Initial Results from a Subject Matter Experts Study Towards the Development of Social Engineering eXposure Index (SEXI)

Abstract

Open source personal information (OSPI) provides cybercriminals and cyberterrorists the means to construct and successfully execute cyber attacks on the U.S. information technology that supports critical infrastructure. To better understand exposure to cybercrime due to OSPI, this study used the Delphi technique to identify, assess, and validate exposure components as well as categories of information and their contributing impact (i.e. weight) towards social engineering attacks, in an effort to construct the Social Engineering eXposure Index (SEXI). A panel of cybersecurity experts was provided with the initial 105 components of personal information extracted from the literature that may contribute to increase potential of individuals to be exposed to social engineering. Moreover, the experts were tasked with validating the list and their related exposure categories as well as validate the hierarchical aggregation to develop the SEXI benchmarking instrument. Validation of the instrument was conducted on a random selection of 50 executives of Fortune 500 organizations and a group of people where exposure of personal information is the norm (50 Hollywood celebrities) using OSPI via the Internet. This paper presents a discussion of the work-in-progress related to the development and validation of SEXI instrument due to OSPI.

Authors:

W. Shawn Wilkerson College of Engineering and Computing, Nova Southeastern University, ww364@mynsu.nova.edu

Dr. Yair Levy, College of Engineering and Computing, Nova Southeastern University

Dr. James Richard Kiper, Federal Bureau of Investigation

Infrastructure: Information Technology

Keywords: social engineering, open source personal information, cybersecurity, online information exposure, identity exposure, privacy, personal information, cyberterrorism, cyber threats

Introduction

The United States (U.S.) information technology (IT) critical infrastructure is under constant threat in the form of inquisitive youths, social engineers, hackers, state-sponsored terrorists, and others. In 2018, nine Iranians affiliated with the Mabna Institute were indicted for their part in a targeted campaign against the IT infrastructure "belonging to 144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children's Fund."[1] In 2016, seven state-sponsored Iranians were indicted, for the execution of distributed denial of service (DDOS)

attacks on approximately 50 U.S. financial institutions during 2011 – 2013, wherein they successfully blocked hundreds of thousands of customers from accessing their accounts, while one of their cohorts repeatedly penetrated the computers of the Bowman Dam.[2] While both sets of indictments relate to the U.S. IT critical infrastructure, the Mabna Institute specifically targeted the accounts of 100,000 professors in over 300 universities and successfully compromised the credentials of over 8,000 professors, thereby accessing an excess of 31 terabytes of intellectual property as well as data worth over $3 billion.[3] Cybercrime costs the global economy an estimated $500 billion each year.[4]

The availability of exposed personal information over the Internet often facilitates successful Social Engineering (SE) attacks on the IT infrastructure[5] and accessibility of Open source personal information (OSPI) increases with the passing of time.[6] OSPI provides access to an ever-growing heterogeneous repository that can be used to create SE attacks across multiple vectors on the IT infrastructure with little effort.[7] Even untrained high school students were able to mimic social engineers when they perpetrated the attack on the Director of the U.S. Central Intelligence Agency (CIA), wherein compromising a personal email account containing the personal information for many individuals associated with the CIA.[8] Those tasked with protecting the U.S. critical infrastructure have themselves become targets of SE attacks,[9] while those developing the technologies designed to protect data (e.g., RSA encryption) have also fallen to SE attacks.[10] Even academic journal articles are being stolen via SE.[11]

Over 1.9 trillion personal information records were exposed via data breaches in 2017 alone, bringing the total to exceed 10 trillion at the beginning of 2018.[12] Additionally, over 68% of American adults share information on Facebook and other social networks about themselves as well as relatives and/or others.[13] Research has also found that people may increase the amount of personal information disclosed if they perceive increased control over their privacy settings,[14] are warned about personal exposure,[15] or when presented with a security cue.[16] Research has also found that cybersecurity training is not providing the once-hoped-for benefit against SE.[17]

The research literature has called for the development of privacy protection tools,[18] as well as predictive tools to better understand information availability, identity exposure, and potential SE attack vectors.[19] Additionally, research has argued that a SE prediction tool could provide decision makers the information required to take an offensive position in risk mitigation and monitoring organizational exposure regarding their IT infrastructure.[20] A tendency exists to focus on a single SE attack vector in the literature, while little is known or shared as to the origination or composition of information that causes individuals to be more exposed than others to such cyber attacks.[21]

