*Proceedings of the Eleventh International Symposium on*
*Human Aspects of Information Security & Assurance (HAISA 2017)*

# Why Open Government is Good for Cybersecurity and Public Trust

C. Culnane and V. Teague

School of Computing and Information Systems, University of Melbourne
e-mail: {cculnane, vjteague}@unimelb.edu.au

## Abstract

We examine Australian cybersecurity public policy through four case studies of electronic systems with critical security and privacy requirements. Our first case studies are open data and electronic voting and counting. We then compare Australian and British approaches to communication interception. We explain why ambiguity and vagueness can prevent a genuine public discussion of a controversial issue, resulting in an outcome that nobody wanted. We highlight Australian examples of rules or proposals that inhibit the transparent disclosure of mistakes and thus prevent open fact-based public discussion. We find a need for greater transparency about how systems work and what problems have occurred, to make systems more secure and engender public trust.

## Keywords

Cybersecurity, public policy, e-voting, encryption, privacy, Awareness and education, Enhancing risk perception, Public understanding of security

## 1. Introduction

The human aspects of information security can be tested by rigorous empirical methods when the human is an ordinary end-user. When the humans are government officials and public policymakers, however, a carefully-controlled empirical test is harder to devise. Here we investigate information security culture, awareness and education methods, risk perception and public understanding of security. Our case studies are Australian public sector IT projects with strong security and privacy requirements.

We consider four examples: open government data, electronic voting and vote counting, and backdooring encryption. We observe several interrelated problems:

- confusion between trustworthiness and trust, *i.e.* between the public's belief in the system's security and the security itself,
- ambiguity in policy and legislation, producing outcomes that nobody intended,
- belief that secrecy keeps things secure,
- describing the identification and disclosure of security problems as irresponsible or trying to make it illegal.

When federal human services minister Alan Tudge said, "Nobody's health records can be accessed just with a Medicare card number and anybody who suggests otherwise is irresponsible and is fearmongering," (Elton-Pym, 2017) he was not only making a technical claim about an access control protocol. He was also objecting to public questions about its security.

We also find a small number of steps in the right direction:

- transparency about systems and processes for securing information,
- honesty about problems that have occurred,
- engagement with experts and other members of the public.

In the short term, projects and policies that are transparent and open to scrutiny will have more obvious errors and their problems will be more widely known to the public. In the longer run, we believe this approach will lead to better engineering, more secure systems, and more genuine and justified public trust.

It is long established in information security that security through obscurity does not work. The most trusted standards, such as those for RSA and AES, are completely open and always have been. When the international cryptography community wants a new standard, they run a long and open process in which proposals and criticisms are equally welcome (NIST CSRC, 2017).

Unfortunately our case studies often illustrate the opposite kind of cycle: good intentions uninformed by technical understanding, create systems or policies with serious flaws. These are often not described openly for fear that their problems will be exposed and that this will reduce public trust.

It would be better to establish a cycle more like that of the scientific cryptography and security community. Software always has bugs and security problems. The government could publish details long in advance, invite criticism and bug fixes, and thus gradually improve the security of its systems and the quality of its policies.

We first examine the re-identification of open government data, then the security and transparency of electronic voting and counting systems. We conclude with an examination of the proposal for compulsory interception of encrypted data. In each case we see that more openness about the details, and more openness to an explanation of its limitations, would have limited the unintended bad consequences.

## 2. Open Government Data

In September 2016 we showed that it was possible to decrypt the supplier IDs in the government's openly released de-identified sample of longitudinal MBS (Medicare Benefits Schedule) and PBS (Pharmaceutical Benefits Schedule) billing records. The method for obscuring supplier IDs was reasonably clearly described online. Hence it was feasible to analyse it, detect a problem and notify the government. The Department of Health (DoH) did the right thing by describing the algorithm in

enough detail that it was obvious what its weaknesses were. If the details hadn't been public, the algorithm would still have been insecure, but it would have been much harder for researchers to demonstrate the weaknesses and get the problem fixed. Unfortunately, like any privacy breach, it was too late when the data had already been published. If a similar level of detail *about the process* had been made available for analysis before the dataset was published, it is possible that the disaster could have been avoided altogether.

The release of highly sensitive longitudinal records as open data was motivated by genuine needs of public health researchers frustrated by the difficulty of accessing such data. De-identification is the process of taking data about individuals and transforming it into a form in which individuals cannot be identified. "De-identifying" the data and then posting it online seemed like a perfect solution for balancing privacy with the advantages of wide dissemination of data for research and informed public policy.

