Privacy: A Review of Publication Trends

Charlie Hinde[*] and Jacques Ophoff[†]
Centre for Information Technology and National Development in Africa (CITANDA)
Dept. of Information Systems
University of Cape Town
Cape Town, South Africa
Email: [*]charliehinde@gmail.com [†]jacques.ophoff@uct.ac.za

***Abstract*—The huge growth in digital data and the commercialisation of personal information has brought privacy to the forefront of world legislation. The impact and growth of the Internet, digitisation of data, network connectivity and data sharing has required a number of new threats to be addressed. As the technological environment has expanded since the 1960's and the use of electronic commerce has become more ubiquitous, so the concern around privacy and personal information protection has increased. Privacy is important at various levels and allows people to develop their individuality apart from the groups to which they belong and offers them the ability to decide what face they want others to see. Based on the recent Snowden leaks there is currently a heightened interest in privacy and related issues worldwide.**

The IEEE Security & Privacy magazine is one of the leading publications devoted to privacy, providing articles with both a practical and research focus by leading thinkers within the security and privacy field. The magazine has a broad audience which includes practitioners, researchers and policy-makers. The objective of this paper is to provide a systematic review of how privacy has been reported in the magazine over the past decade. The paper examines the shifts of privacy within the information security domain, with particular interest to the past three years which have seen revisions and amendments in various national privacy policies. In addition to reviewing the magazine there is input from the magazine's current editor, who shares her views and insights on both the magazine and privacy in general.

Findings show that over the period 2011–2013, privacy articles were predominantly driven by academic research, with the majority of security articles coming from within industry. There is little evidence that privacy has become a more dominant topic over the past ten years. While data loss and security breaches have escalated over the past decade the topic of privacy has taken second place to security.

***Index Terms*—Privacy, Managing Information Security.**

I. Introduction

The rise in information security breaches over the past five years, through either malicious intent or systems weakness, has shown how vulnerable our personal information is to abuse. The theft of laptops, loss of unencrypted USB drives, hackers infiltrating servers, staff deliberately accessing client's personal information, etc. are all regularly reported [1], [2].

The huge growth in digital data and the commercialisation of personal information has brought privacy to the forefront of South African, and world, legislation. The impact and growth of the Internet, digitisation of data, network connectivity and data sharing has required a number of new threats to be addressed. In South Africa, the Protection of Personal Information (PoPI) Act is an attempt to address privacy and lists a number of privacy commitments that businesses will need to attend to: transparency in the form of clear communications with clients; respect of people's personal information; a data subjects choice of whether their personal information can be shared; the accountability of users of personal data; and ensuring that privacy design is part of any new initiative, product or service and complies with regulatory requirements.

Despite this regulation it is not clear how much importance the topic of privacy receives, either from a personal or an informational perspective. Is privacy important in today's society and are there recurring debates? This high-level systematic review of the IEEE Security & Privacy magazine highlights the reporting of privacy-related articles over the magazine's ten year history. The review initially highlights all privacy-related articles before focussing on the past three years (2011–2013) in an attempt to see if there is a reporting trend that correlates to security breaches.

The overall objective of this paper is to provide a high-level review of how privacy has been reported over the past decade. The huge growth in digital data and the commercialisation of personal information has brought privacy to the forefront of world legislation. The impact and growth of the Internet, digitisation of data, network connectivity and data sharing has required a number of new threats to be addressed. This paper seeks to review the shifts, if any, of privacy within the information security domain, with particular interest to the past three years which have seen revisions and amendments in various national privacy policies.

The paper proceeds as follows: first several perspectives on privacy is given through a literature review. Next the research methodology and reviewed articles are discussed. The data analysis and a discussion of the results follows, before the paper is concluded.

II. Literature Review

Data privacy and data security are often used interchangeably. Data security is defined as the preservation of confidentiality, integrity and availability of data [3], or the practices and processes that are put in place to ensure data is being accessed by the right people. Data privacy is concerned with the appropriate use of data – is data used according to the agreed purposes at the time of collection [4].

