ensuring that an adequate level of security can be achieved by a cloud-using organisation, we need to consider three separate layers.

The **first layer** we must consider is our security and privacy goals, which will comprise the traditional triad of Confidentiality, Integrity and Availability, along with any new goals we would care to add, such as Audit and Forensic Trails.

The **second layer** we must consider is the systems architecture of the company, which comprises any traditional systems, services and applications, plus cloud services, such as IaaS, PaaS and SaaS.

The **third layer** is the Business Architecture of a company, which comprises a combination of (a) People, (b) Process and (c) Technology [37].

We illustrate this in Figure 1, where each of the layers is described as an axis point on the model. Where any point of confluence between the three axes occurs, we can very clearly articulate what we seek to address for our security and privacy concerns. Thus, at any particular intersection we can identify what the specific goal will be.

This first stage of developing the framework will allow us to set the declared policies the business will seek to achieve by addressing each of the confluence points.

However, this represents the goals at a high level of abstraction. We can subdivide each of the axes into smaller components. Thus, for example, Z1 could be broken down to identify each individual in the company using their ID code. Y6 can be broken down into each specific application in use. X4 can be broken down into the Audit trail requirement for each application, and so on. By this means, we can increase the granularity of addressed details, retaining essential details.

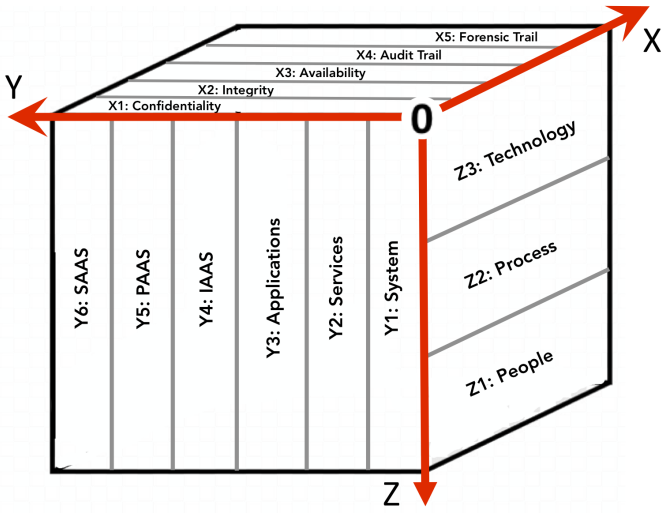

Figure. 1. A Cloud Three-Dimensional Policy Framework Matrix. (X=Security Properties; Y=System Architecture; Z=Business Architecture; 0=Origin)

The next stage will be to consider all known vulnerabilities against each area on the matrix. Thus social engineering attacks would principally relate to Z1, database injection attacks would relate to all instances which use databases on the Y axis, and so on. For each of these attacks, we can collect signatures to identify how each attack can be perpetrated, and can utilise these later for attack detection purposes.

We could also consider adding a risk layer to quantify our perception of risk attaching to each coordinate in the matrix, thus allowing us to evaluate the potential adverse impact of any consequential breach.

For the high-level matrix, we can also borrow from economic utility theory, for example [38], [39], which would allow us to incorporate a simple utility model into these relationships to provide a weighting to express the preferences of the business. This will allow us to develop a simple means of tailoring the model to suit any business.

Thus, to represent the policy of the business at an initial high level of abstraction, there would be three main aims for each of the relationships defined in the model: 1) to provide a mechanism for measurement; 2) to define a target position; 3) to define a utility preference over the target.

To illustrate this point: if we consider coordinate (X3, Y3, Z2): representing “availability for applications to run processes”.