Unfortunately, this idea was not informed by the extensive scientific literature showing a long history of successful re-identifications of data that was released in the belief that it had been de-identified. It has been shown repeatedly to fail (Shmatikov & Narayanan, 2008), (Ohm, 2012). Yet governments persist in using it as a basis for releasing sensitive unit record level data (Australian Department of Health, 2016). Such datasets can often be re-identified, by combining them with auxiliary data, or including them in larger big data analytics processes.

A better and earlier review of the scientific literature would have shown the Department of Health that trying to de-identify such complex unit-record level data was probably not possible without removing most of its utility. Then they could have considered the problem of getting data to researchers in a more secure way.

### 2.1. The Re-identification Amendment

The Australian Attorney General announced the new crime of re-identification, effective immediately, in a short message on his website (Senator the Hon George Brandis QC , 2016). It bans re-identification of open government data that was released on the basis that it was de-identified.

This announcement occurred without warning or consultation, the day before our results on supplier re-identification were made public. Though aware that all the suppliers in the MBS-PBS dataset could be re-identified, the Attorney General claimed, "Data that is released is anonymised so that the individuals who are the subject of that data cannot be identified," (Attorney-General for Australia, 2016) and then went on to declare that re-identifying individuals would be a crime effective immediately. (Very few other impossible acts are crimes).

Legislating against re-identification is unlikely to prevent it (Ohm, 2012), because it can be performed in private without creating any incriminating evidence. There would be some argument for prohibiting certain crimes related to using re-identified

sensitive data, for extortion or discrimination *etc*. However, in Australia, and probably also in the UK when their legislation is written, the crime is broad enough to include researchers who report vulnerabilities to the government and then disclose them to the public.

Criminalising research does nothing to improve the security of the data release. It does, however, greatly inhibit scientific analysis of the privacy protections in the government's other open data releases. The Australian legislation goes as far as to include offences for "aiding, abetting, counselling or procuring" (Australian Government, 2016). Whilst a framework for exemptions is prescribed, requiring pre-approval from the government to conduct such research, there is no protection of the right to publish. This is not just a matter of public criticism (though that is important) – the government itself is likely to get much less careful analysis and accurate information about weaknesses in its methods.

At the time of writing, the bill has been blocked in the Senate. A Senate Inquiry into the legislation garnered 14 submissions, 13 of which recommended significant changes or abandonment. Its legal status is confusing. There is a promise that the legislation, when enacted, will be retrospective, but it looks unlikely to be enacted at all. Any Australian researchers who suspected there might be problems in the de-identification security of this or other datasets would have great difficulty understanding whether they could safely investigate.

So this example combines some very positive and also some of the most negative themes in Australian cybersecurity policy:

- An attempt to solve a genuine problem in a way that sounded like the best of both worlds but was actually disastrously insecure,
- Ambiguity about the legality of further research, including possible heavy penalties (which possibly will never be imposed),
- Some openness about how the data was treated, and an acknowledgement of the problem from the Dept of Health, but an insistence by the Attorney General that the procedure was "strict and standard" and that people could not be re-identified,
- A genuine effort by the Dept of Health to engage with security researchers, interrupted by an effort to make public re-identification a crime.

### 2.2. A better way of protecting privacy and earning trust

We were engaged by Transport New South Wales to examine the privacy-preservation techniques in a proposed release of data from the Opal card. Although the term "de-identified" was applied to the data, it didn't involve unit-record level data from individual people's trips or journeys - each data item was simply a count of the number of tap ons and tap offs at various locations. Scientists from Data61 had applied an algorithm for achieving Differential Privacy to these counts. We found that privacy was generally adequately preserved, though we showed some improbable scenarios in which it was possible to detect the presence of a particular

incident with a small probability. We recommended some modifications to the algorithm before future releases.

A description of the data treatment (Asghar, Tyler, & Kaafar, Differentially Private Release of Public Transport Data: The Opal Use Case, 2017a), our analysis (Culnane, Rubinstein, & Teague, 2017) and Data61's reply (Asghar, Tyler, & Kaafar, On the Privacy of the Opal Data Release: A Response, 2017b) are published online. They didn't entirely agree, which of course is as expected. In this way the discussion about open data becomes part of a grounded, scientific discussion. Other public authorities considering releasing data that derives from individuals can use the discussion, including the disagreements, as a basis for better-informed decisions.

