Privacy exposed

Wottrich, V.M.

REFERENCES

A

Aaker, J., & Fournier, S. (1995). A brand as a character, a partner and a person: Three perspectives on the question of brand personality. In F. R. Kardes & M. Sujan (Eds.), *NA - Advances in Consumer Research Volume 22* (pp. 391–395). Provo, UT: Association for Consumer Research. Retrieved from http://acrwebsite.org/volumes/7775/volumes/v22/NA-22

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–515. http://doi.org/10.2139/ssrn.2580411

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. http://doi.org/10.1109/msp.2005.22

Acquisti, A., & Grossklags, J. (2007). What can behavioral economics teach us about privacy. *Digital Privacy: Theory, Technologies and Practices*, *18*, 363–377. http://doi.org/10.1201/9781420052183.ch18

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274. http://doi.org/10.1086/671754

Adler, J. (1998). Eine informationsökonomische Perspektive des Kaufverhaltens [An information economical perspective of buying behavior]. *Wirtschaftswissenschaftliches Studium*, *27*(7), 341–347.

Agrawal, A., Sodhi, B., & TV, P. (2013). A multi-dimensional measure for intrusion: The intrusiveness quality attribute. In *Proceedings of the 9th International ACM Sigsoft Conference on Quality of Software Architectures* (pp. 63–68). New York, NY, USA: ACM. http://doi.org/10.1145/2465478.2465497

Aguirre, E., Mahr, D., Grewal, D., de Ruyter, K., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing*, *91*(1), 34–49. http://doi.org/10.1016/j.jretai.2014.09.005

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). Berlin and Heidelberg: Springer. http://doi.org/10.1007/978-3-642-69746-3_2

Ajzen, I. (2006). Constructing a TpB questionnaire: Conceptual and methodological considerations. Retrieved from http://www.unibielefeld.de/ikg/zick/ajzen construction a tpb questionnaire.pdf

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social*

behaviour. Englewood Cliffs, NJ: Prentice-Hall.

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole.

Ang, L., & Eisend, M. (2017). Single versus multiple measurement of attitudes. *Journal of Advertising Research*. Advance online publication. Retrieved from http://www.journalofadvertisingresearch.com/content/early/2017/01/12/JAR-2017-001.abstract

Apple. (2017). Use parental controls on your iPhone, iPad, and iPod touch. Retrieved from https://support.apple.com/en-us/HT201304

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*(2), 107–123. Retrieved from http://www.jstor.org/stable/25123858

B

Bailey, R., Wise, K., & Bolls, P. (2009). How avatar customizability affects children's arousal and subjective presence during junk food–sponsored online video games. *CyberPsychology & Behavior*, *12*(3), 277–283. http://doi.org/10.1089/cpb.2008.0292

Ball, K., & Webster, F. (2003). *The intensification of surveillance: Crime, terrorism and warfare in the information era*. London, UK: Pluto Press.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). http://doi.org/10.5210/fm.v11i9.1394

Barney, J. B., & Hansen, M. H. (1994). Trustworthiness as a source of competitive advantage. *Strategic Management Journal*, *15*(8), 175–190. http://doi.org/10.1002/smj.4250150912

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Cambridge, UK: John Wiley & Sons.

BBC. (2013). Is data the oil of the 21st Century? Retrieved from http://www.bbc.com/news/av/business-24516050/is-data-the-oil-of-the-21st-century

Bellman, S., Potter, R. F., Treleaven-Hassard, S., Robinson, J. A., & Varan, D. (2011). The effectiveness of branded mobile phone apps. *Journal of Interactive Marketing*, *25*(4), 191–200. http://doi.org/10.1016/j.intmar.2011.06.001

Berger, C. R., & Calabrese, R. J. (1975). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, *1*(2), 99–112. http://doi.org/10.1111/j.1468-2958.1975.tb00258.x

Bernritter, S. F., Verlegh, P. W. J., & Smit, E. G. (2016). Why nonprofits are easier to endorse on social media: The roles of warmth and brand symbolism. *Journal of Interactive Marketing*, *33*, 27–42. http://doi.org/10.1016/j.intmar.2015.10.002

Bettini, C., & Riboni, D. (2015). Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing*, *17*, 159–174. http://doi.org/10.1016/j.pmcj.2014.09.010

Bies, R. J. (1993). Privacy and procedural justice in organizations. *Social Justice Research*, *6*(1), 69–86. http://doi.org/10.1007/BF01048733

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*(10), 1022–1035. http://doi.org/10.1080/0144929X.2015.1028448

Boyd, D. M. (2008). *Taken out of context. American teen sociality in networked publics* (Doctoral dissertation, University of California). Retrieved from http://www.danah.org/papers/TakenOutOfContext.pdf

Boyles, J. L., Smith, A., & Madden, M. (2012). *Privacy and data management on mobile devices*. Retrieved from http://www.privacylives.com/wp-content/uploads/2012/09/PIP_MobilePrivacyManagement-092012.pdf

Brehm, J. W. (1966). *A theory of psychological reactance*. Oxford, UK: Academic Press.

Buck, C., Horbel, C., Kessler, T., & Christian, C. (2014). Mobile consumer apps: Big data brother is watching you. *Marketing Review St.Gallen*, *31*(1), 26–35. http://doi.org/10.1365/s11621-014-0318-2

Burgoon, J. K. (1982). Privacy and communication. *Communication Yearbook*, *6*, 206–249. http://doi.org/10.1080/23808985.1982.11678499

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48–64. http://doi.org/10.1057/cpcs.2012.13

Business Name Generator. (2017). Generate business name ideas. Retrieved from https://businessnamegenerator.com/

Bylund, C. L., Peterson, E. B., & Cameron, K. A. (2012). A practitioner's guide to interpersonal communication theory: An overview and exploration of selected theories. *Patient Education and Counseling*, *87*(3), 261–267. http://doi.org/10.1016/j.pec.2011.10.006

C

Cambridge Analytica. (2016). CA congratulates Donald Trump and Mike Pence [Press release]. Retrieved from https://ca-political.com/news/ca-congratulates-donald-

trump-and-mike-pence

Cecere, G., & Rochelandet, F. (2013). Privacy intrusiveness and web audiences: Empirical evidence. *Telecommunications Policy*, *37*(10), 1004–1014. http://doi.org/10.1016/j.telpol.2013.09.003

Çeltek, E. (2010). Mobile advergames in tourism marketing. *Journal of Vacation Marketing*, *16*(4), 267–281. http://doi.org/10.1177/1356766710380882

Centraal Bureau voor de Statistiek (CBS). (2015). Bevolking; kerncijfers [Country population; core statistics]. Retrieved from http://statline.cbs.nl/StatWeb/publication/?VW=T&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,60,%28l-1%29,l&HD=130605-0924&HDR=G1&STB=T

Chaudhuri, A., & Holbrook, M. B. (2001). The chain of effects from brand trust and brand affect to brand performance: The role of brand loyalty. *Journal of Marketing*, *65*(2), 81–93. Retrieved from http://www.jstor.org/stable/3203382

Chen, H.-T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19. http://doi.org/10.1089/cyber.2014.0456

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society*, *11*(3), 395–416. http://doi.org/10.1177/1461444808101618

ComScore. (2017). *Cross-platform future in focus*. Retrieved from http://www.comscore.com/Insights/Presentations-and-Whitepapers/2017/2017-US-Cross-Platform-Future-in-Focus?