For each such component of the policy framework model, as specified in Figure 1, that is of interest — let’s assume we index these components by a variable i — we associate a component U_i of a utility function, as follows:

- Measure: M_i; for example, % uptime of systems hardware; in this case, expressed as an average over time;
- Target: m_i, the declarative target for this operation;
- A function f_i expressing how utility depends on deviation from target. For example, a Linex function [40], usually

expressed in the form $g(z) = (exp(\alpha z) - \alpha z - 1)/\alpha^2$, is used to capture a degree of asymmetry that is parameterized by α;
- The weight w_i (between 0 and 1, and $\sum_i w_i = 1$) expressing the managers' weighting/preference for the ith security component of interest;
- This can be expressed thus: $U_i = w_i f_i(M_i - m_i)$;
- System equation $M_i = s_i(x_i)$, where x_i is a vector of control variables and s_i describes M_i's dependency upon them.

Thus the overall utility function is

$$U = \sum_i U_i = \sum_i w_i f_i(M_i - m_i).$$

We can obtain a treatment of the expected utility of the system by introducing suitable stochastic processes into the system functions s_i. In general, such treatment of a system's properties will be too complex to have analytic solutions for the control variables, thus simulations must be used. By evaluating each co-ordinate in the policy framework layer, the business can define their position on the security risks they face and the resulting utility model of the whole will reflect the level of utility they seek, while ensuring compliance with any legislation, regulation and standards. It will also be possible to place constraints on the targets. For example, in the above example, the target may be 99.99%, but the constraint may be that availability should never fall below 98%. In analysing all the co-ordinates of this model, it may be that some threats are subsidiary to others, and that by securing the main threat, this eliminates the subsidiary threats, although this may not always be the case. Each business can take a view on whether they cover these threats individually, or as related groups, depending on what would be appropriate to suit particular needs.

VI. Anticipated Usage of the Cloud Security and Privacy Framework

Now that we have developed a framework to address our needs, we need to understand how we might anticipate its usage in practice. The framework allows us to define what our cloud security and privacy goals are, and to identify how important they are to the company. As it is the company that is responsible for ensuring the security and privacy of PII, on pain of potentially significant fines, the company is therefore accountable for its actions.

Having identified what the security and privacy goals are, we have a good starting point to begin using the framework. In order to understand and measure the degree to which a company using this framework would be compliant, we need to examine our systems to see what has actually transpired during the period under examination. We can examine audit trails, forensic trails, system logs and carry out whatever other analytics are necessary to identify what exactly has been happening during the period under scrutiny. By compiling the metrics we seek to use to reflect real events, we can now compare those against the targets we have set for compliance. Again, to use an example from the previous section, in looking at that example, if our target is 99.99% and the constraint is a minimum of 98%, then if our actual figure shows 95%, then we will have failed our minimum compliance test. With a result of 98.5%, we would have passed our minimum compliance target of 98%, but failed our ultimate goal of 99.99%.

In the event that we fail on any part of the framework, we can then investigate to understand whether the failure arises due to an as yet unidentified attack, or from some other performance failure. In this way, we can identify where our weaknesses lie and take corrective action to ensure these failures do not arise again. If, on the other hand, we discover that an attack has occurred, then we will be in a good position to effect immediate action. Given the average time between breach and discovery of 200 days [41], we will find ourselves in a much stronger position than we otherwise might.

This will give us the comfort that we can identify poor performance and can quantify what that might be, also that we might identify any attack that has been perpetrated, and pick up the fact considerably in advance of the time in which we might otherwise be able to detect it.

For those users who do not have a high level of understanding of cyber security issues, there is an alternative, simpler approach to take. The user can make a list of all the known vulnerabilities already listed by the CSA and OWASP, to which they can add vulnerability lists from any other sources. Each vulnerability can be classified according to the framework matrix. As new vulnerabilities are discovered, these can be added, thus building up a more complete framework over time. Once they have specified their performance targets, they can no run their systems through the various open source tools to see which vulnerabilities are present in their systems, which they can then address. By regularly measuring performance using the framework matrix, they will be able to ensure they are addressing all the most important vulnerabilities.

However, these are not the only ways we can use the framework. Should we decide to implement an intrusion detection system, we will have identified the main known vulnerabilities to which our systems architecture are vulnerable, and can implement the necessary patterns into the intrusion detection software, meaning that we will be better placed to discover the occurrence of such attacks. While that will still leave us exposed to new attacks, which would be the case regardless of whether we operated the framework or not, there is a possibility that something uncharacteristic will show up somewhere in the system as a consequence of the intrusion.