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

A. What is Privacy – An Overview

The Oxford Dictionary defines privacy, as “the state of being left alone and not watched or disturbed by other people”. A person’s right to privacy is extended further than being merely ‘left alone’ and includes the right to having control over his or her personal information and the ability to conduct their personal affairs relatively free from unwanted intrusions [5]. Considered a fundamental human right it is recognised by the Universal Declaration of Human Rights , the International Covenant on Civil and Political Rights and in many other international and regional treaties [6]. Although privacy has deep seated roots in history (the law of privacy can be traced as far back as 1361, when the English Justices of the Peace Act provided for the arrest of peeping toms and eavesdroppers [6]), it is considered one of the most difficult human rights to define. While the definition of privacy describes how far society can intrude into a person’s affairs, privacy advocates describe privacy as having several aspects or categories [6]–[8]:

- Information privacy, involving the establishment of rules governing the collection and handling of personal data such as credit information and medical records
- Bodily privacy, concerning the protection of people’s physical beings against invasive procedures such as drug testing and cavity searches
- Privacy of communications, covering the security and privacy of mail, telephones, email and other forms of communication
- Territorial/physical privacy, concerning the setting of limits on intrusion into the domestic and other environments such as the work place or public space

B. Privacy and Data Protection

As the technological environment has expanded since the 1960’s, and the use of electronic commerce has become more ubiquitous, so the concern around privacy and personal information protection has increased [9], [10]. The advent of electronic communication has removed the obstacles of distance and time when transferring information and with this has come the possibility of information or data being intercepted and falling into the hands of unintended parties [8].

As the digitisation of information continues into the foreseeable future the question of whether privacy is distinct from data protection needs to be answered. The Information Technology Act of India, section 2(o), provides a comprehensive definition of data:

> …data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

Using this definition, data protection indicates the protection of information that can be generated using computer systems. Utilising the definition of data and applying it to the categories (aspects) of information privacy and privacy of communications mentioned earlier, it becomes apparent that data protection is also an aspect of privacy.

C. Why is Information Privacy Important?

As the sophistication of information technology escalates, and the interconnectivity of networks providing unprecedented methods of collecting, analysing and disseminating information on individuals increases, so the concern of the invasion of privacy, or the potential of invasion, increases correspondingly. [6] extend the technological aspects of privacy invasion to include three important trends:

- Globalisation removes geographical limitations to the flow of data - the development of the Internet is perhaps the best known example of a global technology
- Convergence is leading to the elimination of technological barriers between systems. Modem information systems are increasingly inter-operable with other systems, and can mutually exchange and process different forms of data
- Multi-media fuses many forms of transmission and expression of data and images so that information gathered in a certain form canbe easily translated into other forms

[11] provides four reasons why privacy is important, and these become more evident when considering the ease of proliferation of information, and the corresponding invasion thereof:

- Privacy is psychologically important: “People need private space. . . . We need to be able to glance around, judge whether the people in the vicinity are a threat, and then perform actions that are potentially embarrassing.”
- Privacy is sociologically important: “People need to be free to behave and to associate with others, subject to broad social mores, but without the continual threat of being observed.”
- Privacy is economically important: “People need to be free to innovate. International competition is fierce, so countries with high labour-costs need to be clever if they want to sustain their standard-of-living. And cleverness has to be continually reinvented.”
- Privacy is politically important: “People need to be free to think, and argue, and act. Surveillance chills behaviour and speech, and threatens democracy.”

Privacy allows people to develop their individuality apart from the groups to which they belong and offers them the ability to decide what face they want others to see [12].

D. The Costs of Protecting Privacy

While the protection of privacy outlined by [11] offers benefits to both society and individuals it must be tempered with the associated costs. While privacy allows individuals the opportunity to decide “what face they want others to see it is not an absolute good because it imposes real costs on society" [12, p. 465]. A broadly defined privacy right allows for the opportunity of withholding true information from society therefore protecting some individual rights at the expense of others. Promoting the possibility of misinformation can have both social and economic impacts as people are less able to make fully informed decisions such as whether a "child's babysitter had been convicted for child abuse or whether a physician had a history of malpractice" [12, p. 465].

The midpoint between too little or too much privacy is what progressive governments need to find the balance between. When looking at global privacy legislation there tends to be a minimum level of privacy protection without a maximum set [12]. In the case of South African legislation "the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests" [4].

E. International Privacy Legislation

Apart from the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, internationally privacy has been recognised as an important right to be protected. The advent of globalisation and economic imperatives has brought with it the need for nations to cooperate at numerous levels, one of which is ensuring the privacy of individuals.