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin*, *79*(2), 73–91. http://doi.org/10.1037/h0033950

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*(2), 10–19. http://doi.org/10.1002/dir.4000090204

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. http://doi.org/10.1287/orsc.10.1.104

D

Dahlén, M. (2005). The medium as a contextual cue: Effects of creative media choice. *Journal of Advertising*, *34*(3), 89–98. Retrieved from http://www.jstor.org/stable/4189311

Dardis, F. E., Schmierbach, M., & Limperos, A. M. (2012). The impact of game

customization and control mechanisms on recall of integral and peripheral brand placements in videogames. *Journal of Interactive Advertising*, *12*(2), 1–12. http://doi.org/10.1080/15252019.2012.10722192

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer- Mediated Communication*, *15*(1), 83–108. http://doi.org/10.1111/j.1083-6101.2009.01494.x

Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin*, *125*(6), 627–668. http://doi.org/10.1037/0033-2909.125.6.627

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic motivation and self-determination in human behavior*. New York, NY: Plenum.

Deci, E. L., & Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological Inquiry*, *11*(4), 227–268. http://doi.org/10.1207/s15327965pli1104_01

Delgado-Ballester, E. (2004). Applicability of a brand trust scale across product categories. *European Journal of Marketing*, *38*(5), 573–592. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/03090560410529222

Delgado-Ballester, E., & Munuera-Alemán, J. L. (2001). Brand trust in the context of consumer loyalty. *European Journal of Marketing*, *35*(11), 1238–1258. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/EUM0000000006475

Delgado-Ballester, E., & Munuera-Alemán, J. L. (2005). Does brand trust matter to brand equity? *Journal of Product & Brand Management*, *14*(3), 187–196. http://doi.org/10.1108/10610420510601058

Delgado-Ballester, E., Munuera-Alemán, J. L., & Yague-Guillen, M. J. (2003). Development and validation of a brand trust scale. *International Journal of Market Research*, *45*(1), 35–54. Retrieved from https://www.warc.com/ContentandPartners/MarketResearchSociety.info

Derlega, V. J. (1988). Self-disclosure: Inside or outside the mainstream of social psychological research? *Journal of Social Behavior & Personality*, *3*, 27–34. Retrieved from https://search.proquest.com/docview/1292239849?pq-origsite=gscholar

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. http://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research*, *17*(1), 61–80. http://doi.org/10.1287/

isre.1060.0080

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. http://doi.org/10.1057/ejis.2012.23

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, *17*(2), 34–51. http://doi.org/10.1002/dir.10053

Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *The Academy of Management Review*, *19*(2), 252–284. http://doi.org/10.2307/258705

Dunfee, T. W., Smith, N. C., & Ross, W. T. (1999). Social contracts and marketing ethics. *Journal of Marketing*, *63*(3), 14–32. Retrieved from http://proxy.uba.uva.nl:2048/docview/1296598925?accountid=14615

E

Eastin, M. S., Brinson, N. H., Doorey, A., & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior*, *58*, 214–220. http://doi.org/10.1016/j.chb.2015.12.050

Edwards, S. M., Li, H., & Lee, J.-H. (2002). Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads. *Journal of Advertising*, *31*(3), 83–95. http://doi.org/10.1080/00913367.2002.10673678

Egelman, S., Felt, A., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 211–236). Berlin and Heidelberg: Springer. http://doi.org/10.1007/978-3-642-39498-0_10

Eling, N., Widjaja, T., Krasnova, H., & Buxmann, P. (2013). Will you accept an app? Empirical investigation of the decisional calculus behind the adoption of applications on Facebook. In *Proceedings of the Thirty Fourth International Conference on Information Systems* (pp. 1–20). Milan, Italy: AISeL. Retrieved from http://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/8/

Esposti, S. D. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society*, *12*(2), 209–225. Retrieved from https://search.proquest.com/docview/1547988838?pq-origsite=gscholar

EU Data Protection Directive. (1995). Directive 95/46/EC of the European Parliament and of the council of 24 October 1995 on the protection of individuals with regard

to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, *38*(281), 31–50. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

EU ePrivacy Directive. (2002). Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). *Official Journal of the European Communities*, *201*, 37–47. Retrieved from http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

EU General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC. *Official Journal of the European Union*, *119*(1). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/%0D HTML/?uriDCELEX:32016R0679&fromDEN

European Commission. (2011). *Special Eurobarometer 359: Attitudes on data protection and electronic identity in the European Union.* Retrieved from https://data.europa.eu/euodp/en/data/dataset/S864_74_3_EBS359

European Commission. (2012). Safer Internet centres. Retrieved from https://ec.europa.eu/digital-single-market/en/safer-internet-centres

European Commission. (2015). Agreement on commission's EU data protection reform will boost digital single market [Press release]. Retrieved from http://europa.eu/rapid/press-release_IP-15-6321_en.htm

European Commission. (2018). Protection of personal data. Retrieved from http://ec.europa.eu/justice/data-protection/

F

Federal Trade Commission. (2013). *Mobile privacy disclosures: Building trust through transparency*. Retrieved from www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security Article No. 3*. Washington, DC, USA: ACM. http://doi.org/10.1145/2335356.2335360

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. London, UK: Sage.

Fife, E., & Orjuela, J. (2012). The privacy calculus: Mobile apps and user perceptions of privacy and security. *International Journal of Engineering Business Management*, *4*,

1–10. http://doi.org/10.5772/51645

Figueiredo, B., & Scaraboto, D. (2016). The systemic creation of value through circulation in collaborative consumer networks. *Journal of Consumer Research*, *43*(4), 509–533. http://doi.org/10.1093/jcr/ucw038

Flaherty, A. (2013, September 5). Americans growing more concerned over their online privacy: Study. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/09/05/online-privacystudy_%0Dn_3870670.html.

G

Good, N., Dhamija, R., Grossklags, J., Aronovitz, S., Thaw, D., Mulligan, D., & Konstan, J. (2005). Stopping spyware at the gate. In *Proceedings of the 2005 Symposium on Usable Privacy and Security* (pp. 43–52). Pittsburgh, PA, USA: ACM. http://doi.org/10.1145/1073001.1073006

Google. (2018). Control your app permissions on Android 6.0 and up. Retrieved from https://support.google.com/googleplay/answer/6270602?hl=en

Grassegger, H., & Krogerus, M. (2016, December 3). Ich habe nur gezeigt, dass es die Bombe gibt. *Das Magazin*. Retrieved from https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/

Grossklags, J., & Acquisti, A. (2007). When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *Proceedings (online) of the Sixth Workshop on Economics of Information Security (WEIS)*. Pittsburgh, PA, USA: WEIS. Retrieved from weis07.infosecon.net

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. http://doi.org/10.1016/j.dss.2016.10.002

H

Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). Online information privacy: Measuring the cost-benefit trade-off. In *Proceedings (online) of the 33rd International Conference on Information Systems (ICIS)*. AISeL. Retrieved from http://aisel.aisnet.org/icis2002/1

Harney, K. R. (2017, November 21). Equifax breach already taking a toll on consumers. *Chicago Tribune*. Retrieved from http://www.chicagotribune.com/classified/realestate/ct-re-1126-kenneth-harney-20171120-story.html

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York, NY: Guilford Press.