## 3. Government Data that should be open: electronic counting code

Although sensitive unit-record level data about individuals should not be open, there is plenty of data about government that could be safely published. A long-running disagreement between the Australian Electoral Commission (AEC) and the Senate over the source code for the Senate count is a good example.

In 2014 the Australian Senate passed a resolution mandating the publication of the source code for the electronic Senate count. This supported a rejected Freedom of Information (FoI) request from Michael Cordover. The House of Representatives declined to pass the motion when the responsible minister argued "... that publication of the software could leave the voting system open to hacking or manipulation … The AEC classifies the relevant software as commercial-in-confidence," (Sharma, 2014). By the time the AEC brought the matter to the Administrative Appeals Tribunal, only the commercial-in-confidence argument remained, but the House motion had by then been defeated on spurious grounds.

Mr Cordover argued convincingly that all software has bugs and that it would be better to find and correct them than to allow them to go unnoticed. This argument is well supported by prior discoveries that the Australian Capital Territory's (ACT) counting code had errors (Logic and Computation Group NICTA, 2003), Conway *et al*'s discovery that the NSW counting code had errors that had led to a highly improbable election outcome (Conway, Blom, Naish, & Teague, 2016), and recent news that German counting code has "a host of problems and security holes" (Chaos Computer Club, 2017). The AEC attempted to have Mr Cordover labelled a "vexatious applicant" for FoI.

Thus a very simple matter, of opening code for which the equivalent is already online in Victoria and the ACT, illustrates three of the points in our introduction:

- a belief that obscuring errors will lead to public trust,
- a mistaken faith in secrecy as a guarantor of security,
- personal discrediting of the person who tried to bring the issues to light.

## 4. Internet voting

The NSW iVote internet voting system has been controversial since its inception. The system receives votes over the Internet and allows voters to "verify" them by telephoning an automated vote-reading system to query what vote is recorded for them. The source code for the system is not available to the public, and the processes for receiving votes and incorporating them into the count can be observed only by an auditor appointed by the electoral commission. Scrutineers can watch the auditor, but do not directly scrutinise the system or the votes. Independent security analyses by us and our colleagues have found a number of serious problems relating to vote privacy and integrity.

Although the system is marketed as verifiable, a number of problems in the conduct of state elections have come to light only after the expiry of the period in which a candidate may challenge the election result. In the 2011 state election, it was revealed months after the election that many of the ballots printed by the system had included at least one letter 'N' instead of a number. Immediately after the 2015 state election, the commission claimed on their website that "Some 1.7% of electors who voted using iVote also used the verification service and none of them identified any anomalies with their vote (NSW Electoral Commission, 2015). An official later admitted (after the opportunity to challenge the result had expired) that a handful of voters had indicated that they heard the wrong vote, and about 10% of verification attempts had not been able to retrieve any vote at all (Parliament of New South Wales, Joint Standing Committee on Electoral Matters, 2016). By this stage it was much too late for any careful investigation of why the problem might have occurred, including whether votes were affected.

The NSW electoral commission (NSWEC) was annoyed by negative press associated with independent security analysis. The NSWEC's Recommendations for legislative change in their report on the 2015 state election, recommended: "enhancing the electoral commissioner's ability to make approved procedures in connection with the iVote system that will ensure responsible disclosure of iVote system vulnerabilities." Note here the ambiguity in the term "responsible disclosure", which in the security research community means balancing the need to get problems fixed before publication with the public's right to learn about the risk as soon as possible. NSWEC stated, "The Commission believes that the appropriate time and place to engage in a discussion about the future direction of iVote in NSW is at the Joint Standing Committee on Electoral Matters," They do not seem to have considered that during the election period was a good time for voters to discuss the security of the voting system, nor for candidates to engage in a discussion about whether the validity of the result might be questioned.

When scrutineers or voters observe paper-based electoral processes, they have an opportunity to notice problems and engage in discussion immediately. A properly-run count leaves the observers with reasonable confidence that the outcome is correct. The internet-based process does not. The protocol does not necessarily detect all possible forms of error or manipulation. Even when it does, there is a

history of those problems not being reported to scrutineers or the public. In the short term, this retains public trust that might otherwise be negatively affected by the truthful disclosure of problems. In the longer term, we risk substantially undermining public trust in our electoral process.