The genesis of modern privacy legislation can be traced back to the Land of Hesse in Germany in 1970 which then prompted countries like Sweden (1973), Germany (1977) and France (1977) to follow suit [6]. Using this early legislation as a foundation two crucial international instruments evolved – The Council of Europe's (COE) 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data , and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. Both instruments lay out specific rules covering the handling of electronic data which now forms the core of many global data protection laws [6].

The European Union has extended the COEs 1981 legislation to take into consideration the globalisation of the information economy [13] and currently utilises the 1995 Data Protection Directive (in January 2012 the European Commission unveiled a draft European General Data Protection Legislation which will supersede the Data Protection Directive [14]). While Europe has legislated data privacy at a national level the United States has followed an industry-based self-regulation process. This laissez-faire governance system, where markets set the industry agenda, has resulted in existing legislation that is reactive and issue-specific [15], and is characterised as a "patchwork quilt" [16, p. 1] with no single overarching privacy law [17].

Globally there are many countries that now protect privacy under human rights legislation within their Constitutions: Kingdom of the Netherlands (Constitution of the Kingdom of the Netherlands, 1989), Republic of the Philippines (Part III, Constitution of the Republic of the Philippines, 1987), and the Russian Federation (art 23, Constitution of the Russian Federation, 1993). While the definition of data protection may vary across international laws and declarations, the attributes of personal information are consistently described as being: obtained fairly and lawfully; used only for the original specified purpose; adequate, relevant and not excessive to purpose; accurate and up to date; accessible to the subject; kept secure; and destroyed after its purpose is completed [6].

F. South African Privacy Legislation

In South Africa the right to privacy is protected in terms of both common law and the in the Constitution (section 14). However, the right to privacy is not absolute and consideration is given to competing interests such as maintaining law and order, protecting commercial interests, and the administration of national social programs [18]. While the right to privacy is balanced with other rights entrenched in the Constitution the recognition it has within the Constitution as a fundamental human right indicates its importance.

Apart from the Constitution (and common law) there is currently no legislation which deals specifically and fully with information protection [18]. In November 2000 the South African Minister of Justice and Constitutional Development requested the South African Law Reform Commission (SALRC) to investigate concerns around the protection of personal information. In September 2003 the SALRC published a comprehensive Issue Paper for information and comment entitled "Privacy and Data Protection" (known as Project 124) and received written comment from 34 persons and institutions. In October 2005 the SALRC published a Discussion Paper with draft legislation and invited comment towards the creation of the PoPI Bill (B9-2009).

In May 2009 the SALRC approved the investigation into privacy and data protection that the Minister of Justice initiated in 2000. The subsequent PoPI Act will protect individuals' personal information by penalising organisations and other parties that do not adequately protect personal information [13]. The objective of PoPI is to regulate the processing of personal information by public and private bodies while working within international standards – particularly European legislation.

Having outlined the concepts and challenges of privacy, the next section discusses the research methodology, including the rationale for the sample chosen.

III. Research Methodology

In order to gain an insight into digital privacy developments a descriptive literature review was undertaken. The review retrospectively analysed a decade's worth of privacy-related articles. The articles analysed was limited to the IEEE Security & Privacy magazine (S&P). S&P consists of an annual volume with six issues published and was first published in January 2003. The magazine currently has an impact factor of 0.9 [19].

S&P is one of 160 journals, magazines and research collections published by the IEEE. Providing articles with both a practical and research focus by leading thinkers within the

TABLE I
KEYWORD SEARCH LIST

Keyword Search Terms	No. of Articles
Privacy (information)	88
Security (information)	22
Data (protected/sharing)	14
Information Security (personal)	14
Identity (management)	9
Assurance (policy)	7
Law (privacy)	4
Personal information (data)	4
Policies (privacy)	4
Regulation (privacy)	2
Total	168

security and privacy field, the magazine provides case studies, tutorials, columns, book reviews, and in-depth interviews from within the information security industry.

The objective of S&P is best quoted as per their website [1]:

> The primary objective of IEEE Security & Privacy is to stimulate and track advances in information assurance and security and present these advances in a form that can be useful to a broad cross-section of the professional community-ranging from academic researchers to industry practitioners. It is intended to serve a broad readership.