Personal Information

Personal information, in its broadest sense, means any information that identifies an individual.[22] Personally identifiable information (PII) refers to information that has the potential to identify an individual.[23] Open source refers to unclassified and non-secret data.[24] OSPI is defined as personal information openly available to anyone having access to the Internet.[25]

The research literature has indicated some difficulty in understanding personal information: it is highly contextual,[26] subjective,[27] and difficult to define.[28] Researchers have also found that the availability of exposed personal information often facilitates successful SE attacks.[29] Sets of personal information are often shared and sold via underground hacker markets, leading to multiple similar attacks occurring within 72 hours of the first penetration.[30]

To identify a U.S. citizen only their zip code, birthdate, and gender is required.[31] In addition, researchers have sounded the alarm of mass identity theft due to the simplicity of predicting Social Security Numbers,[32] while others stated that the entire concept of PII is broken.[33] Supporting this perspective is the ease by which deidentified data can be reidentified.[34]

National Institute for Standards and Technology (NIST) Special Publication 800-122 attributed three levels of potential harm to personal information using risk nomenclature of low, moderated, and high.[35] Similarly, Schwartz and Solove (2011) believed that the concept of PII needed to be expanded to delineate information that can distinguish an individual from personal information that cannot, in and of itself, identify an individual.[36] Following Schwartz and Solove (2011) as well as McCallister, Grance, and Scarfone (2010[31][31]), Table 1 presents the exposure categories identified, assessed, and validated for the SEXI benchmarking instrument.

Table 1

Exposure Categories

Term	**Potential Harm**	**Definition**
Personally distinguishable information (PDI)	High	"any information about an individual… that can be used to distinguish or trace an individual's identity… and is linked or linkable to an individual". (Section 2-1) [30, Section 2.1][37]
Personally identifiable information (PII)	Moderate	"refers to information that can be used to identify or locate an individual."(188)[38]
Personally unidentifiable information (PUI)	Low	"information that, taken alone, cannot be used to identify or locate an individual."(46)[39]

Personal Information Candidate Components

A literature review was performed to populate the initial list of personal information candidate components (PICC). Items were retrieved from big data,[40] confidentiality,[41] Federal Information Processing Standard (FIPS) Publication 201,[42] Health Insurance Portability and Accountability Act (HIIPA) of 1996,[43] intimate exchanges,[44] legal,[45] NIST SP 800-122,[46] Payment Card Industry Data Security Standard (PCI-DSS),[47] smartphone,[48] and social network[49] sources. For reference, the PICCs were arranged according to PDI, PII, or PUI based on how the respective

literature associated it or referred to it to establish a baseline. Duplicate or similar PICCs (e.g., birthdate/date of birth) were merged to reduce the number to 105 items. An alphabetical list of the PICCs was then presented to a Delphi panel, comprised of those individuals with a minimum of seven years in information privacy as well as having industry certification.

The panel of experts was asked to assess the level of exposure on a scale of 0-10 for each PICC, as to how in-and-of-itself, it would identify an individual. Items assigned an aggregate of less than one were discarded, an aggregate score from 1-3 was assigned to the PUI exposure category, an aggregate of 4-8 was assigned to PII, and those with an aggregate score of 9-10 were designated as PDI. Consensus for Delphi rounds with the PICCs presented on a 0-10 ordinal scale was set at 75%.[50]

Table 2

Classification of Exposure Categories with 80% Consensus

Category	Exposure Level	Low Thresh hold	High Thresh hold
DNA	Does Not Apply	0	< 1
PUI	Unidentifiable	≥ 1	< 3
PII	Identifiable	≥ 3	< 9
PDI	Identified	≥ 9	10

The Delphi panel was also asked to suggest additional personal information items for each category. The panel of experts was presented the additional suggestions and discarded items for their consideration. Upon reaching consensus for each PICC, expert-suggest item, and items designated for removal using ordinal scales, the aggregated categories (e.g., Discard, PDI, PII, PUI) of PICCs were presented to the panel of experts. Consensus for rounds with the PICCs presented in nominal categories was set at 80%.[51]

Instrument Validation

The elicited feedback from the Delphi panel provided a prototype benchmarking tool to measure exposure to SE due to OSPI. An object-relational model (ORM) was created from the expert panel feedback, directly relaying the expert-approved benchmarking tool to a prototype modular Web application, with each module representing a different API (e.g., Facebook, Google, Twitter metadata, Open Graph microdata). Initially, only three modules were identified to validate the instrument, while the possibility exists to add additional modules in the future.