Hayes, A. F., & Matthes, J. (2009). Computational procedures for probing interactions

in OLS and logistic regression: SPSS and SAS implementations. *Behavior Research Methods*, *41*(3), 924–936. http://doi.org/10.3758/brm.41.3.924

Hu, Q., & Dinev, T. (2005). Is spyware an Internet nuisance or public menace? *Communications of the ACM*, *48*(8), 61–66. http://doi.org/10.1145/1076211.1076241

I

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. http://doi.org/10.1016/j.cose.2011.10.007

IMCO. (2011). *Consumer behaviour in a digital environment. Study.* Retrieved from http://www.europarl.europa.eu/document/activities/cont/201108/20110825ATT25258/20110825ATT25258EN.pdf

Isaac, M., Benner, K., & Frenkel, S. (2017, November 21). Uber hid 2016 breach, paying hackers to delete stolen data. *The New York Times*. Retrieved from https://www.nytimes.com/2017/11/21/technology/uber-hack.html

J

Jaffe, J. (2005). *Life after the 30-second spot: Energize your brand with a bold mix of alternatives to traditional advertising*. Hoboken, NJ: Wiley.

Jahangir, N., & Begum, N. (2007). Effect of perceived usefulness, ease of use, security and privacy on customer attitude and adaptation in the context of e-banking. *Journal of Management Research*, *7*(3), 147–157. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bah&AN=31603264&site=ehost-live

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research*, *37*(5), 858–873. http://doi.org/0.0.4.62/656423

K

Kahneman, D. (1973). *Attention and effort*. Englewood Cliffs, NJ: Prentice-Hall.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, *25*(6), 607–635. http://doi.org/10.1111/isj.12062

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. http://doi.org/10.1016/j.ijhcs.2013.08.016

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13* (pp. 3393–3402). Paris, France: ACM. http://doi.org/10.1145/2470654.2466466

Kellogg's. (2016a). Kellogg's Dino Dig Advergame. Retrieved January 2, 2016, from https://www.clubkelloggs.ca/en/dino-dig/

Kellogg's. (2016b). Kellogg's Fruit Loops Advergame. Retrieved January 2, 2016, from https://www.clubkelloggs.ca/contests/fl16q1/en/contest.aspx

Kesswani, N., & Lin, F. (2016). How privacy invasive Android apps are? In *Proceedings (online) of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 3731–3734). New Delhi, India: IEEE. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7724959&isnumber=7724213

Kim, S. J., Wang, R. J.-H., & Malthouse, E. C. (2015). The effects of adopting and using a brand's mobile application on customers' subsequent purchase behavior. *Journal of Interactive Marketing*, *31*, 28–41. http://doi.org/10.1016/j.intmar.2015.05.004

King, J., Lampinen, A., & Smolen, A. (2011). Privacy: Is there an app for that? In *Proceedings of the Seventh Symposium on Usable Privacy and Security Article 12*. New York, NY, USA: ACM. http://doi.org/10.1145/2078827.2078843

King, N. J., & Jessen, P. W. (2010). Profiling the mobile customer – Privacy concerns when behavioural advertisers target mobile phones – Part I. *Computer Law & Security Review*, *26*(5), 455–478. http://doi.org/10.1016/j.clsr.2010.07.001

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. http://doi.org/10.1016/j.cose.2015.07.002

Krafft, M., Arden, C. M., & Verhoef, P. C. (2017). Permission marketing and privacy concerns — why do customers (not) grant permissions? *Journal of Interactive Marketing*, *39*, 39–54. http://doi.org/10.1016/j.intmar.2017.03.001

Kwak, D. H., Clavio, G. E., Eagleman, A. N., & Kim, K. T. (2010). Exploring the antecedents and consequences of personalizing sport video game experiences. *Sport Marketing Quarterly*, *19*(4), 217–225. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=57194758&site=ehost-live

L

Lang, A. (2000). The limited capacity model of mediated message processing. *Journal of Communication*, *50*(1), 46–70. http://doi.org/10.1093/joc/50.1.46

Lavy, S., Mikulincer, M., Shaver, P. R., & Gillath, O. (2009). Intrusiveness in romantic

relationships: A cross-cultural perspective on imbalances between proximity and autonomy. *Journal of Social and Personal Relationships* , *26*(6–7), 989–1008. http://doi.org/10.1177/0265407509347934

Lee, D., LaRose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445–454. http://doi.org/10.1080/01449290600879344

Lee, M., & Youn, S. (2008). Leading national advertisers' uses of advergames. *Journal of Current Issues & Research in Advertising*, *30*(2), 1–13. http://doi.org/10.1080/10641734.2008.10505243

LeFebvre, R. (2012). The human element in cyber security: A study on student motivation to act. In *Proceedings of the 2012 Information Security Curriculum Development Conference* (pp. 1–8). Kennesaw, GA, USA: ACM. http://doi.org/10.1145/2390317.2390318

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62–71. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bah&AN=54525529&site=ehost-live

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems*, *54*(1), 471–481. http://doi.org/10.1016/j.dss.2012.06.010

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 501–510). Pittsburgh, PA, USA: ACM. http://doi.org/10.1145/2370216.2370290

Lin, Y.-H., Fang, C.-H., & Hsu, C.-L. (2014). Determining uses and gratifications for mobile phone apps. In J. Park, Y. Pan, K. CS, & Y. Yang (Eds.), *Future information technology. Lecture notes in electrical engineering, vol 309* (pp. 661–668). Berlin and Heidelberg: Springer. http://doi.org/10.1007/978-3-642-55038-6_103

Liu, Y. (2014). User control of personal information concerning mobile-app: Notice and consent? *Computer Law & Security Review*, *30*(5), 521–529. http://doi.org/10.1016/j.clsr.2014.07.008

Luzak, J. A. (2014). Privacy notice for dummies? Towards European guidelines on how to give "clear and comprehensive information" on the cookies' use in order to protect the Internet users' right to online privacy. *Journal of Consumer Policy*, *37*(4), 547–559. http://doi.org/10.1007/s10603-014-9263-3

M

Macneil, I. R. (1980). *The New Social Contract*. New Haven, CT: Yale University Press.

Malone, T. W., & Lepper, M. R. (1987). Making learning fun: A taxonomy of intrinsic motivations for learning. In R. E. Snow & M. J. Farr (Eds.), *Aptitude, learning, and instruction* (Vol. 3, pp. 223–253). Hillsdale, NJ: Lawrence Erlbaum.