S&P is envisioned to provide a unique combination of research articles, case studies, tutorials, and regular departments covering diverse aspects of information assurance such as legal and ethical issues, privacy concerns, tools to help secure information, analysis of vulnerabilities and attacks, trends and new developments, pedagogical and curricular issues in educating the next generation of security professionals, secure operating systems and applications, security issues in wireless networks, design and test strategies for secure and survivable systems, and cryptology [1].

According to the editor S&P opted to publish as a magazine (and not a journal) because "we have a broad audience: practitioners, researchers and policy-makers, and we try to make our articles accessible to all three types of readers. So, unlike a journal, which tends to report research by and for researchers, we try to inform our readers in an accessible way about the things they need to do their jobs" [20].

Having identified S&P as a reputable source of information, the indexes of each publication were captured into Microsoft Excel from the IEEE Xplore Digital Library. Each magazine index was then grouped per year and converted to a tabular format for easier analysis. Having obtained all the indexes and grouping them by their respective years, a keyword search was applied according to the words, or groupings of words, found in the titles of the articles to differentiate possible privacy-related articles. The results are shown in Table I in decreasing order of frequency. Note that an article could contain multiple keywords.

Applying the keywords, and reviewing the context in which they were used in the title of the article, provided an initial base for the identification of articles pertaining to privacy. A high-level abstract review of each article then followed to ensure no mismatches occurred. The initial application of the keywords provided a high correlation to the overall article-count and only three mismatched articles were identified following the abstract review and removed.

Having identified mismatched articles the data was then checked for any magazine volumes that revealed no privacy-related articles. The sub-categories of Privacy Interests and S&P Economics were subsequently reviewed for possible missing articles. This second review process provided an additional five articles which were initially missed by the keyword search as the respective terms were not in the article title. These articles were subsequently added to the overall total of privacy-related articles.

The next section presents the publication trends of privacy-related articles. It also presents possible explanations for these trends.

IV. Data Analysis and Discussion

The total number of privacy-related articles was 133. The distribution of privacy-related articles over a ten year period is illustrated in Table II. The first seven years show a fairly consistent publication of privacy-related articles. However, consideration needs to be given to the fact that the magazine prints on average approximately 100 articles per year, of which privacy articles make-up on average 13 articles of the total per annum (13%). In addition, the magazine offers insight into relevant topics in each issue by providing a "special edition" focusing on a central theme. There was no indication that these special editions included an additional focus on privacy-related topics.

The article count indicated a shift from the lowest recorded number of privacy-related articles (7) to the highest number (16) over the ten year period (see Figure 1), which could indicate a shift in public perception of privacy, or possibly legislative changes. With this in mind each privacy-related article from 2011-2013 was reviewed and summarised to provide insight into the increased article count over the three year period.

A. Privacy vs. Practice in 2011

There is a marked drop in privacy-related articles in 2011, as shown in Table III. Compared to 2010, half as many privacy articles appear in 2011, with the 4th volume of 2011 not having a single article. The predominant feature throughout the year's publications revolved around security, cyber-attacks, encryption, and secure IT infrastructure. This correlated closely to what was happening in the "IT world" in general, as a review of 2011 revealed major concerns around:

- hacktivism
- malicious code being spread by social media and the web (the Stuxnet worm was still a hot topic although it had been uncovered in 2010)
- attacks on high profile businesses like RSA

TABLE II
PRIVACY-RELATED ARTICLES BY YEAR

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	Total
Issue 1	2	3	3	2	2	2	3	2	2	2	2	25
Issue 2	4	3	2	1	1	4	2	1	2	1	2	23
Issue 3	1	1	1	3	3	1	2	1	1	1	8	23
Issue 4	1	2	1	2	1	1	3	4	0	1	2	18
Issue 5	2	1	2	1	4	5	1	1	1	2	2	22
Issue 6	4	3	1	3	2	1	1	5	1	1	0	22
Total	14	13	10	12	13	14	12	14	7	8	16	133