VII. Conclusion

Thus we can see that using this framework, it will be possible to improve our security and privacy posture in the business. We will be able to detect where poor performance impacts on security and privacy compliance, but more importantly, where a breach does occur, we will have an advanced warning of that fact and will be able to do something constructive about it long in advance of what might be possible otherwise.

 ISBN: 978-1-61208-703-0

It is certainly the case that the sooner we are in a position to discover the incidence of an attack having arisen, the sooner we can take defensive and corrective action. If we have take a sensible approach to holding data in encrypted form, then we are likely to be significantly mitigate the impact of any potential breach. There is no doubt that breaches will arise, but the more we can do to mitigate the impact, the better it will be for all concerned, and in particular the users who have no real control over what might happen to their PII.

Given the misalignment of the agendas of all the actors in cloud ecosystems, it is likely that the use of our proposed framework will provide a much more secure environment for retaining users' PII, and thus reducing the impact of any breach we sustain to a considerable extent.

REFERENCES

[1] P. Mell, T. Grance, and Others, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Tech. Rep., 2011.

[2] N. Goud, "Cyber attack on cloud computing company makes france news websites go dark," 2017, https://www.cybersecurity-insiders.com/cyber-attack-on-cloud-computing-company-makes-france-news-websites-go-dark/.

[3] Verizon, "2012 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others," Tech. Rep., 2012, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.

[4] Verizon, "2013 Data Breach Investigation Report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and Others accessed 28/03/19," Tech. Rep., 2013, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf.

[5] Verizon, "2014 Data Breach Investigations Report," Tech. Rep. 1, 2014. [Online]. Available: \url{http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf}Accessed28/03/19

[6] Verizon, "2015 Data Breach Investigation Report," Tech. Rep., 2015, https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf Accessed 28/03/19.

[7] Verizon, "2016 Verizon Data Breach Report," Tech. Rep., 2016, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf Accessed 28/03/19.

[8] Verizon, "Verizon Security Breach Report 2017," Tech. Rep., 2017, https://www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/ Accessed 28/03/19.

[9] D. Pudles, "Hackers target cloud services," 2018, https://www.forbes.com/sites/steveandriole/2018/09/10/cyber-apocalypse-now-how-bad-what-to-do/\#687b4a611638, Accessed 14/4/2019.

[10] S. Andriole, "Cyber apocalypse now - how bad? what to do," 2018, https://www.forbes.com/sites/steveandriole/2018/09/10/cyber-apocalypse-now-how-bad-what-to-do/ Sept 10.

[11] EU Parliament, "Home Page of EU GDPR," 2018, https://www.eugdpr.org/(Accessed 14/4/2018).

[12] S. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11, no. 9, 2006.

[13] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[14] T. Marceddo, "The battle of the cloud: The digital front," 2018, https://www.cso.com.au/article/646311/battle-cloud-digital-front/06 September, Accessed 14/4/2019.

[15] N. Ntuli, "No help for victim of identity theft," 2018, https://www.news24.com/SouthAfrica/News/no-help-for-victim-of-identity-theft-20180117 Accessed 10/4/2019.

[16] S. T. Margulis, "Conceptions of privacy: Current status and next steps," *Journal of Social Issues*, vol. 33, no. 3, pp. 5–21, 1977.

[17] D. J. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review*, vol. 154, p. 477, 2005.

[18] European Convention, "Article 8 of the European Convention on Human Rights," 2012, http://www.equalityhumanrights.com/sites/default/files/documents/humanrights/hrr_article_8.pdf.

[19] Amnesty International, *Dangerously disproportionate: The ever-expanding national security state in Europe*. Amnesty International, 2017.

[20] Liberty International, "The people vs. the snoopers charter part 2," 2018, https://www.crowdjustice.com/case/snooperscharterpart2/ Accessed 14/4/2019.