Marketing Science Institute. (2014). 2014–2016 Research Priorities. Retrieved from http://www.jstor.org.proxy.uba.uva.nl:2048/stable/300000913

Martí-Parreño, J., Aldás-Manzano, J., Currás-Pérez, R., & Sánchez-García, I. (2013). Factors contributing brand attitude in advergames: Entertainment and irritation. *Journal of Brand Management*, *20*(5), 374–388. http://doi.org/10.1057/bm.2012.22

Maslowska, E., Putte, B. van den, & Smit, E. G. (2011). The effectiveness of personalized e-mail newsletters and the role of personal characteristics. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 765–770. http://doi.org/10.1089/cyber.2011.0050

Mattioli, D. (2012, August 23). On Orbitz, Mac users steered to pricier hotels. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB10001424052702304458604577488822667325882

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*(3), 709–734. http://doi.org/10.5465/amr.1995.9508080335

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, *4*, 540–565. Retrieved from http://heinonline.org/HOL/Page?handle=hein.journals/isjlpsoc4&div=27&g_sent=1&casa_token=&collection=journals

McDonald, A. M., & Cranor, L. F. (2010). Americans' attitudes about Internet behavioral advertising practices. In *Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society* (pp. 63–72). Chicago, IL, USA: ACM. http://doi.org/10.1145/1866919.1866929

McLaughlin, D., & Bodoni, S. (2016, August 29). Facebook's WhatsApp privacy changes raise EU, U.S. concerns. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-08-29/whatsapp-privacy-changes-raise-eu-concern-over-user-data-control

Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Computers in Human Behavior*, *28*(4), 1471–1477. http://doi.org/10.1016/j.chb.2012.03.010

Milne, G. R. (1997). Consumer participation in mailing lists: A field experiment. *Journal of Public Policy & Marketing*, *16*(2), 298–309. Retrieved from http://www.jstor.org.

proxy.uba.uva.nl:2048/stable/30000453

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*, *18*(3), 15–29. http://doi.org/10.1002/dir.20009

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, *25*(2), 238–249. Retrieved from http://www.jstor.org/stable/30000697

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing*, *12*(2), 206–215. Retrieved from http://www.jstor.org.proxy.uba.uva.nl:2048/stable/30000091

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449–473. http://doi.org/10.1111/j.1745-6606.2009.01148.x

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. http://doi.org/10.1016/j.chb.2012.07.008

Molesworth, M. (2006). Real brands in imaginary worlds: Investigating players' experiences of brand placement in digital games. *Journal of Consumer Behaviour*, *5*(4), 355–366. http://doi.org/10.1002/cb.186

Montgomery, A. L., & Smith, M. D. (2009). Prospects for personalization on the Internet. *Journal of Interactive Marketing*, *23*(2), 130–137. http://doi.org/10.1016/j.intmar.2009.02.001

Moore, E. S. (2006). *It's child's play: Advergaming and the online marketing of food to children*. Menlo Park, CA: Kaiser Family Foundation.

Morman, M. T. (2000). The influence of fear appeals, message design, and masculinity on men's motivation to perform the testicular self–exam. *Journal of Applied Communication Research*, *28*(2), 91–116. http://doi.org/10.1080/00909880009365558

Morosan, C., & DeFranco, A. (2015). Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management*, *47*, 120–130. http://doi.org/10.1016/j.ijhm.2015.03.008

MyPermissions. (2017). MyPermissions helps you reclaim control over your privacy online and on your devices. Retrieved from https://mypermissions.com/

N

Nabi, R. L., Roskos-Ewoldsen, D., & Dillman Carpentier, F. (2008). Subjective knowledge and fear appeal effectiveness: Implications for message design. *Health*

Communication, *23*(2), 191–201. http://doi.org/10.1080/10410230701808327

Narayanan, M., Koo, B., & Cozzarin, B. P. (2012). Fear of fraud and Internet purchasing. *Applied Economics Letters*, *19*(16), 1615–1619. http://doi.org/10.1080/13504851.2011.648313

Nass, C., & Moon, Y. (2000). Machines and mindlessness: Social responses to computers. *Journal of Social Issues*, *56*(1), 81–103. http://doi.org/10.1111/0022-4537.00153

Nass, C., Moon, Y., & Carney, P. (1999). Are people polite to computers? Responses to computer-based interviewing systems. *Journal of Applied Social Psychology*, *29*(5), 1093–1109. http://doi.org/10.1111/j.1559-1816.1999.tb00142.x

Nelson, M. R., & Waiguny, M. K. J. (2012). Psychological processing of in-game advertising and advergaming: Branded entertainment or entertaining persuasion? In L. J. Shrum (Ed.), *The psychology of entertainment media: Blurring the lines between entertainment and persuasion* (2nd ed., pp. 93–144). New York, NY: Routledge.

Nelson, M. R., Yaros, R. A., & Keum, H. (2006). Examining the influence of telepresence on spectator and player processing of real and fictitious brands in a computer game. *Journal of Advertising*, *35*(4), 87–99. http://doi.org/10.2753/joa0091-3367350406

Neys, J. L. D., Jansz, J., & Tan, E. S. H. (2014). Exploring persistence in gaming: The role of self-determination and social identity. *Computers in Human Behavior*, *37*(0), 196–209. http://doi.org/10.1016/j.chb.2014.04.047

Ng, J. Y. Y., Ntoumanis, N., Thøgersen-Ntoumani, C., Deci, E. L., Ryan, R. M., Duda, J. L., & Williams, G. C. (2012). Self-determination theory applied to health contexts: A meta-analysis. *Perspectives on Psychological Science*, *7*(4), 325–340. http://doi.org/10.1177/1745691612447309

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press. Retrieved from http://www.sup.org/books/title/?id=8862

Nissenbaum, H. (2015). *Respect for context as a benchmark for privacy online: What it is and isn't*. (B. Ruessker & D. Mokrosinska, Eds.), *Social dimensions of privacy*. Cambridge, UK: Cambridge University Press.

Noble, S. M., & Phillips, J. (2004). Relationship hindrance: Why would consumers not want a relationship with a retailer? *Journal of Retailing*, *80*(4), 289–303. http://doi.org/10.1016/j.jretai.2004.10.005

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. http://doi.org/10.1111/j.1745-6606.2006.00070.x

Nowak, G. J., & Phelps, J. (1992). Understanding privacy concerns. An assessment of

consumers' information-related knowledge and beliefs. *Journal of Direct Marketing*, *6*(4), 28–39. http://doi.org/10.1002/dir.4000060407

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing*, *9*(3), 46–60. http://doi.org/10.1002/dir.4000090307

NPO. (2016). Jongeren vertrouwen Facebook en Google niet [Young people don't trust Facebook and Google]. Retrieved from http://jij.eenvandaag.nl/uitslagen/69830/jongeren_vertrouwen_facebook_en_google_niet

O

Okazaki, S., Katsukura, A., & Nishiyama, M. (2007). How mobile advertising works: The role of trust in improving attitudes and recall. *Journal of Advertising Research*, *47*(2), 165–178. http://doi.org/10.2501/s0021849907070195

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising*, *38*(4), 63–77. http://doi.org/10.2753/JOA0091-3367380405

P

Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, *82*(4), 331–338. http://doi.org/10.1016/j.jretai.2006.08.006

Papacharissi, Z., & Gibson, P. L. (2011). Fifteen minutes of privacy: Privacy, sociality, and publicity on social network sites. In S. Trepte & L. Reinecke (Eds.), *Privacy online* (pp. 75–89). Heidelberg and New York: Springer.

