Bibliography

[1] M. Abe. Universally Verifiable Mix-Net with Verification Work Independent of the Number of Mix-Servers. *IEICE transactions on fundamentals of electronics, communications and computer sciences*, 83(7):1431–1440, 2000.

[2] K. Aberer. P-Grid: A Self-Organizing Access Structure for P2P Information Systems. *Lecture Notes in Computer Science*, 2172:179–194, 2001.

[3] K. Aberer and Z. Despotovic. Managing trust in a peer-2-peer information system. In H. Paques, L. Liu, and D. Grossman, editors, *Proceedings of the Tenth International Conference on Information and Knowledge Management (CIKM01)*, pages 10 – 317. ACM Press, 2001.

[4] E. Adar. User 4xxxxx9: Anonymizing query logs. In *Workshop on Query Log Analysis at the 16th World Wide Web Conference*, 2007.

[5] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. Hippocratic Databases. In *VLDB*, pages 143–154, 2002.

[6] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. An XPath-based preference language for P3P. In *WWW '03: Proceedings of the 12th international conference on World Wide Web*, pages 629–639, New York, NY, USA, 2003. ACM.

[7] R. Albert, H. Jeong, and A. Barabási. The diameter of the world wide web. *CoRR*, cond-mat/9907038, 1999.

[8] H. Aljifri and D. S. Navarro. Search engines and privacy. *Computers & Security*, 23(5):379–388, 2004.

[9] R. J. Anderson and F. A. P. Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16:474–481, 1998.

[10] F. Anklesaria, M. McCahill, P. Lindner, D. Johnson, D. Torrey, and B. Albert. The Internet Gopher Protocol (a distributed document search and retrieval protocol). RFC 1436 (Informational), March 1993.

[11] F. Arajo. *Position-Based Distributed Hash Tables*. PhD thesis, Department of Informatics, University of Lisbon, May 2006. DI/FCUL TR-06-7.

[12] A. Arasu, J. Cho, H. Garcia-Molina, A. Paepcke, and S. Raghavan. Searching the Web. Technical Report 2000-37, Stanford InfoLab, 2000.

[13] S. Asadi and H. R. Jamali. Shifts in Search Engine Development: A Review of Past, Present and Future Trends in Research on Search Engines. *Webology*, 1(2), December 2004.

[14] P. Ashley, S. Hada, G. Karjoth, and M. Schunter. E-P3P privacy policies and privacy authorization. In *WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*, pages 103–109, New York, NY, USA, 2002. ACM.

[15] R. Atterer and A. Schmidt. Tracking the interaction of users with ajax applications for usability testing. In *CHI*, pages 1347–1350, 2007.

[16] R. Atterer, M. Wnuk, and A. Schmidt. Knowing the user's every move: user activity tracking for website usability evaluation and implicit interaction. In *WWW*, pages 203–212, 2006.

[17] R. Meech P. Laxminarayan B. Kitts, B. LeBlanc. Click Fraud. *Bulletin of the American Society for Information Science and Technology*, 32:14–16, 2005.

[18] M. Backes, B. Pfitzmann, and M. Schunter. A Toolkit for Managing Enterprise Privacy Policies. In *Proceedings of 8th European Symposium on Research in Computer Security (ESORICS)*, volume 2808 of *Lecture Notes in Computer Science*, pages 162–180. Springer, October 2003.

[19] M. Barbaro. A Face Is Exposed for AOL Searcher No. 4417749. The New York Times, available online at http://wa.la/3E1, August 2006.

[20] M. Bartiromo. Inside Google. CNBC, available online at http://wa.la/3E0, December 2009.

[21] S. M. Beitzel, E. C. Jensen, A. Chowdhury, D. Grossman, and O. Frieder. Hourly analysis of a very large topically categorized web

query log. In *SIGIR '04: Proceedings of the 27th annual international ACM SIGIR conference on Research and development in information retrieval*, pages 321–328, New York, NY, USA, 2004. ACM.

[22] O. Berthold, H. Federrath, and S. Köpsell. Web MIXes: A system for anonymous and unobservable Internet access. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 115–129. Springer-Verlag, LNCS 2009, July 2000.

[23] N. Borisov, I. Goldberg, and E. Brewer. Off-the-record communication, or, why not to use PGP. In *WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 77–84, New York, NY, USA, 2004. ACM Press.

[24] M. Boyle. A Shared Vocabulary for Privacy. In *Workshop on Ubicomp Communities: Privacy as Boundary Negotiation. Held as part of the UBICOM'2003 5th International Conference on Ubiquitous Computing*, October 2003.

[25] S. Brin and L. Page. The anatomy of a large-scale hypertextual Web search engine. *Computer Networks and ISDN Systems*, 30(1–7):107–117, 1998.

[26] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4(2), February 1981.