## 5. The laws of mathematics are very commendable, but backdooring encryption is not

Attempts to weaken or "backdoor" encryption have a long history, including numerous demonstrations that the mechanisms designed for law enforcement access can also be exploited by others. The US Clipper chip was abandoned when security researchers showed that it leaked the decryption keys. In 2015 the FREAK and logjam attacks were demonstrated against the "export grade" encryption that used to be mandated by the US (with parameters that still apply in Australia's Defence Trade Controls Act (2012)). A flawed pseudorandom number generator – the Dual EC DRBG – has been found in use with a rekeyed backdoor (Checkoway, et al., 2016).

The introduction of the UK's Investigatory Powers Act would appear to present a new approach. The legislation is so ambiguous that it is not possible to determine whether or not it mandates the backdooring of encryption.

The part of the act that is of relevance to this discussion is Chapter 9, Section 253 (HM Government, 2016), which introduces technical capability notices. These notices can be used to impose on a telecommunication provider the requirement that they maintain the capability, where technically feasible, to intercept communications, including removing electronic protections. Clearly, a telecommunication provider that provides an end-to-end encrypted communication service is not going to be able to comply with such a requirement without either modifying their service so it is not end-to-end encrypted, or compromising the underlying cryptography in some way.

The definition of what is technically feasible is not provided, and despite repeated questioning, the Home Office has maintained a resolutely ambiguous stance. Since the scope of the legislation is dependent on the interpretation of what "technically feasible" means, the process by which Technical Capability Notices will be issued and challenged is vital. However, such notices are covered by a secrecy requirement, making it a criminal offence to disclose the receipt or contents of such notices. The technical capability notice does not constitute an interception warrant, or even result in the commencement of interception, it merely compels the receiver to maintain the capability to intercept if required to do so in the future. We see no legitimate national security reason for secrecy. It allows the government to compel private companies to maintain the capability to breach public privacy without public oversight or challenge.

The obfuscation of purpose and scope appears to be deliberate. It is extremely unfortunate because it prevents anyone analysing the proposal for weaknesses, let alone demonstrating them in order to have them corrected.

### 5.1. When a backdoor is not a backdoor

The Australian authorities have explicitly ruled out asking for a cryptographic backdoor. However, the Attorney General stated "...we don't propose to require backdoors as they're sometimes called, though there is a debate about what is and is not a backdoor. What we are proposing to do, [...], is to extend the existing law that says to individuals, citizens and to companies, that in certain circumstances you have an obligation to assist law enforcement if it's within your power to do so." (ABC, 2017) This is perfect example of ambiguity and contradiction. It creates the sense of ambiguity around what a "backdoor" is, despite there being very little debate in the field. It then proceeds to frame the requirement around assisting law enforcement, though such assistance would be impossible for a properly-implemented secure device or end-to-end encrypted service.

Clearly a communication provider has the power to introduce a backdoor or modify its protocol or device to make interception easier, which in turn would assist law enforcement. Many providers that make money out of analysing and reselling data already collect vast information about each user. Removing end-to-end encryption would make interception easy, since the service provider becomes a trusted third party who has the ability to intercept communication. Usage of such a protocol would not strictly be a backdoor, although it would be a serious weakening of security. Skype has made exactly such a switch over a number of years, culminating in it disabling the last remnants of its end-to-end encryption in 2017 (Skype, 2017). We should stress that there is no evidence that the move away was for reasons of interception. It could be entirely coincidental that the changes coincided with evidence of the NSA being able to intercept Skype communications (Greenwald, MacAskill, Poitras, Ackerman, & Rushe, 2013)

It can only be assumed that any new efforts to undermine encryption and device security will be as easy for bad actors to exploit as prior efforts have been. Ambiguity in the law will not make the systems more secure, it will simply make it difficult for companies to understand what they are obliged to do, and for security researchers to demonstrate weaknesses before bad actors find them.

If the government's intention is only to access the information that is already available to a provider, then it should say so clearly. This would leave companies free to engineer the best possible security and privacy protections for their customers. If the government's intention is to mandate the re-engineering of systems and devices to allow government access, then it should explain exactly what is required, so that the proposal is amenable to public analysis and a discussion of whether its benefits outweigh its risks.

## 6. Conclusion

In the next year more Australians will vote online, and more health data will be uploaded to the Internet. The federal government is already well advanced in planning a universal electronic identity and authentication system. We may, or may

not, have to do these things using devices and protocols that have been deliberately re-engineered to facilitate government data access.