Pariser, E. (2012). *The filter bubble: How the new personalized web is changing what we read and how we think*. London, UK: Penguin Books.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236. http://doi.org/10.1177/0093650211418338

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303. http://doi.org/10.1016/j.chb.2014.05.041

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 101–134. Retrieved from http://www.jstor.org/stable/27751067

Peng, W., Lin, J.-H., Pfeiffer, K. A., & Winn, B. (2012). Need satisfaction supportive game features as motivational determinants: An experimental study of a self-determination theory guided exergame. *Media Psychology*, *15*(2), 175–196. http://

doi.org/10.1080/15213269.2012.673850

Perlroth, N., & Bilton, N. (2012, February 15). Mobile apps take data without permission. *The New York Times*. Retrieved from https://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/

Persily, N. (2017). Can democracy survive the Internet? *Journal of Democracy*, *28*(2), 63–76. http://doi.org/10.1353/jod.2017.0025

Phelps, J., Nowak, G. J., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. Retrieved from http://www.jstor.org/stable/30000485

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. http://doi.org/10.1037/0021-9010.88.5.879

Przybylski, A. K., Rigby, C. S., & Ryan, R. M. (2010). A motivational model of video game engagement. *Review of General Psychology*, *14*(2), 154–166. http://doi.org/10.1037/a0019440

Pultier, A., Harrand, N., & Brandtzæg, P. B. (2016). *Privacy in mobile apps. Measuring privacy risks in mobile apps. SINTEF Rapport*. SINTEF. Retrieved from https://www.sintef.no/en/publications/publication/?pubid=CRIStin+1342265

R

Raney, A. A., Arpan, L. M., Pashupati, K., & Brill, D. A. (2003). At the movies, on the Web: An investigation of the effects of entertaining and interactive Web content on site and brand evaluations. *Journal of Interactive Marketing*, *17*(4), 38–53. http://doi.org/10.1002/dir.10064

Reding, V. (2012, February 23). How Europe is dealing with online privacy. *CNN*. Retrieved from http://edition.cnn.com/2012/02/23/opinion/reding-europe/

Redondo, I. (2012). The effectiveness of casual advergames on adolescents' brand attitudes. *European Journal of Marketing*, *46*(11), 1671–1688. Retrieved from http://www.emeraldinsight.com/doi/abs/10.1108/03090561211260031

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of Personality and Social Psychology*, *49*(1), 95–112. http://doi.org/10.1037/0022-3514.49.1.95

Reyns, B. W. (2013). Online routines and identity theft victimization. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238. http://doi.org/10.1177/0022427811425539

Rigby, S., & Ryan, R. M. (2011). *Glued to games: How video games draw us in and hold us spellbound*. Santa Barbara, CA: Praeger.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. http://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). New York, NY: Guilford.

Rossiter, J. R. (2011). *Measurement for the social sciences: The C-OAR-SE method and why it must replace psychometrics*. Berlin: Springer.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68–78. http://doi.org/10.1037//0003-066x.55.1.68

Ryan, R. M., Mims, V., & Koestner, R. (1983). Relation of reward contingency and interpersonal context to intrinsic motivation: A review and test using cognitive evaluation theory. *Journal of Personality and Social Psychology*, *45*(4), 736–750. http://doi.org/10.1037/0022-3514.45.4.736

Ryan, R. M., Rigby, C. S., & Przybylski, A. (2006). The motivational pull of video games: A self-determination theory approach. *Motivation and Emotion*, *30*(4), 344–360. http://doi.org/10.1037//0022-3514.45.4.736

S

Schein, V. E. (1977). Individual privacy and personnel psychology: The need for a broader perspective. *Journal of Social Issues*, *33*(3), 154–168. http://doi.org/10.1111/j.1540-4560.1977.tb01888.x

Shade, L., & Shepherd, T. (2013). Viewing youth and mobile privacy through a digital policy literacy framework. *First Monday*, *18*(12). http://doi.org/10.5210/fm.v18i12.4807

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising*, *28*(3), 37–51. http://doi.org/10.1080/00913367.1999.10673588

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. http://doi.org/10.1016/j.chb.2015.01.046

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the 32nd annual ACM conference on Human factors in*

computing systems (pp. 2347–2356). Seoul, Republic of Korea: ACM. http://doi.org/10.1145/2556288.2557421

Sichtmann, C. (2007). An analysis of antecedents and consequences of trust in a corporate brand. *European Journal of Marketing*, *41*(9/10), 999–1015. http://doi.org/10.1108/03090560710773318

Simon, H. A. (1982). *Models of bounded rationality: Empirically grounded economic reason*. Cambridge Massachusetts and London: MIT Press.

Sipior, J. C., Ward, B. T., & Volonino, L. (2014). Privacy concerns associated with smartphone use. *Journal of Internet Commerce*, *13*(3–4), 177–193. http://doi.org/10.1080/15332861.2014.947902

SmartInsights. (2017). *Mobile marketing statistics compilation*. Retrieved from https://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Smit, E. G., Bronner, F., & Tolboom, M. (2007). Brand relationship quality and its value for personal contact. *Journal of Business Research*, *60*(6), 627–633. http://doi.org/10.1016/j.jbusres.2006.06.012

Smit, E. G., van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, *32*, 15–22. http://doi.org/10.1016/j.chb.2013.11.008

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196. http://doi.org/10.2307/249477

Smith, Dinev, & Xu. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1015. http://doi.org/10.2307/41409970

So, J. (2013). A further extension of the extended parallel process model (E-EPPM): Implications of cognitive appraisal theory of emotion and dispositional coping style. *Health Communication*, *28*(1), 72–83. http://doi.org/10.1080/10410236.2012.708633

Statista. (2017). Number of apps available in leading app stores as of March 2017. Retrieved from https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Steel, E. (2013, June 12). Companies scramble for consumer data. *Financial Times*. Retrieved from http://ig-legacy.ft.com/content/f0b6edc0-d342-11e2-b3ff-00144feab7de#axzz3DHhrW6Hj

Sutanto, J., Palme, E., Tan, C.-H., & Chee, W. P. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, *37*(4), 1141–1164. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=91906295&site=ehost-live

T

Taddicken, M. (2014). The "privacy paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. http://doi.org/10.1111/jcc4.12052

Taggart, K. (2017, February 16). The truth about the Trump data team that people are freaking out about. *BuzzFeed News*. Retrieved from https://www.buzzfeed.com/kendalltaggart/the-truth-about-the-trump-data-team-that-people-are-freaking?utm_term=.qfoD5NWoR#.ugVNwMXKm

Tamborini, R., Bowman, N. D., Eden, A., Grizzard, M., & Organ, A. (2010). Defining media enjoyment as the satisfaction of intrinsic needs. *Journal of Communication*, *60*(4), 758–777. http://doi.org/10.1111/j.1460-2466.2010.01513.x

Teng, C.-I. (2010). Customization, immersion satisfaction, and online gamer loyalty. *Computers in Human Behavior*, *26*(6), 1547–1554. http://doi.org/10.1016/j.chb.2010.05.029

Terlutter, R., & Capella, M. L. (2013). The gamification of advertising: Analysis and research directions of in-game advertising, advergames, and advertising in social network games. *Journal of Advertising*, *42*(2–3), 95–112. http://doi.org/10.1080/00913367.2013.774610

Threema. (2018). Threema rigorously protects your privacy. Retrieved from https://threema.ch/en/

Thurm, S., & Kane, Y. I. (2010, December 17). What they know: Your apps are watching you. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/SB10001424052748704694004576020083703574602

TRUSTe. (2014). TRUSTe privacy index. 2014 consumer confidence edition. Retrieved from https://www.truste.com/resources/privacy-research/us-consumer-confidence-index-2014/

Tsang, M. M., Ho, S.-C., & Liang, T.-P. (2004). Consumer attitudes toward mobile advertising: An empirical study. *International Journal of Electronic Commerce*, *8*(3), 65–78. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/10864415.2004.11044301

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, *28*(1), 20–36. http://doi.org/10.1177/0270467607311484

Turow, J. (2013). *The daily you: How the new advertising industry is defining your identity and your worth*. New Haven, CT: Yale University Press.