Two groups of people were identified to validate the instrument: 50 Hollywood personas due to their high level of exposure and 50 executives of Fortune 500 companies, all done via OSPI available on the Internet. Each person was assessed to ascertain their level of exposure to SE to determine their respective SEXI classification. The aggregate score for each instrument item was compared between the two groups to ascertain if any statistically significant mean difference existed. The aggregate SEXI of the 50 Hollywood personas was compared with that of the 50

Fortune 500 executives to understand if one group was more vulnerable to SE attack due to OSPI.

Conclusions

The amount of personal information exposed through open sources continues to increase. Often, the exposed personal information of an individual facilitates the successful execution of a SE attack. The purpose of this research is to better understand the intersection of personal information and SE, investigated herein as exposure of OSPI. A study-in-progress proposed developmental research was presented, that intends to quantify exposure to SE due to OSPI. The proposed work would facilitate an offensive stance in organizational security, risk mitigation, cybersecurity, and decision making.

References

[1] U.S. Department of Justice. (2018). *Nine Iranians charged with conducting massive cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps*. Available: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[2] Federal Bureau of Investigation. (2016). *Iranians charged with hacking U.S. financial sector*. Available: https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector/iranians-charged-with-hacking-us-financial-sector

[3] N. Y. Conteh and P. J. Schmick, "Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research,* vol. 6, no. 23, 2016. doi: 10.19101/IJACR.2016.623006

[4] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys,* vol. 48, no. 3, pp. 1-39, 2015. doi: 10.1145/2835375

[5] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science,* vol. 347, no. 6221, pp. 509-514, 2015. doi: 10.1126/science.aaa1465

[6] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. New York, NY: John Wiley & Sons, 2002.

[7] L. Franceschi-Bicchierai. (2015, May 28, 2016). *Teen hackers: A '5-year-old' could have hacked into CIA Director's emails*. Available: https://motherboard.vice.com/read/teen-hackers-a-5-year-old-could-have-hacked-into-cia-directors-emails

[8] K. Krombholz, H. Hobel, G. P. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," *Proceedings of the 6th International Conference on Security of Information and Networks,* pp. 28-35, 2013. doi: 10.1145/2523514.2523596

[9] J. Hong, "The state of phishing attacks," *Communications of the ACM,* vol. 55, no. 1, pp. 74-81, 2012. doi: 10.1145/2063176.2063197

[10] M. Dadkhah and A. Quliyeva, "Social engineering in academic world," *Journal of Contemporary Applied Mathematics-ISSN: 2222-5498,* vol. 4, no. 2, 2015.

[11] Privacy Rights Clearinghouse. (2018, January 01, 2018). *Data Breaches*. Available: https://www.privacyrights.org/data-breaches

[12] S. Greenwood, A. Perrin, and M. Duggan. (2016). *Social media update 2016*. Available: assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/10132827/PI_2016.11.11_Social-Media-Update_FINAL.pdf

[13] J. Sutanto, E. Palme, C.-H. Tan, and C. W. Phang, "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users," *MIS Quarterly,* Article vol. 37, no. 4, pp. 1141-A5, 2013. doi: 10.25300/misq/2013/37.4.07

[14] M. Junger, L. Montoya, and F. J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Computers in Human Behavior,* vol. 66, pp. 75-87, 2017. doi: 10.1016/j.chb.2016.09.012

[15] B. Zhang, M. Wu, H. Kang, E. Go, and S. S. Sundar, "Effects of security warnings and instant gratification cues on attitudes toward mobile websites," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 111-114, 2557347: ACM. doi: 10.1145/2556288.2557347

[16] P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behaviour & Information Technology,* vol. 32, no. 10, pp. 1014-1023, 2013. doi: 10.1080/0144929X.2013.763860

[17] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly,* Article vol. 35, no. 4, pp. 1017-A36, 2011. doi: 10.2307/41409971

[18] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security,* vol. 59, pp. 186-209, 2016. doi: 10.1016/j.cose.2016.03.004

[19] 18 U.S.C. § 2725.