[27] D. Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability. *J. Cryptol.*, 1(1):65–75, 1988.

[28] A. Cooper. A survey of query log privacy-enhancing techniques from a policy perspective. *ACM Trans. Web*, 2(4):1–27, 2008.

[29] K. Coyle. P3P: Pretty Poor Privacy? A Social analysis of the Platform for Privacy Preferences, June 1999 1999.

[30] L. Cranor. P3P: Making Privacy Policies More Useful. *IEEE Security and Privacy*, 01(6):50–55, 2003.

[31] L. Cranor, M. Langheinrich, M. Marchiori, and J. Reagle. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Recommendation, 2005.

[32] L. Cranor and J. Reagle. The Platform for Privacy Preferences. *Communications of the ACM*, 4(2):48 – 55, February 1999. Also in Japanese at IPSJ (Information Processing Society of Japan) Magazine. Vol.40 No.7 July 1999; also as W3C NOTE. 31 July 1998.

[33] G. Danezis, R. Dingledine, D. Hopwood, and N. Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. In *In Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 2–15, 2003.

[34] N. Daswani and M. Stoppelman. The anatomy of Clickbot.A. In *HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets*, pages 11–11, Berkeley, CA, USA, 2007. USENIX Association.

[35] J. D. Day and H. Zimmerman. The OSI Reference Model. *Proceedings of the IEEE*, 71:1334–1340, 1983.

[36] J. DeCew. Privacy. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Fall 2006.

[37] P. Deutsch and A. Emtage. The archie System: An Internet Electronic Directory Service. *Connexions*, 6(2), 1992.

[38] M. Dewey. *Decimal Classification & Relative Index*. Forest Press, 1919.

[39] C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. In R. Dingledine and P. Syverson, editor, *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*. Springer-Verlag, LNCS 2482, April 2002.

[40] T. Dierks and C. Allen. The TLS Protocol Version 1.0. RFC 2246 (Proposed Standard), January 1999. Obsoleted by RFC 4346, updated by RFC 3546.

[41] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346 (Proposed Standard), April 2006. Obsoleted by RFC 5246, updated by RFCs 4366, 4680, 4681.

[42] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[43] B. Edelman, M. Ostrovsky, and M. Schwarz. Internet Advertising and the Generalized Second-Price Auction: Selling Billions of Dollars Worth of Keywords. *The American Economic Review*, 97(1):242–259, March 2007.

[44] D. Eroshenko. Click fraud. The state of the industry. *Pay per Click Analyst*, pages 10 – 19, 2004.

[45] D. Fahrenholtz and W. Lamesdorf. Transactional Security for a Distributed Reputation Management System. In *Proceedings of the Third International Conference on E-Commerce and Web Technologies (EC-Web)*, volume LNCS 2455, pages 214 – 223. Springer, September 2002.

[46] C. Faloutsos. Access Methods for Text. *ACM Comput. Surv.*, 17(1):49–74, 1985.

[47] H. Federrath. Privacy Enhanced Technologies: Methods - Markets - Misuse. In *TrustBus*, pages 1–9, 2005.

[48] W. Feller. *An Introduction to Probability Theory and Its Applications, Volume 1.* Wiley, January 1968.

[49] E. Felten and M. Schneider. Timing attacks on Web privacy. In *ACM Conference on Computer and Communications Security*, pages 25–32, 2000.

[50] M. J. Freedman and R. Morris. Tarzan: A Peer-to-Peer Anonymizing Network Layer. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)*, Washington, D.C., November 2002.

[51] A. O. Freier, P. Karlton, and P. C. Kocher. *SSL Version 3.0*, 12 1995. Internet Draft.

[52] E. Gabber, P. B. Gibbons, D. M. Kristol, Y. Matias, and A. Mayer. On secure and pseudonymous client-relationships with multiple servers. *ACM Trans. Inf. Syst. Secur.*, 2(4):390–415, 1999.

[53] E. Gabber, P. B. Gibbons, Y. Matias, and A. J. Mayer. How to Make Personalized Web Browsing Simple, Secure, and Anonymous. In *Financial Cryptography*, pages 17–32, 1997.

[54] L. Garcés-Erice, K. W. Ross, E. W. Biersack, P. Felber, and G. Urvoy-Keller. Topology-Centric Look-Up Service. In *Networked Group Communication*, pages 58–69, 2003.

[55] R. Gavison. Privacy and the limits of the law. In D. G. Johnson and H. Nissenbaum, editor, *Computers, Ethics, and Social Values*, pages 332–351. Prentice Hall, 1995.

[56] I. Goldberg. Privacy-enhancing Technologies for the Internet, II: Five Years Later. In R. Dingledine and P. Syverson, editors, *Proceedings of Privacy Enhancing Technologies workshop (PET 2002)*. Springer-Verlag, LNCS 2482, April 2002.