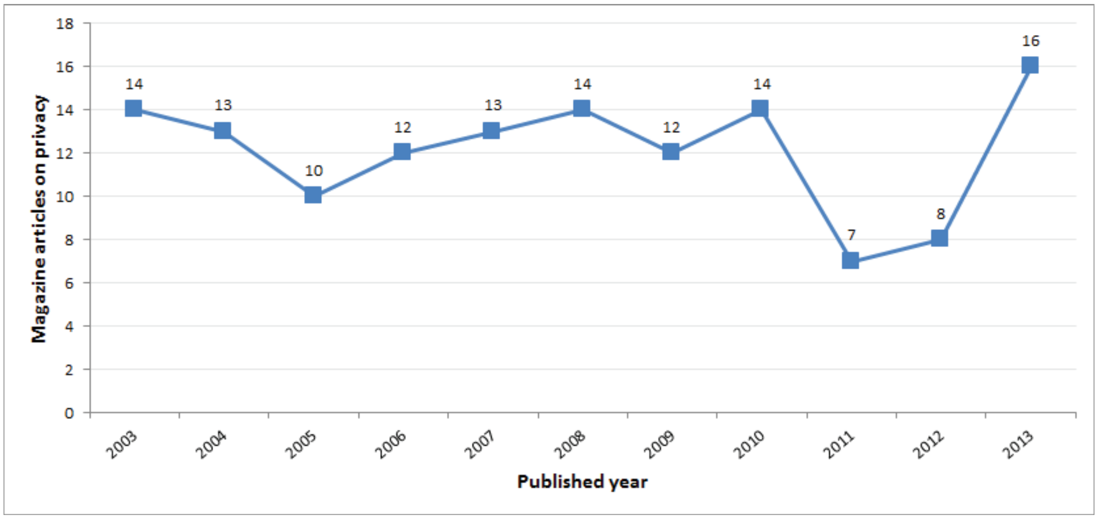

Fig. 1. Privacy-related Articles Published in S&P

- the undermining of SSL certificates and the companies that provide them (Comodo, GlobalSign, Digicert, OpenSSL and DigiNotar)
- the increase of bring your own device (BYOD) within business and the rise of the smartphone and the mobile revolution
- cyber warfare and the targeting of national assets, e.g. electricity grids [21], [22]

B. Privacy vs. Practice in 2012

Data from 2012 (illustrated in Table IV) reveal a similar pattern to 2011 with most of the focus on authentication, security, infrastructure security, software security, cyber warfare and cryptography. The magazine continued to run special editions throughout the year looking mainly at security related issues. Reviewing two security focused websites, Security Week and Sophos, 2012 is deemed to be another year where security lagged behind hackers and social engineering in terms of data breaches. Web servers and databases remained easy targets with IT professionals not implementing security policies and procedures effectively. Cybercriminal toolkits continued to evolve, mostly in response to security anti-virus firms understanding the shifts in security requirements. The growth of smartphones in 2012, with continued integration with social media platforms, improved technologies like near field communication (NFC) and GPS becoming pervasive in applications, provided greater exploitation mechanisms for both security and privacy [23], [24].

C. Privacy vs. Practice in 2013

The sudden increase in privacy-related articles in 2013 (illustrated in Table V) seems to be a direct response to the increase in online social networks activity, combined with the huge growth in smartphones and the BYOD phenomenon that IT departments throughout business are grappling with. The third volume of S&P in 2013 is dedicated to “Privacy & Online Social Networks” with 6 direct articles and 2 indirect articles – the largest single publication looking at privacy making up almost 50% of the articles for the volume. However, it must be noted that if the special edition focusing on privacy did not appear in 2013, the article count would be similar to the previous two years, with only 10 articles appearing after 5 volumes (volume 6 had not been published at the time of this review).

Reviewing the European Union Agency for Network and Information Security (ENISA) 2013 mid-year report shows a continued upward trend in malware, SQL code injections, exploit kits, botnets, identity theft and the abuse of information leakage [25]. While securing networks, servers, databases and websites requires IT security solutions like encryption, secure certification, password management and user authentication, the continued breaches that occur across all business sectors [2] indicates that utilising a technology-only approach is limited.