[20] R. K. Chellappa and R. G. Sin, "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management,* vol. 6, no. 2-3, pp. 181-202, 2005. doi: 10.1007/s10799-005-5879-y

[21] C. S. Fleisher, "Using open source data in developing competitive and marketing intelligence," *European Journal of Marketing,* vol. 42, no. 7/8, pp. 852-866, 2008. doi: doi:10.1108/03090560810877196

[22] W. Hong and J. Y. L. Thong, "Internet privacy concerns: An integrated conceptualization and four empirical studies," *MIS Quarterly,* Article vol. 37, no. 1, pp. 275-298, 2013. doi: 10.25300/misq/2013/37.1.12

[23] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature,* vol. 54, no. 2, pp. 442-92, 2016. doi: 10.1257/jel.54.2.442

[24] D. J. Solove, "A taxonomy of privacy," (in English), *University of Pennsylvania Law Review,* Article vol. 154, no. 3, pp. 477-560, 2006. doi: 10.2307/40041279

[25] S. E. Jasper, "U.S. cyber threat intelligence sharing frameworks," *International Journal of Intelligence and CounterIntelligence,* vol. 30, no. 1, pp. 53-65, 2017. doi: 10.1080/08850607.2016.1230701

[26] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," *Proceedings of the 2nd ACM workshop on Online social networks,* pp. 7-12, 2009. doi: 10.1145/1592665.1592668

[27] A. Acquisti and R. Gross, "Predicting Social Security numbers from public data," *Proceedings of the National Academy of Sciences,* vol. 106, no. 27, pp. 10975-10980, 2009. doi: 10.1073/pnas.0904891106

[28] R. Anderson *et al.*, "Measuring the cost of cybercrime," in *The economics of information security and privacy*: Springer, 2013, pp. 265-300. doi:DOI 10.1007/978-3-642-39498-0__12

[29] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *The Journal Of Law, Medicine & Ethics: A Journal Of The American Society Of Law, Medicine & Ethics,* vol. 25, no. 2-3, pp. 98-110, 1997. doi: 10.1111/j.1748-720x.1997.tb01885.x

[30] U.S. Department of Commerce. (2010). *SP 800-122, Guide to protecting the confidentiality of personally identifiable information (PII)*. Available: http://doi.org/10.6028/NIST.SP.800-122

[31] P. M. Schwartz and D. J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information," *New York University Law Review,* vol. 86, no. 6, pp. 1814-1894, 2011.

[32] Federal Trade Commission, "Privacy online: Fair information practices in the electronic marketplace: A federal trade commission report to Congress," *Washington DC: FTC,* 2000.

[33] K. E. Martin, "Ethical issues in the big data industry," *MIS Quarterly Executive,* vol. 14, no. 2, 2015.

[34] (2013). *FIPS PUB 201-2, Personal identity verification (PIV) of federal employees and contractors*. Available: http://dx.doi.org/10.6028/nist.fips.201-2

[35] "Health Insurance Portability and Accountability Act of 1996," ed, 1996.

[36] Y. Moon, "Intimate exchanges: Using computers to elicit self-disclosure from consumers," *Journal of Consumer Research,* Article vol. 26, no. 4, pp. 323-339, 2000. doi: 10.1086/209566

[37] PCI Security Standards Council. (2016). *Payment Card Industry (PCI) Data Security Standard, v3.2*. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

[38] J. Kang, K. Shilton, D. Estrin, and J. Burke, "Self-surveillance privacy," *Iowa Law Review,* vol. 97, pp. 809-848, 2011. doi: 10.2139/ssrn.1729332

[39] I. R. Diamond *et al.*, "Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies," *Journal of Clinical Epidemiology,* vol. 67, no. 4, pp. 401-409, 2014. doi: 10.1016/j.jclinepi.2013.12.002

---

[1] [1] U.S. Department of Justice. (2018). *Nine Iranians charged with conducting massive cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps*. Available: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[2] [2] Federal Bureau of Investigation. (2016). *Iranians charged with hacking U.S. financial sector.* Available: https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector/iranians-charged-with-hacking-us-financial-sector

[3] [1] U.S. Department of Justice. (2018). *Nine Iranians charged with conducting massive cyber theft campaign on behalf of the Islamic Revolutionary Guard Corps*. Available: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

[4] [3] N. Y. Conteh and P. J. Schmick, "Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research,* vol. 6, no. 23, 2016. doi: 10.19101/IJACR.2016.623006

[5] [4] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys,* vol. 48, no. 3, pp. 1-39, 2015. doi: 10.1145/2835375

[6] [5] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science,* vol. 347, no. 6221, pp. 509-514, 2015. doi: 10.1126/science.aaa1465

[7] [6] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. New York, NY: John Wiley & Sons, 2002.