[57] I. Goldberg. Privacy-enhancing Technologies for the Internet III: Ten Years Later. In A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, editors, *Digital Privacy: Theory, Technologies, and Practices*. Auerbach Publications (Taylor and Francis Group), 2007.

[58] I. Goldberg, D. Wagner, and E. Brewer. Privacy-enhancing Technologies for the Internet. In *Proc. of 42nd IEEE Spring COMPCON*. IEEE Computer Society Press, February 1997.

[59] D. Goldschlag, M. Reed, and P. Syverson. Onion Routing for Anonymous and Private Internet Connections. *Communications of the ACM*, 42:39–41, 1999.

[60] M. Götz, A. Machanavajjhala, H. Wang, X. Xiao, and J. Gehrke. Privacy in Search Logs. *CoRR*, abs/0904.0682, 2009.

[61] C. G. Günther. An identity-based key-exchange protocol. In *EUROCRYPT '89: Proceedings of the workshop on the theory and application of cryptographic techniques on Advances in cryptology*, pages 29–37, New York, NY, USA, 1990. Springer-Verlag New York, Inc.

[62] Q. Guo and E. Agichtein. Exploring mouse movements for inferring query intent. In *SIGIR*, pages 707–708, 2008.

[63] M. Gupta, P. Judge, and M. Ammar. A reputation system for peer-to-peer networks. In *Proceedings of the 13th international workshop on Network and operating Systems support for digital audio and video (NOSSDAV)*, 2003.

[64] L. Hall. Inventory of privacy-enhancing technologies (PETs). Report DSTI/ICCP/REG(2001)1/FINAL, Working Party on Information Security and Privacy, Organisation for Economic Co-operation and Development, 2002.

[65] H. Hochheiser. The Platform for Privacy Preference as a Social Protocol: An Examination Within the US Policy Context. *ACM Transactions on Internet Technology (TOIT)*, 2(4):276 – 306, November 2002.

[66] D. Howe and H. Nissenbaum. TrackMeNot: Resisting Surveillance in Web Search. In *Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society*, pages 417–436. Oxford University Press, 2009.

[67] L. Introna and A. Pouloudi. Privacy in the Information Age: Stakeholders, Interests and Values. *Journal of Business Ethics*, 22:27 – 38, 1999.

[68] J. Cho and H. Garcia-Molina. The Evolution of the Web and Implications for an Incremental Crawler. Technical Report 1999-22, Stanford InfoLab, 1999.

[69] M. Jakobsson. Flash Mixing. In *In Principles of Distributed Computing - PODC '99. ACM*, pages 83–89. ACM, 1999.

[70] B. J. Jansen. Adversarial information retrieval aspects of sponsored search. *Adversarial Information Retrieval on the Web Workshop at SIGIR 2006*, 2006.

[71] B. J. Jansen and A. Spink. How are we searching the World Wide Web? A comparison of nine search engine transaction logs. *Inf. Process. Manage.*, 42(1):248–263, 2006.

[72] N. F. Johnson and S. Jajodia. Exploring Steganography: Seeing the Unseen. *IEEE Computer*, pages 26–34, February 1998.

[73] A. Jøsang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43(2):618 – 644, March 2007.

[74] D. Karger, E. Lehman, T. Leighton, M. Levine, D. Lewin, and R. Panigrahy. Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web. In *ACM Symposium on Theory of Computing*, pages 654–663, May 1997.

[75] G. Karjoth, M. Schunter, and M. Waidner. Platform for Enterprise Privacy Practices: Privacy-Enabled Management of Customer Data. In *Privacy Enhancing Technologies*, pages 69–84, 2002.

[76] A. Korolova, K. Kenthapadi, N. Mishra, and A. Ntoulas. Releasing Search Queries and Clicks Privately. In *18th International World Wide Web Conference (WWW2009)*, April 2009.

[77] M. Koster. ALIWEB - Archie-like Indexing in the WEB. *Computer Networks and ISDN Systems*, 27(2):175–182, 1994.

[78] M. Langheinrich, L. Cranor, and M. Marchiori. APPEL: A P3P Preference Exchange Language. W3C Working Draft, April 2002.

[79] M. Leino-Kilpi. Privacy: a review of the literature. *International journal of nursing studies*, 38(6):663–71, 2002. Affiliaton: University of Turku, Finland. heleno.leino-kilpi@utu.fi.

[80] B. Levine and C. Shields. Hordes: A Multicast Based Protocol for Anonymity. *Journal of Computer Security*, 10(3):213–240, 2002.

[81] B. N. Levine, M. Reiter, C. Wang, and M. Wright. Timing Attacks in Low-Latency Mix Systems. In *Proc. Financial Cryptography (FC) (LNCS 3110)*, pages 251—265, February 2004.