Obscuring the details, denying problems, or deliberately using ambiguity to confuse debate, tends only to delay the notification of errors or vulnerabilities. The problems are still there, but the public (and often the government itself) doesn't have an opportunity to understand and address them.

If the Open Government philosophy is applied to the projects themselves, the details of how the systems work will be made openly available for public scrutiny. Like all good security projects, the government will welcome responsible notifications of errors and vulnerabilities, will tell the public honestly about them, and get them fixed. In this way systems will become gradually more secure over time and the government will be more trusted, not to keep things perfectly secure (which is impossible), but to be honest about what risks are known. Projects that adopt a transparent, open and engineering-focused approach to cybersecurity are much more likely to succeed.

## 7. References

ABC. (2017). Transcript ABC AM: Social media companies to face new Australian laws to force agency access to encrypted messages. Retrieved Sept 8, 2017, from http://www.abc.net.au/am/content/2016/s4701675.htm

ACOPEA. (2012). African Child Online Protection Education \& Awareness Centre. available online from: http://www.cto.int/media/events/pst-ev/2013/CTO%20Forum/African%20Child%20Online%20Protection%20Education%20\&%20Awareness%20Centre.pdf, Accessed on [12 November 2013].

Akester, P. (2009). Technological accommodation of conflicts between freedom of expression and DRM: the first empirical assessment. Cambridge: University of Cambridge.

Anderson, R. (2008). Security Engineering (2nd ed.). Hoboken: Wiley.

Antwi-bekoe, E., & Nimako, S. G. (2012). Computer Security Awareness and Vulnerabilities : An Exploratory Study for Two Public Higher Institutions in Ghana. Journal of Science and Technology, 1, 358-375.

Asghar, H. J., Tyler, P., & Kaafar, M. A. (2017a). Differentially Private Release of Public Transport Data: The Opal Use Case. CoRR, abs/1705.05957.

Asghar, H. J., Tyler, P., & Kaafar, M. A. (2017b). On the Privacy of the Opal Data Release: A Response. CoRR, abs/1705.08994.

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people . Computer Fraud \& Security , 2009(7), 13-19. Retrieved from http://www.sciencedirect.com/science/article/pii/S1361372309700880

Attorney-General for Australia. (2016). Amendment to the Privacy Act to further protect de-identified data. Retrieved Oct 23, 2017, from https://www.attorneygeneral.gov.au/Mediareleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx

Australian Department of Health. (2016). Public Release of Linkable 10% sample of Medicare Benefits Scheme (Medicare) and Pharmaceutical Benefits Scheme (PBS) Data. Retrieved Sept 8, 2017, from http://www.pbs.gov.au/info/news/2016/08/public-release-of-linkable-10-percent-mbs-and-pbs-data

Australian Government. (2016). Privacy Amendment (Re-identification Offence) Bill 2016. Commonwealth Government.

Ayodele, T., Shoniregun, C., & Akmayeva, G. (2012). Anti-Phishing Prevention Measure for Email Systems. Internet Security (WorldCIS), (pp. 208-211). Guelph.

Böhle, K. (2008). Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe. Retrieved April 16, 2015, from http://www.indicare.org/tiki-page.php?pageName=Downloads

Balta-Ozkan, N., Davidson, R., Bicket , M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. Energy Policy, 63, 363-374.

Becta. (2009). AUPs in context: Establishing safe and responsible online behaviours. available online from: http://education.qld.gov.au/studentservices/behaviour/qsaav/docs/establishing-safe-responsible-online-behaviours.pdf, Accessed on [10 November 2013].

Bhaveer, B., & Flowerday, S. (2013). Using participatory crowdsourcing in South Africa to create a safer living environment. International Journal of Distriuted Sensor Networks, 1-13.

Buhl, H. U., & Jetter, M. (2009). BISE's Responsibility for our Planet. Business and Information Systems Engineering, 1(4), pp. 273-276.

Byron, T. (2008). Safer Children in a Digital World. available online from: http://webarchive.nationalarchives.gov.uk/20130401151715/https://www.education.gov.uk/publications/eOrderingDownload/DCSF-00334-2008.pdf, Accessed on [5 November 2013].

Caragliu, A., Del Bo, C., & Nijkamp, P. (2009). Smart Cities in Europe. Series Research Memoranda 0048. Amsterdam: University of Amsterdam, Faculty of Economics, Business Administration and Econometrics.