TABLE III
ARTICLES IN 2011

Issue	Includes Special Edition	Special Edition Topic	Special Edition Articles	Privacy-related Articles
1	Yes	Engineering Secure Systems	3	2
2	Yes	Shouldn't All Security Be Usable?	2	2
3	Yes	The Science of Security	3	1
4	No	–	–	0
5	Yes	Cyber warfare	4	1
6	Yes	Living with Insecurity	6	1

TABLE IV
ARTICLES IN 2012

Issue	Includes Special Edition	Special Edition Topic	Special Edition Articles	Privacy-related Articles
1	Yes	Authentication – Are We Doing Well Enough?	4	2
2	Yes	Security Training and Education	4	1
3	Yes	Software Assurance for the Masses	4	1
4	Yes	Internet Infrastructure Security	5	1
5	Yes	E-voting Security	5	2
6	Yes	Lost Treasures	5	1

TABLE V
ARTICLES IN 2013

Issue	Includes Special Edition	Special Edition Topic	Special Edition Articles	Privacy-related Articles
1	Yes	A View from the C-Suite	4	2
2	Yes	Transferring Security Technology	4	2
3	Yes	Privacy & Online Social Networks	6	8
4	Yes	Safety-Critical Systems	3	2
5	No	–	–	2
6	N/A	Not published at time of writing	–	–

TABLE VI
PRIVACY-RELATED ARTICLES BY SOURCE

Year	Academic	Non-Academic	Mixed	Total
2011	6	1	0	7
2012	5	2	1	8
2013	9	5	2	16
Total	20	8	3	31

D. Discussion

Reviewing the privacy-related articles from 2011–2013 provides an interesting observation – the majority of articles are written from an academic perspective (see Table VI). This is despite the fact that S&P is not a traditional academic journal.

From an academic perspective, a method of influencing privacy is by approaching government or regulatory bodies. In the United States the Federal Trade Commission (FTC), which comprises the Bureaus of Competition, Economics, and Consumer Protection, is the only federal agency with general jurisdiction over unfair and deceptive privacy practices. According to [26, p. 79] "the FTC's work is greatly facilitated by input from academic research communities, journalists, and independent researchers." [26, p. 82] continues by saying that research within the privacy field often aims to "directly inform technically sound policy decisions for everyone from national governments to end users."

It is interesting to note that over the period 2011–2013 privacy articles were predominantly driven by academic research, with the majority of security articles coming from within industry. According to the S&P editor the biggest shift with respect to privacy is:

> …the robust discussion based on Snowden's (Edward Snowden, the former NSA contractor who leaked US government surveillance secrets) recent revelations; before that, many people were ready to say that there is no longer any such thing as privacy. Now, that said, I'd say the European privacy directive laid the groundwork for the Snowden-related discussions.

The interplay between academia, industry and regulators is an important factor and should be taken into account in any intended publication to ensure that it is well-rounded.

V. CONCLUSION

The high-level systematic analysis of privacy-related articles within S&P provided little evidence that privacy has become a more dominant topic over the past ten years. While data loss and security breaches have escalated over the past decade the topic of privacy has taken second place to security.

No matter the strength of the preventative methods, guidelines or processes put in place, people continue to unwittingly hand over personal information (including passwords and other credentials). While social engineering has become sophisticated there is still a trusting naivete among users. The continued technological escalation between fraudster and IT security at times neglects the end user, and it is evident that technology on its own does not provide the only solution towards stopping privacy breaches. This is echoed by the editor of S&P, who notes that the biggest shifts in privacy noted over the years is that “a lot of technologists thought that technology would solve privacy problems; now I think they are realizing that it takes a combination of technology and policy – so the conversation is more informed by behavioural scientists than it used to be” [20]. The recent revelations published by Edward Snowden of the mass surveillance programs conducted by the United States, Israeli and British governments will hopefully shift the reporting of privacy from sporadic articles, to a more front-and-centre status as the public realize that privacy is a human right still worth protecting.

A limitation of this research is it’s focus on a single publication for review. Future research can build on it’s findings by adding additional journals or conference proceedings (academic as well as industry conferences such as Black Hat or DefCon) to affirm the identified trends. Investigation into reports of security breaches and privacy leaks can also provide additional insight into the academic versus professional reactions to these events.

References

[1] Security & Privacy, IEEE, “Security & privacy, IEEE,” 2013. [Online]. Available: http://ieeexplore.ieee.org/xpl/aboutJournal.jsp?punumber=8013

[2] Privacy Rights Clearinghouse, “Public policy & reports,” 2013. [Online]. Available: https://www.privacyrights.org/speeches-testimony

[3] ISO/IEC, “ISO 27001: Information technology - security techniques - information security management systems - requirements,” 2005.