[21] K. Renaud, S. Flowerday, R. English, and M. Volkamer, "Why don't UK citizens protest against privacy-invading dragnet surveillance?" *Information & Computer Security*, vol. 24, no. 4, pp. 400–415, 2016.

[22] ISO/IEC 29100, "Privacy Framework, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)," 2011, https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:29100:en Accessed 14/4/2019.

[23] ISO/IEC 27001, "Information Security Management Systems, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)." 2013, https://www.iso.org/isoiec-27001-information-security.html Accessed 14/4/2019.

[24] ICO, "Information commissioner's office (results for 'cloud')," https://icosearch.ico.org.uk/s/search.html?query=cloud&collection=ico-meta&profile=_default accessed 12/4/2019.

[25] D. Palmer, "Cloud computing: Why a major cyber-attack could be as costly as a hurricane," 2018, https://www.zdnet.com/article/cloud-computing-why-a-major-cyber-attack-could-be-as-costly-as-a-hurricane/.

[26] SPA Future Thinking, "Report on Information Commissioner's Office Annual Track 2012/13," online, 11 2014, https://ico.org.uk.

[27] S. Barlyn, "Insurance giant Lloyd's of London: Global cyber attack could trigger $53 billion in losses the same as Hurricane Sandy," 2017, https://www.businessinsider.com/r-global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-2017-7 Jul. 17 Accessed 14/4/2019.

[28] Cloud Security Alliance, "The notorious nine–cloud computing top threats in 2013," 2013, https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf Accessed 14/4/2019.

[29] B. Duncan, "FAST-CFP: Finding a Solution To The Cloud Forensic Problem," in *The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization*. Barcelona: IARIA, 2018, p. 3.

[30] I. Ferguson, K. Renaud, and A. Irons, "Dark Clouds on the Horizon: The Challenge of Cloud Forensics," *Cloud Computing*, p. 61, 2018.

[31] McAfee, "Cloud adoption and risk report," 2019, https://www.skyhighnetworks.com/cloud-report/ Accessed 14/4/2019.

[32] J. Fruhlinger, "The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet," 2018, mAR 9 https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html Accessed 14/4/2019.

[33] M. Mimoso, "Windows Botnet Spreading Mirai Variant," 2017, https://threatpost.com/windows-botnet-spreading-mirai-variant/123805/ 21 February, Accessed 14/4/2019.

[34] E. Meelhuysen, "Danger within: Defending cloud environments against insider threats," 2018, https://www.cloudcomputing-news.net/news/2018/may/01/danger-within-defending-cloud-environments-against-insider-threats/ 1 May, Accessed 14/4/209.

[35] Datacenters.com, "Locations," https://www.datacenters.com/locations/aws Accessed 12/4/2019.

[36] C. O'Donoghue and E. Brooks, "UK: Security Challenges Arising Out Of The Convergence Of Internet Of Things And Cloud Computing," 2018, http://www.mondaq.com/uk/x/739914/Security/Security+Challenges+Arising+Out+Of+The+Convergence+Of+Internet+Of+Things+And+Cloud+Computing 26 Sept, Accessed 14/4/2019.

[37] PWC, "UK Information Security Breaches Survey - Technical Report 2012 accessed 14/4/2019," PWC, Tech. Rep. April, 2012.

[38] R. Keeney and H. Raiffa, *Decisions with multiple objectives - preferences and value*. Cambridge University Press, 1994, vol. 39, no. 2.

[39] B. Duncan, D. J. Pym, and M. Whittington, "Developing a Conceptual Framework for Cloud Security Assurance," in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on (Volume 2)*. IEEE, 2013, pp. 120–125.

[40] A. Zellner, "Bayesian Estimation and Prediction Using Asymmetric Loss Functions," *Journal of the American Statistical Association*, vol. 81, no. 394, pp. 446–451, 1986.

[41] OWASP, "OWASP home page," 2017, https://www.owasp.org/index.php/Main_Page Accessed 14/4/2019.

 ISBN: 978-1-61208-703-0