Challener, J. D. (2013). Trusted Platform Module Evolution. JOHN HOPKINS APL TECHNICAL DIGEST , 32(2), 1.

Chaos Computer Club. (2017). Software to capture votes in upcoming national election is insecure. Retrieved Oct 23, 2017, from https://ccc.de/en/updates/2017/pc-wahl

Checkoway, S., Maskiewicz, J., Garman, C., Fried, J., Cohney, S., Green, M., . . . Shacham, H. (2016). A Systematic Analysis of the Juniper Dual EC Incident. Vienna, Austria: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.

Chen, J., & Guo, C. (2006). Online Detection and Prevention of Phishing Attacks. Communications and Networking in China, 2006. ChinaCom '06. First International Conference, (pp. 1-7). Beijing.

Chourabi, H., Nam, T., Walker , S., Gil-Garcia, J., Mellouli, S., Nahon, K., & Scholl, H. (2012). Understanding Smart Cities: An Integrative Framework. 45th System Science (HICSS) Hawaii International Conference (pp. 2289-2297). Hawaii: HICSS.

Christin, D. (2010). Impenetrable Obscurity vs Informed Decisions: Privacy Solutions for Participatory Sensing. In Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications (pp. 847-848). Mannheim: IEEE.

Christin, D., Kanhere, S., Reinhardt, A., & Hollick , M. (2011). A Survey on Privacy in Mobile Participatory Sensing Applications. Journal of Systems and Software, 84(11), 1928-1946.

Cilliers, L., & Flowerday , S. (2014). Information security in a public safety, participatory crowdsourcing smart city project. World CIS Conference (pp. 1-5). London: World CIS.

Cole, K., Chetty, M., Larosa, C., Rietta, F., Schmitt, D. K., & Goodman, S. E. (2008). Cybersecurity in Africa : An Assessment. available online from: http://s3.amazonaws.com/zanran_storage/www.cistp.gatech.edu/ContentPages/43945844.pdf, Accessed on [22 November 2013].

Conway, A., Blom, M. L., Naish, L., & Teague, V. (2016). An analysis of New South Wales electronic vote counting. CoRR, abs/1611.02015.

Culnane, C., Rubinstein, B. I., & Teague, V. (2017). Privacy Assessment of De-identified Opal Data: A report for Transport for NSW. CoRR, abs/1704.08547.

Darroch, C. (2012). Problems and Progress in the Protection of Videogames: A Legal and Sociological Perspective. The Manchester Review of Law, Crime and Ethics , 1(1), 136-172.

de Lange, M., & von Solms, R. (2012). An e-Safety Educational Framework in South Africa. Proceesing of the Southern Africa Telecommunication Networks and Applications Conference (SATNAC).

Diehl, E. (2012). Securing Digital Video (1 ed.). New York: Springer.

Dimitriou, T. (2012). Smart Internet of things in future cities (with emphasis on security). Berlin: Germany.

Dlamini, I., Taute, B., & Radebe, J. (2011). Framework for an African policy towards creating cyber security awareness. Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW), 15-31.

e4Africa. (2011). Technology in schools – for better or for worse. available online from: http://www.e4africa.co.za/?p=3516, Accessed on [20 November 2013].

Elton-Pym, J. (2017, July 4). Medicare data breach is the tip of the iceberg in the world of Australian dark web fraud . Retrieved from http://www.sbs.com.au/news/article/2017/07/04/medicare-data-breach-tip-iceberg-world-australian-dark-web-fraud?cid=inbody:government-and-afp-investigating-report-medicare-card-details-for-sale

Felten, E. W. (2003). A skeptical view of DRM and fair use. Communications of the ACM, 46(4), 57-59.

Flowerday, S., & Vol Solms, R. (2006). Trust: An Element of Information Security. SEC.

Furnell, S. (2005). Why users cannot use security. Computers & Security(24), 274-279.

Fuzile, L. (2011). Local Government budgets and expenditure. Pretoria: National Treasury.

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., & Rushe, D. (2013). Microsoft handed the NSA access to encrypted messages. Retrieved Sept 8, 2017, from https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

Grobler, M., & Dlamini, Z. (2012). Global Cyber Trends a South African Reality. IST-Africa 2012 Conference Proceedings.

Halder, B. (2014). Evolution of crowdsourcing: potential data protection, privacy and security concerns under the new Media Age. Democracia Digital eGoverno Electronico, 337-393.