[4] Minister of Justice and Constitutional Development, “The protection of personal information bill,” 2012.

[5] J. Neethling, J. Potgieter, and P. Visser, *Neethling’s law of personality*. Butterworths, 1996. [Online]. Available: http://books.google.co.za/books?id=c2c_AQAAIAAJ

[6] D. Banisar and S. Davies, “Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments,” *John Marshall Journal of Computer & Information Law*, vol. 18, no. 1, pp. 1–108, 1999.

[7] S. Kim, “Safeguarding consumer privacy in a technological era: A comparison of privacy protections in new zealand and california,” Fulbright New Zealand, Tech. Rep., 2006. [Online]. Available: http://www.fulbright.org.nz/wp-content/uploads/2011/12/axford2006_kim.pdf

[8] A. Marsoof, “The right to privacy in the information era: A south asian perspective,” *SCRIPT-ed*, vol. 5, no. 3, 2008.

[9] D. Hurley and V. Mayer-Schönberger, “Information policy and governance,” *JS Nye und JD Donahue (Hg.) Governance in a Globalizing World, Cambridge*, pp. 330–346, 2000.

[10] J. Zysman and S. Weber, *Governance and Politics of the Internet Economy: Historical Transformation Or Ordinary Politics With a New Vocabulary?* Berkeley Roundtable on the International Economy, 2000.

[11] R. Clarke, “Introduction to dataveillance and information privacy, and definitions of terms,” Aug. 1997. [Online]. Available: http://www.rogerclarke.com/DV/Intro.html

[12] J. M. Fromholz, “European union data privacy directive, the,” *Berk. Tech. LJ*, vol. 15, p. 461, 2000.

[13] Information Security Group of Africa, “Revealing privacy in south africa: What you need to know,” Information Security Group of Africa, Tech. Rep., 2011.

[14] M Law Group, “New draft european data protection regime,” Feb. 2012. [Online]. Available: http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227

[15] S. J. Kobrin, “Safe harbours are hard to find: the trans-atlantic data privacy dispute, territorial jurisdiction and global governance,” *Review of International Studies*, vol. 30, no. 1, p. 111131, 2004.

[16] J. Holvast, W. Madsen, and P. Roth, *The Global Encyclopaedia of Data Protection Regulations*, ser. The Global Encyclopaedia of Data Protection Regulations. Kluwer Law International, 1999, no. v. 1. [Online]. Available: http://books.google.co.za/books?id=TsvQkQEACAAJ

[17] L. B. Movius and N. Krup, “US and EU privacy policy: Comparison of regulatory approaches,” *International Journal of Communication*, vol. 3, p. 19, 2009.

[18] South African Law Reform Commission, “(Project 124) Privacy and Data Protection,” 2005. [Online]. Available: http://www.justice.gov.za/salrc/dpapers/dp109.pdf

[19] Research Gate, “IEEE security and privacy magazine (IEEE SECUR PRIV),” 2013. [Online]. Available: http://www.researchgate.net/journal/1540-7993_IEEE_Security_and_Privacy_Magazine

[20] S. L. Pfleeger, “Security & privacy magazine,” Nov. 2013.

[21] J. Hudson, “2011 IT security review. will 2012 be the year of ubiquitous encryption?” Dec. 2011. [Online]. Available: http://www.securityweek.com/2011-it-security-review-will-2012-be-year-ubiquitous-encryption

[22] J. Lyne, “Year in review: 2011,” 2011. [Online]. Available: http://www.sophos.com/en-us/security-news-trends/security-trends/2011-year-in-review.aspx

[23] F. Rashid, “’Tis the season for security resolutions, not predictions,” Dec. 2012. [Online]. Available: http://www.securityweek.com/tis-season-security-resolutions-not-predictions

[24] G. Eschelbeck, *Sophos Security Threat Report 2014*. Sophos, Dec. 2013. [Online]. Available: http://blogs.sophos.com/2013/12/10/sophos-security-threat-report-2014/

[25] European Union Agency for Network and Information Security, “ENISA threat landscape mid year 2013,” ENISA, Tech. Rep., 2013. [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013

[26] M. Brennan, “Academic impact at the federal trade commission,” *IEEE Security & Privacy*, vol. 10, no. 6, p. 7882, 2012.