V

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance Society*, *12*(2), 197–208. Retrieved from https://search.proquest.com/docview/1547988865?pq-origsite=gscholar

van Doorn, J., & Hoekstra, J. C. (2013). Customization of online advertising: The role of intrusiveness. *Marketing Letters*, *24*(4), 339–351. http://doi.org/10.1007/s11002-012-9222-1

van Noort, G., Antheunis, M. L., & Verlegh, P. W. J. (2014). Enhancing the effects of social network site marketing campaigns. *International Journal of Advertising*, *33*(2), 235–252. http://doi.org/10.2501/IJA-33-2-235-252

van Reijmersdal, E. A., Lammers, N., Rozendaal, E., & Buijzen, M. (2015). Disclosing the persuasive nature of advergames: Moderation effects of mood on brand responses via persuasion knowledge. *International Journal of Advertising*, *34*(1), 70–84. http://doi.org/10.1080/02650487.2014.993795

van Reijmersdal, E. A., Rozendaal, E., & Buijzen, M. (2012). Effects of prominence, involvement, and persuasion knowledge on children's cognitive and affective responses to advergames. *Journal of Interactive Marketing*, *26*(1), 33–42. http://doi.org/10.1016/j.intmar.2011.04.005

Vesanen, J. (2007). What is personalization? A conceptual framework. *European Journal of Marketing*, *41*(5/6), 409–418. http://doi.org/10.1108/03090560710737534

Vishwanath, A., & Chen, H. (2008). Personal communication technologies as an extension of the self: A cross-cultural comparison of people's associations with technology and their symbolic proximity with others. *Journal of the Association for Information Science and Technology*, *59*(11), 1761–1775. http://doi.org/10.1002/asi.20892

Vroom, V. H. (1964). *Work and motivation*. New York, NY: John Wiley & Sons.

W

Waiguny, M. K. J., Nelson, M. R., & Marko, B. (2013). How advergame content influences explicit and implicit brand attitudes: When violence spills over. *Journal of Advertising*, *42*(2–3), 155–169. http://doi.org/10.1080/00913367.2013.774590

Waiguny, M. K. J., Nelson, M. R., & Terlutter, R. (2014). The relationship of persuasion knowledge, identification of commercial intent and persuasion outcomes in advergames—the role of media context and presence. *Journal of Consumer Policy*, *37*(2), 257–277. http://doi.org/10.1007/s10603-013-9227-z

Wang, R. J., Kim, S., & Malthouse, E. C. (2016). Branded apps and mobile platforms as new tools for advertising. In R. E. Brown, V. K. Jones, & M. Wang (Eds.), *The new*

advertising: Branding, content, and consumer relationships in the data-driven social media era (pp. 123–156). Santa Barbara, CA: ABC-CLIO.

Wei, R., & Lo, V.-H. (2006). Staying connected while on the move: Cell phone use and social connectedness. *New Media & Society*, *8*(1), 53–72. http://doi.org/10.1177/1461444806059870

Westin, A. F. (1967). *Privacy and freedom*. New York, NY: Athenaeum.

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, *18*(4), 326–348. http://doi.org/10.1108/09564230710778128

Wise, K., Bolls, P. D., Kim, H., Venkataraman, A., & Meyer, R. (2008). Enjoyment of advergames and brand attitudes. *Journal of Interactive Advertising*, *9*(1), 27–36. http://doi.org/10.1080/15252019.2008.10722145

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=ufh&AN=9301100383&site=ehost-live

Wottrich, V. M., Verlegh, P. W. J., & Smit, E. G. (2017). The role of customization, brand trust, and privacy concerns in advergaming. *International Journal of Advertising*, *36*(1), 60–81. http://doi.org/10.1080/02650487.2016.1186951

X

Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. In *Proceedings of the 29th International Conference on Information Systems (ICIS) Paper 6*. Paris, France: AISeL. Retrieved from http://aisel.aisnet.org/icis2008/6

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. In *Proceedings of the 33rd International Conference on Information Systems (ICIS) Paper 10*. Orlando, Florida, USA: AISeL. Retrieved from http://aisel.aisnet.org/icis2012/proceedings/ISSecurity/10/

Y

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722. http://doi.org/10.1002/asi.20530

Yoon, S., Choi, Y. K., & Song, S. (2011). When intrusive can be likable. *Journal of Advertising*, *40*(2), 63–76. http://doi.org/10.2753/JOA0091-3367400205

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy

protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. http://doi.org/10.1111/j.1745-6606.2009.01146.x

Youn, S., & Lee, M. (2005). Advergame playing motivations and effectiveness. In M. R. Stafford & R. J. Faber (Eds.), *Advertising, promotion, and new media* (pp. 320–347). Armonk, NY: ME Sharpe.

Z

ZARA. (2013). ZARA Privacy Policy. Retrieved from http://static.zara.net/static//pdfs/US/privacy-policy/privacy-policy-en_US-20131125.pdf

Zhang, F., Shih, F., & Weitzner, D. (2013). No surprises: Measuring intrusiveness of smartphone applications by detecting objective context deviations. In *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society* (pp. 291–296). New York, NY, USA: ACM. http://doi.org/10.1145/2517840.2517864

Zuiderveen Borgesius, F. J. (2013). Behavioral targeting: A European legal perspective. *IEEE Security & Privacy*, *11*(1), 82–85. http://doi.org/10.1109/msp.2013.5

Zuiderveen Borgesius, F. J. (2015). Informed consent: We can do better to defend privacy. *IEEE Security & Privacy*, *13*(2), 103–107. http://doi.org/10.1109/msp.2015.34

AUTHOR CONTRIBUTIONS

Authors' Initials

Verena M. Wottrich (VW), Eva A. van Reijmersdal (EvR), Edith G. Smit (EGS), Peeter W. J. Verlegh (PV)

Chapter 2

App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps

Verena M. Wottrich, Eva A. van Reijmersdal, & Edith G. Smit

Conceptualization: VW, EvR, EGS. Methodology: VW, EvR, EGS. Data collection: VW. Analysis: VW. Writing (original draft preparation): VW. Writing (review and editing): VW, EvR, EGS. Visualization: VW.

Chapter 3

The Privacy Trade-Off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns

Verena M. Wottrich, Eva A. van Reijmersdal, & Edith G. Smit

Conceptualization: VW, EvR, EGS. Methodology: VW, EvR, EGS. Data collection: VW. Analysis: VW. Writing (original draft preparation): VW. Writing (review and editing): VW, EvR, EGS. Visualization: VW.

Chapter 4

The Role of Customization, Brand Trust, and Privacy Concerns in Advergaming

Verena M. Wottrich, Peeter W. J. Verlegh, & Edith G. Smit

Conceptualization: VW, PV, EGS. Methodology: VW, PV, EGS. Data collection: VW. Analysis: VW. Writing (original draft preparation): VW. Writing (review and editing): VW, PV, EGS. Visualization: VW.