[8] [7] L. Franceschi-Bicchierai. (2015, May 28, 2016). *Teen hackers: A '5-year-old' could have hacked into CIA Director's emails*. Available: https://motherboard.vice.com/read/teen-hackers-a-5-year-old-could-have-hacked-into-cia-directors-emails

[9] [8] K. Krombholz, H. Hobel, G. P. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," *Proceedings of the 6th International Conference on Security of Information and Networks,* pp. 28-35, 2013. doi: 10.1145/2523514.2523596

[10] [9] J. Hong, "The state of phishing attacks," *Communications of the ACM,* vol. 55, no. 1, pp. 74-81, 2012. doi: 10.1145/2063176.2063197

[11] [10] M. Dadkhah and A. Quliyeva, "Social engineering in academic world," *Journal of Contemporary Applied Mathematics-ISSN: 2222-5498,* vol. 4, no. 2, 2015.

[12] [11] Privacy Rights Clearinghouse. (2018, January 01, 2018). *Data Breaches*. Available: https://www.privacyrights.org/data-breaches

[13] [12] S. Greenwood, A. Perrin, and M. Duggan. (2016). *Social media update 2016.* Available: assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/10132827/PI_2016.11.11_Social-Media-Update_FINAL.pdf

[14] [13] J. Sutanto, E. Palme, C.-H. Tan, and C. W. Phang, "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users," *MIS Quarterly,* Article vol. 37, no. 4, pp. 1141-A5, 2013. doi: 10.25300/misq/2013/37.4.07

[15] [14] M. Junger, L. Montoya, and F. J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Computers in Human Behavior,* vol. 66, pp. 75-87, 2017. doi: 10.1016/j.chb.2016.09.012

[16] [15] B. Zhang, M. Wu, H. Kang, E. Go, and S. S. Sundar, "Effects of security warnings and instant gratification cues on attitudes toward mobile websites," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 111-114, 2557347: ACM. doi: 10.1145/2556288.2557347

[17] [16] P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behaviour & Information Technology,* vol. 32, no. 10, pp. 1014-1023, 2013. doi: 10.1080/0144929X.2013.763860

[18] [17] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly,* Article vol. 35, no. 4, pp. 1017-A36, 2011. doi: 10.2307/41409971

[19] [4] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys,* vol. 48, no. 3, pp. 1-39, 2015. doi: 10.1145/2835375

[20] [18] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Computers & Security,* vol. 59, pp. 186-209, 2016. doi: 10.1016/j.cose.2016.03.004

[21] [16] P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behaviour & Information Technology,* vol. 32, no. 10, pp. 1014-1023, 2013. doi: 10.1080/0144929X.2013.763860

[22] [19] 18 U.S.C. § 2725.

[23] [20] R. K. Chellappa and R. G. Sin, "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management,* vol. 6, no. 2-3, pp. 181-202, 2005. doi: 10.1007/s10799-005-5879-y

[24] [21] C. S. Fleisher, "Using open source data in developing competitive and marketing intelligence," *European Journal of Marketing,* vol. 42, no. 7/8, pp. 852-866, 2008. doi: doi:10.1108/03090560810877196

[25] [21] ibid.

[26] [22] W. Hong and J. Y. L. Thong, "Internet privacy concerns: An integrated conceptualization and four empirical studies," *MIS Quarterly,* Article vol. 37, no. 1, pp. 275-298, 2013. doi: 10.25300/misq/2013/37.1.12

[27] [23] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature,* vol. 54, no. 2, pp. 442-92, 2016. doi: 10.1257/jel.54.2.442

[28] [24] D. J. Solove, "A taxonomy of privacy," (in English), *University of Pennsylvania Law Review,* Article vol. 154, no. 3, pp. 477-560, 2006. doi: 10.2307/40041279