Harrison, C., & Donnelly, I. (2011). A theoryof smart cities. Proceedings of the 55th Annual Meeting of the ISSS. London: University of Hull Business School.

Hart, H. (1955). Are there any natural rights. The Philosophical Review, 64(2), 175 -191.

HM Government. (2016). Investigatory Powers Act 2016. Retrieved Sept 8, 2017, from http://www.legislation.gov.uk/ukpga/2016/25/section/253/enacted

Huang, J., & Nicol, D. (2014). Evidence-based trust reasoning. HotSoS2014 (pp. 1-2). Raleigh: ACM.

IBM. (2010). Smarter Thinking for a Smarter Planet. Retrieved February 28, 2013, from IBM: http://www.ibm.com/smarterplanet/global/files/us_en_us_1oud_ibmlbn0041_transtasman_book.pdf

Introna, L. (1997). Privacy and the computer: why we need privacy in the Information Society. Metaphilosophy, 28(3), 259-275.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005, December 15). Social Phishing. Bloomington.

Janssen, C. (n.d.). Spear Phishing. Retrieved April 29, 2013, from Techopedia: http://www.techopedia.com/definition/4121/spear-phishing

Jisc. (2012). A guide to open educational resources. available online from: http://www.jisc.ac.uk/publications/programmerelated/2013/Openeducationalresources.aspx Accessed on [20 November 2013].

Kanyesigye, F. (n.d.). New drive to fight hackers, New Times. available online from: http://www.newtimes.co.rw/news/index.php?a=66437&i=15343, Accessed on [22 November 2013]., 2013.

Karadağ, T. (2013). An evolution of the Smart City Approach. Middle East Technical University.

Kortjan, N., & von Solms, R. (2013). Cyber Security Education in Developing Countries: A South African Perspective. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 119, 289-297.

Kritzinger, E. (2011). Cyber Awareness Implementation Plan (CAIP) for schools. Presentation for Southern African Cyber Security Awareness Workshop (SACSAW).

Ling, A., & Masao, M. (2011). Smart grid information security (IS) functional requirements. arXiv preprint arXiv:1109.4474, 2011.

Logic and Computation Group NICTA. (2003). Electronic Voting - A Review of the Hare-Clark Model of eVACS. Retrieved Oct 23, 2017, from http://users.cecs.anu.edu.au/~rpg/EVoting/evote_revacs.html

Mallalieu, L. (2005). An examination of the role of customer attributions in understanding trust loss and recovery in buyer-seller relationships. Supply Chain Forum: an International Journal, 6(2), 68-80.

Managa, S. (2012). Unfulfilled Promises and their Consequences: A Reflection on Local Goverment Performance and the Critical Issue of Poor Service Delivery in South Africa . Africa Insitute of South Africa, 76, 1-8.

Mars, M., & Erasmus, L. (2012). Telemedicine can lower health care costs in Africa. Innovate, 7, 32-33.

Mayer, R., Davis, J., & Schoorman, F. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), pp. 709-734.

Mehta, S. M. (2011, August 25). Mobile 311: a framework for 311 services with mobile technology. San Diego: San Diego State University.

Migrant. (2013). M-PESA International Money Transfer Service, Safaricom. available online from: http://www.ilo.org/dyn/migpractice/migmain.showPractice?p_lang=en\&p_practice_id=70, Accessed on [12 November 2013].

Miles, D. (2011). Youth protection: Digital citizenship - Principles and new resources. Second Worldwide Cybersecurity Summit (WCS), (pp. 1-3).

NIST CSRC. (2017). Post-Quantum Cryptography. Retrieved Oct 23, 2017, from https://csrc.nist.gov/projects/post-quantum-cryptography

NSW Electoral Commission. (2015). Response from the NSW Electoral Commission to iVote Security Allegations. Retrieved Oct 23, 2017, from http://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports/response_from_the_nsw_electoral_commission_to_ivote_security_allegations

OER_Africa. (2013). Understanding OER. available online from: http://www.oerafrica.org/understandingoer/UnderstandingOER/tabid/56/Default.aspx, Accessed on [20 November 2013].

Ohm, P. (2012). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA law review 57, p. 1701.

Parakkattu, S., & Kunnathur, A. (2010). A framework for research in infomration security management. Northeast Decision Sciences Institute Proceedings, 318-323.