Chapter 5
Exploring the Impact of Branded App Intrusiveness on Consumers' App and Brand Perceptions

Verena M. Wottrich, Eva A. van Reijmersdal, & Edith G. Smit

Conceptualization: VW, EvR, EGS. Methodology: VW, EvR, EGS. Data collection: VW. Analysis: VW. Writing (original draft preparation): VW. Writing (review and editing): VW, EvR, EGS. Visualization: VW.

ENGLISH SUMMARY

Today, mobile devices, such as smartphones and tablet PCs, play an important role in our lives. Almost always on and with us, they offer unprecedented, instant, and often free access to information, entertainment, and social interaction at any time and from any place. However, these benefits do not come without risks. By downloading and using mobile applications ("apps"), smartphone and tablet users constantly —and often unwittingly— create quantifiable information online. This information is often collected, stored, used, and auctioned off by third parties, such as app developers, data brokers, analytics companies, and marketers. These data collection and usage practices might impose a threat to app users' privacy, because the gathered information is often used for discriminating between users in buying situations, social sorting, (hidden) manipulation, or fraudulent behaviors, such as identity theft. Currently, app users' influence on the gathering of personal information via mobile apps is limited. As they often cannot selectively grant or decline certain permission requests or simply "opt out" of the tracking, the guiding principle is often "all-or-nothing": accept the information request or do not install the app.

So far, literature on how consumers respond to this situation is scarce and mixed. While some studies show that app users engage in privacy protecting behavior (e.g., uninstalling apps) due to privacy concerns, others demonstrate that users willingly trade their privacy for convenience, functionality, or financial gains. To get more insights into how consumers respond to data collection and usage practices of mobile apps, this dissertation investigated (1) the status quo of privacy protection behavior, (2) the drivers of information disclosure, and (3) the consequences of information disclosure in the privacy-sensitive context of mobile apps.

Conclusions

This dissertation reports the results of four empirical studies, which are based on seven different datasets gathered among more than 4,000 participants. Together, these studies provide five main conclusions about consumers' responses toward data collection and usage practices of mobile apps:

1. **Mobile app users are currently not empowered and motivated enough to tackle the data collection and usage practices of mobile apps.**

App users' current knowledge about the data collection and usage practices of mobile apps is very limited. Moreover, app users are only moderately concerned about their privacy, they do not feel very vulnerable to potential privacy invasions caused by mobile apps, and they only have moderate confidence in their own ability to control the disclosure and subsequent use of personal information in the mobile app context. Currently, app users' are moderately motivated to protect their privacy, however, they barely engage in actual privacy protection behavior in the mobile app context.

2. **Mobile app users are more likely to engage in privacy protection, when they feel vulnerable, concerned, and think that they are able to protect themselves from the data collection and usage practices of apps.**

Mobile app users are more inclined to protect their privacy when they think that privacy invasions caused by mobile apps can, in fact, also affect them. Moreover, they are more likely to protect themselves if they are concerned about their privacy and have confidence in their own ability to control the disclosure and subsequent use of their personal information. Surprisingly, higher levels of knowledge about the data collection and usage practices of apps were not associated with more, but with less, protection motivation and behavior, which is raising doubts concerning the assumption of informed privacy decision-making in the context of mobile apps.

3. **Mobile app users engage in a privacy trade-off when downloading mobile apps in which app value trumps app intrusiveness and privacy concerns.**

Mobile app users tend to trade their privacy for apps that are of value to them. The benefits of an app (i.e., app value) seem to trump the costs (i.e., intrusiveness, privacy concerns) in the privacy trade-off.

4. **In branded gaming apps (i.e., advergames), customization features and brand trust may increase information disclosure and brand attitude, but this influence is strongly conditioned by consumers' privacy concerns.**

Privacy concerns may provide a boundary condition to the effects of customization features and brand trust in branded gaming apps. Privacy concerned players respond more negatively to gaming features than less concerned players.

5. **Branded app intrusiveness has a damaging effect on app and brand perceptions for fictitious apps, but not for real apps.**

Collecting data about consumers via branded mobile apps could have negative consequences for marketers. The more information a fictitious, unknown branded app collects, the more negatively consumers respond to this app in terms of app attitude and app trust. However, intrusiveness does not seem to have an effect on consumers' app and brand perceptions when the app is originating from a real brand.

Conclusion and Practical Implications

This dissertation provides new insights into how consumers respond to data collection and usage practices of apps. It does not only contribute to the scientific literature on privacy decision-making in various ways, but it also provides three important take-aways for policy makers, consumers, and marketers. First of all, this dissertation raises doubts as to whether the current self-regulation principle in general, and the informed consent regulations more specifically, are effective in protecting consumer privacy. Instead of placing too much responsibility for the protection of their privacy on consumers, this dissertation encourages policy makers to better empower consumers and to reassess whether app permission pages in their current form are the right means for educating consumers about the data collection and usage practices of apps. Second, this dissertation shows that mobile app users can do better to protect their privacy in apps. Although it might seem difficult, there are still some steps consumers can take to protect their privacy and this dissertation encourages them to make use of the means that are already available. Mobile app users can, for example, actively look for more information about data collection and usage practices of apps on educational websites, such as www.veiliginternetten.nl, or they could consider downloading alternative apps offering the same service as privacy-invading apps. Third, marketers should be aware that collecting too much data and raising privacy concerns might have negative consequences for their brand. Before employing apps that collect consumer information, marketers should investigate how sensitive their target group is when it comes to privacy. Based on this investigation, they should decide how much consumer information they can collect without running the risk to "scare off" consumers. All in all, this dissertation provides a more nuanced understanding of consumers' responses to data collection and usage practices of mobile apps, which will hopefully shape future inquiries in the area of information privacy and consumer protection.

NEDERLANDSE SAMENVATTING

Mobiele apparaten, zoals smartphones en tablet-pc's, spelen tegenwoordig een belangrijke rol in ons leven. Doordat we ze bijna altijd aan hebben staan en bij ons hebben, bieden ze een tot nu toe ongekende, directe en vaak kosteloze toegang tot informatie, entertainment en sociale interactie op elk moment en vanaf elke plek. Deze voordelen zijn echter niet zonder risico's. Door mobiele applicaties ("apps") te downloaden en gebruiken, produceren gebruikers van smartphones en tablets constant —en vaak onbewust— kwantificeerbare informatie online. Deze informatie wordt regelmatig verzameld, opgeslagen, gebruikt en geveild door derden, zoals app-ontwikkelaars, databrokers, analysebedrijven en marketeers. Deze gegevensverzameling en -gebruikspraktijken kunnen een bedreiging vormen voor de privacy van app-gebruikers, omdat de verzamelde informatie vaak wordt gebruikt voor prijsdiscriminatie, sociale sortering, (verborgen) manipulatie of frauduleus gedrag, zoals identiteitsdiefstal. Momenteel hebben app-gebruikers maar een beperkte invloed op het verzamelen van persoonlijke informatie via mobiele apps. Omdat ze meestal niet selectief bepaalde toestemmingsverzoeken kunnen toestaan of weigeren of aan kunnen geven dat ze niet willen worden getrackt ("opt-out"), is het leidende principe vaak "alles-of-niets": accepteer het informatieverzoek of installeer de app niet.