[29] [4] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Computing Surveys,* vol. 48, no. 3, pp. 1-39, 2015. doi: 10.1145/2835375

[30] [25] S. E. Jasper, "U.S. cyber threat intelligence sharing frameworks," *International Journal of Intelligence and CounterIntelligence,* vol. 30, no. 1, pp. 53-65, 2017. doi: 10.1080/08850607.2016.1230701

[31] [26] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," *Proceedings of the 2nd ACM workshop on Online social networks,* pp. 7-12, 2009. doi: 10.1145/1592665.1592668

[32] [27] A. Acquisti and R. Gross, "Predicting Social Security numbers from public data," *Proceedings of the National Academy of Sciences,* vol. 106, no. 27, pp. 10975-10980, 2009. doi: 10.1073/pnas.0904891106

[33] [28] R. Anderson *et al.*, "Measuring the cost of cybercrime," in *The economics of information security and privacy*: Springer, 2013, pp. 265-300. doi:DOI 10.1007/978-3-642-39498-0__12

[34] [29] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *The Journal Of Law, Medicine & Ethics: A Journal Of The American Society Of Law, Medicine & Ethics,* vol. 25, no. 2-3, pp. 98-110, 1997. doi: 10.1111/j.1748-720x.1997.tb01885.x

[35] [30] U.S. Department of Commerce. (2010). *SP 800-122, Guide to protecting the confidentiality of personally identifiable information (PII)*. Available: http://doi.org/10.6028/NIST.SP.800-122

[36] [31] P. M. Schwartz and D. J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information," *New York University Law Review,* vol. 86, no. 6, pp. 1814-1894, 2011.

[37] [30] U.S. Department of Commerce. (2010). *SP 800-122, Guide to protecting the confidentiality of personally identifiable information (PII)*. Available: http://doi.org/10.6028/NIST.SP.800-122

[38] [20] R. K. Chellappa and R. G. Sin, "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management,* vol. 6, no. 2-3, pp. 181-202, 2005. doi: 10.1007/s10799-005-5879-y

[39] [32] Federal Trade Commission, "Privacy online: Fair information practices in the electronic marketplace: A federal trade commission report to Congress," *Washington DC: FTC,* 2000.

[40] [33] K. E. Martin, "Ethical issues in the big data industry," *MIS Quarterly Executive,* vol. 14, no. 2, 2015.
[41] [29] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *The Journal Of Law, Medicine & Ethics: A Journal Of The American Society Of Law, Medicine & Ethics,* vol. 25, no. 2-3, pp. 98-110, 1997. doi: 10.1111/j.1748-720x.1997.tb01885.x
[42] [34] (2013). *FIPS PUB 201-2, Personal identity verification (PIV) of federal employees and contractors*. Available: http://dx.doi.org/10.6028/nist.fips.201-2
[43] [35] "Health Insurance Portability and Accountability Act of 1996," ed, 1996.
[44] [36] Y. Moon, "Intimate exchanges: Using computers to elicit self-disclosure from consumers," *Journal of Consumer Research,* Article vol. 26, no. 4, pp. 323-339, 2000. doi: 10.1086/209566
[45] [31] P. M. Schwartz and D. J. Solove, "The PII problem: Privacy and a new concept of personally identifiable information," *New York University Law Review,* vol. 86, no. 6, pp. 1814-1894, 2011.
[46] [30] U.S. Department of Commerce. (2010). *SP 800-122, Guide to protecting the confidentiality of personally identifiable information (PII)*. Available: http://doi.org/10.6028/NIST.SP.800-122
[47] [37] PCI Security Standards Council. (2016). *Payment Card Industry (PCI) Data Security Standard, v3.2*. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf
[48] [38] J. Kang, K. Shilton, D. Estrin, and J. Burke, "Self-surveillance privacy," *Iowa Law Review,* vol. 97, pp. 809-848, 2011. doi: 10.2139/ssrn.1729332
[49] [5] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science,* vol. 347, no. 6221, pp. 509-514, 2015. doi: 10.1126/science.aaa1465
[50] [39] I. R. Diamond *et al.*, "Defining consensus: A systematic review recommends methodologic criteria for reporting of Delphi studies," *Journal of Clinical Epidemiology,* vol. 67, no. 4, pp. 401-409, 2014. doi: 10.1016/j.jclinepi.2013.12.002
[51] [39] ibid.