Parliament of New South Wales, Joint Standing Committee on Electoral Matters. (2016). Hansard - Administration of the 2015 NSW election and related matters. Retrieved from https://www.parliament.nsw.gov.au/committees/inquiries/Pages/inquiry-hearing.aspx?pk=6951

Pearson, S. (2012). Privacy, security and trust in cloud computing. New York: IBM.

Pew Research Centre. (2014). Emerging nations embrace the Internet. Washington: Mobile Technology.

PWC. (2012). Telecoms in Africa: innovating and inspiring. Communications Review.

Qun, G. (2010). Digital Contents Interoperability between Diverse DRM Systems. Shandong : Intelligent Computing and Intelligent Systems .

Reed, M. (2012). Press release: Africa mobile subscriptions count to cross 750 million mark in fourth quarter of 2012. Informa Telecoms \& Media.

Safaricom. (2012). iCow. available online from: http://www.safaricom.co.ke/personal/value-added-services/social-innovation/icow, Accessed on [12 November 2013].

Safaricom. (2012). Relax, you've got M-Pesa. available online from: http://www.safaricom.co.ke/personal/m-pesa/m-pesa-services-tariffs/relax-you-have-got-m-pesa, Accessed on [12 November 2013].

Samuelson, P. (2003). DRM {and, or, vs.} the law. Communications of the ACM, 46(4), 41 - 45.

Sarwar, A., & Khan, M. (2013). A review of trust aspects in cloud computing security. International Journal of Cloud Computing and Services Science, 116-122.

Sato, N. (2013). ICT stakeholders discuss emerging issues on African cyber security. available online from: http://www.humanipo.com/news/32773/ict-stakeholders-discuss-emerging-issues-on-cyber-security, Accessed on [21 November 2013].

Senator the Hon George Brandis QC . (2016). Amendment to the Privacy Act to further protect de-identified data. Retrieved Sept 8, 2017, from https://www.attorneygeneral.gov.au/Mediareleases/Pages/2016/ThirdQuarter/Amendment-to-the-Privacy-Act-to-further-protect-de-identified-data.aspx

Sharma, M. (2014). Government rejects Senate order to disclose Electoral Commission software code. Retrieved Sept 8, 2017, from http://www.smh.com.au/it-pro/government-it/government-rejects-senate-order-to-disclose-electoral-commission-software-code-20140715-zti03.html

Shmatikov, V., & Narayanan, A. (2008). Robust de-anonymization of large sparse datasets. IEEE Symposium on Security and Privacy.

Skype. (2017). What does it mean that Skype is moving from peer-to-peer to the cloud. Retrieved Sept 8, 2017, from https://support.skype.com/en/faq/FA12381/what-does-it-mean-that-skype-is-moving-from-peer-to-peer-to-the-cloud

Spamhaus. (2010, January). Whitepapers: Effective filtering. Retrieved July 16, 2013, from Spamhaus: http://www.spamhaus.org/whitepapers/effective_filtering/

StatsSA. (2011). Key results: Census 2011. Retrieved January 21, 2015, from Stats South Africa: www.statssa.gov.za/Census2011/.../Census_2011_Key_results.pdf

Suna, D., Chang, G., Suna, L., & Wanga, X. (2011). Advanced in Control Engineering and Information Science surveying and analysing security, privacy and trust issues in cloud computing environments. Procedia Engineering, 2852-2856.

TeleGeography. (2013). Africa's international bandwidth growth to lead the world. TeleGeography: Global Bandwidth Forecast Service.

Think_U_Know. (2008). Welcome to Hector's World. available online from: http://www.thinkuknow.co.uk/5_7/hectorsworld/, Accessed on [15 November 2013].

Townsend, M. (2015). Parliament Square fence crushes protest rights, says Occupy Democracy. Retrieved April 13th, 2015, from http://www.theguardian.com/uk-news/2015/jan/03/boris-johnson-occupy-democracy-london-protest-fence

Varadharajan, V. (2009). A note on trust-enhanced security. IEEE Security and Privacy, 7, 57-59.

Wang, Y., Huang, Y., & Louis, C. (2012). Respecting user privacy in mobile crowdsourcing. ASE2012 (pp. 1-15). London: ASE.

Westin, A. (1967). Privacy and Freedom. New York: Atheneum Publishers.

Whitman, B., & Mattord, H. (2009). Principles of information security. Boston : Thomson Course Technology.