Tot nu toe is literatuur over hoe consumenten op deze situatie reageren schaars en gemengd. Hoewel sommige onderzoeken aantonen dat app-gebruikers privacybeschermd gedrag vertonen (bijvoorbeeld door apps te verwijderen) vanwege privacyzorgen, laten andere onderzoeken zien dat gebruikers vrijwillig hun privacy ruilen voor gemak, functionaliteit of financiële voordelen. Om meer inzicht te krijgen in hoe consumenten reageren op de gegevensverzameling en -gebruikspraktijken van mobiele apps, heeft dit proefschrift onderzoek gedaan naar (1) de status-quo van privacybeschermingsgedrag, (2) de drijfveren om informatie te delen in mobiele apps en (3) de gevolgen van het delen van informatie in de privacygevoelige context van mobiele apps.

Conclusies

Dit proefschrift rapporteert de resultaten van vier empirische onderzoeken, die gebaseerd zijn op zeven verschillende datasets verzameld onder meer dan 4.000 deelnemers. Samen bieden deze studies vijf hoofdconclusies over de reacties van consumenten op gegevensverzameling en -gebruikspraktijken van mobiele apps:

1. **Mobiele app-gebruikers zijn momenteel niet gemachtigd en gemotiveerd genoeg om de gegevensverzameling en -gebruikspraktijken van mobiele apps aan te pakken.**

De huidige kennis van app-gebruikers over de gegevensverzameling en -gebruikspraktijken van mobiele apps is zeer beperkt. Bovendien maken app-gebruikers zich slechts matig zorgen over hun privacy, voelen ze zich niet erg kwetsbaar voor potentiële privacyschendingen die worden veroorzaakt door mobiele apps, en hebben ze slechts matig vertrouwen in hun eigen vermogen om het delen en het gebruik van hun persoonlijke informatie in de app-context te beheersen. Op dit moment zijn app-gebruikers matig gemotiveerd om hun privacy te beschermen, maar ze tonen nauwelijks privacybeschermingsgedrag.

2. **Mobiele app-gebruikers zullen eerder hun privacy beschermen wanneer ze zich kwetsbaar en bezorgd voelen en denken dat ze zichzelf kunnen beschermen tegen de gegevensverzameling en -gebruikspraktijken van apps.**

Gebruikers van mobiele apps zijn meer geneigd om hun privacy te beschermen wanneer ze denken dat privacyschendingen veroorzaakt door mobiele apps ook daadwerkelijk van invloed kunnen zijn op hen. Bovendien is de kans groter dat ze zichzelf beschermen wanneer ze zich zorgen maken over hun privacy en vertrouwen hebben in hun eigen vermogen om het delen en het gebruik van hun persoonlijke informatie te beheersen. Verrassend was dat hogere niveaus van kennis over de gegevensverzameling en -gebruikspraktijken van apps niet waren geassocieerd met meer, maar met minder, beschermingsmotivatie en -gedrag, wat twijfels opwekt over de aanname van goed geïnformeerde privacybeslissingen in de context van mobiele apps.

3. **Mobiele app-gebruikers gaan een privacyafweging aan bij het downloaden van mobiele apps waarin de waarde van de app belangrijker is dan privacyzorgen en de opdringerigheid van de app.**

Mobiele app-gebruikers hebben de neiging hun privacy in te ruilen voor apps die voor hen van waarde zijn. De voordelen van een app (d.w.z. app-waarde) lijken de kosten te overtreffen (d.w.z. opdringerigheid, privacyzorgen) in de privacyafweging.

4. In gaming-apps die afkomstig zijn van een merk (d.w.z. advergames) kunnen aanpassingsfuncties en merkvertrouwen het delen van informatie en de merkhouding versterken, maar deze invloed wordt sterk bepaald door de privacyzorgen van consumenten.

Privacyzorgen kunnen een randvoorwaarde vormen voor de effecten van aanpassingsfuncties en merkvertrouwen in gaming-apps. Spelers die bezorgd zijn over hun privacy reageren negatiever op gamefuncties dan minder bezorgde spelers.

5. De opdringerigheid van branded apps heeft een schadelijk effect op de percepties van apps en merken voor fictieve apps, maar niet voor echte apps.

Het verzamelen van gegevens over consumenten via mobiele apps die afkomstig zijn van een merk (d.w.z. branded apps) kan negatieve gevolgen hebben voor marketeers. Hoe meer informatie een fictieve app van een onbekend merk verzamelt, hoe negatiever consumenten reageren op deze app in termen van app-attitude en app-vertrouwen. Opdringerigheid lijkt echter geen effect te hebben op de app- en merkperceptie van consumenten wanneer de app afkomstig is van een echt merk.

Conclusie en Aanbevelingen voor de Praktijk

Dit proefschrift biedt nieuwe inzichten in hoe consumenten reageren op gegevensverzameling en -gebruikspraktijken van apps. Het levert niet alleen op verschillende manieren een bijdrage aan de wetenschappelijke literatuur over privacy-besluitvorming, maar biedt ook drie belangrijke aanbevelingen voor beleidsmakers, consumenten en marketeers. Allereerst roept dit proefschrift de vraag op of het huidige zelfreguleringsprincipe in het algemeen en de geïnformeerde toestemmingregelingen in het specifiek, effectief zijn in het beschermen van de privacy van consumenten. In plaats van te veel verantwoordelijkheid te leggen bij de consument voor de bescherming van hun privacy, moedigt dit proefschrift beleidsmakers aan om consumenten beter in staat te stellen hun privacy te beschermen en te heroverwegen of app-machtigingspagina's in hun huidige vorm het juiste middel zijn om consumenten voor te lichten over de gegevensverzameling en -gebruikspraktijken van apps.

Ten tweede laat dit proefschrift zien dat gebruikers van mobiele apps meer zouden kunnen doen om hun privacy in apps te beschermen. Hoewel het misschien moeilijk lijkt, zijn er nog steeds enkele stappen die consumenten kunnen nemen om hun privacy te beschermen en dit proefschrift moedigt hen aan om gebruik te maken van de middelen die al beschikbaar zijn. Gebruikers van mobiele apps kunnen

bijvoorbeeld actief op zoek gaan naar meer informatie over gegevensverzameling en -gebruikspraktijken van apps op educatieve websites, zoals www.veiliginternetten.nl, of ze zouden kunnen overwegen om alternatieve apps te downloaden die dezelfde service bieden als apps die privacy schenden.

Ten derde is het beter als marketeers beseffen dat het verzamelen van te veel gegevens en het opwekken van privacyzorgen negatieve gevolgen kan hebben voor hun merk. Voordat marketeers consumenteninformatie gaan verzamelen met behulp van apps, kunnen ze beter onderzoeken hoe gevoelig hun doelgroep is als het gaat om privacy. Op basis van dit onderzoek moeten zij bepalen hoeveel consumenteninformatie zij kunnen verzamelen zonder het risico te lopen consumenten "af te schrikken". Al met al biedt dit proefschrift een meer genuanceerd inzicht in de reacties van consumenten op de gegevensverzameling en -gebruikspraktijken van apps, wat hopelijk toekomstige onderzoeken op het gebied van informatieprivacy en consumentenbescherming zal inspireren.