[82] L. Macaulay. Privacy Enhancing Technologies - State of the Art Review Version 1. Technical Report TRS-2002-001, Computation Department, University of Manchester Institute of Science and Technology, Manchester, UK, 2002.

[83] E. P. Markatos. On caching search engine query results. *Computer Communications*, 24(2):137–143, 2001.

[84] C.P. McParland and R. Connolly. Empirical Research on Technology-Related Privacy Concerns: A Review and Critical Assessment. In *16th European Conference on Information Systems (Golden W, Acton T, Conboy K, van der Heijden H, Tuunainen VK eds.)*, pages 658 – 668, Galway, Ireland, 2008.

[85] E. Nakashima. AOL Search Queries Open Window Onto Users' Worlds. Washington Post, available online at http://wa.la/3DZ, August 2006.

[86] G. Ng-Kruelle, J. Felix Hampe, P. A. Swatman, and D. S. Rebne. The Price of Convenience: Privacy and Mobile Commerce. *Quarterly Journal of Electronic Commerce*, 3(3):273–385, 2002.

[87] O. Berthold and H. Federrath and M. Köhntopp. Project "anonymity and unobservability in the Internet". In *CFP '00: Proceedings of the*

tenth conference on Computers, freedom and privacy, pages 57–65, New York, NY, USA, 2000. ACM.

[88] R. Olbrich and C. D. Schultz. Search Engine Marketing and Click Fraud, 2008.

[89] M. S. Olivier. A Layered Architecture for Privacy-enhancing Technologies. In Jan H P Eloff, Hein S Venter, Les Labuschagne, and Mariki M Eloff, editors, *Proceedings of the Third Annual Information Security South Africa Conference (ISSA2003)*, pages 113–126, Sandton, South Africa, July 2003.

[90] M. S. Olivier. Flocks: Distributed Proxies for Browsing Privacy. In Gary Marsden, Paula Kotzé, and Ayodele Adesina-Ojo, editors, *Proceedings of SAICSIT 2004 — fulfilling the promise of ICT*, pages 79–88, Stellenbosch, South Africa, October 2004.

[91] M. S. Olivier. Privacy under Conditions of Concurrent Interaction with Multiple Parties. In de Capitani di Vimercati, Sabrina and Indrakshi Ray and Indrajit Ray, editor, *Data and Applications Security XVII — Status and Prospects*, pages 105–118. Kluwer, 2004.

[92] L. Øverlier and P. Syverson. Locating Hidden Servers. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, pages 100–114. IEEE Computer Society, May 2006.

[93] G. Pass, A. Chowdhury, and C. Torgeson. A picture of search. In *Infoscale*, page 1, 2006.

[94] A. Pfitzmann and M. Koehntopp. Anonymity, unobservability, and pseudonymity – a proposal for terminology. In *Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability*, volume 2009/2001 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2001.

[95] A. Pfitzmann and M. Waidner. Networks Without User Observability. *Computers and Security*, 2(6):158–166, 1987.

[96] B. Pinkerton. Finding What People Want: Experiences with the WebCrawler. In Anonymous, editor, *Proceedings of the 2nd International World Wide Web*, volume 18(6) of *Online & CDROM review: the international journal of*, Medford, NJ, USA, 1994. Learned Information.

[97] J. Postel and J. Reynolds. File Transfer Protocol. RFC 959 (Standard), October 1985. Updated by RFCs 2228, 2640, 2773, 3659.

[98] J. Postel and J.K. Reynolds. Telnet Protocol Specification. RFC 854 (Standard), May 1983. Updated by RFC 5198.

[99] M. G. Reed, P. F. Syverson, and D. M. Goldschlag. Anonymous Connections and Onion Routing. *IEEE Journal on Selected Areas in Communications*, 16(4):482–494, May 1998.

[100] M. K. Reiter and A. D. Rubin. Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[101] P. Resnick and R. Zeckhauser. Trust Among Strangers in Electronic Transactions: Empirical Analysis of eBay's Reputation System. *Advances in Applied Microeconomics*, 11, 2002.

[102] P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood. The Value of Reputation on eBay: A Controlled Experiment, 2003.

[103] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 26(1):96–99, 1983.

[104] M. Rotenberg. Fair information practices and the architecture of privacy. *Stanford Technology Law Review*, 1, 2001.

[105] A. Rowstron and P. Druschel. Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems. In *IFIP/ACM International Conference on Distributed Systems Platforms (Middleware)*, pages 329–350, November 2001.

[106] A. Rutherford, R. A Botha, and M. S Olivier. Towards a Hippocratic Log File Architecture. In Gary Marsden and Paula Kotzé and Ayodele Adesina-Ojo, editor, *Proceedings of SAICSIT 2004 — fulfilling the promise of ICT*, pages 186–193, Stellenbosch, South Africa, October 2004.

[107] A. Rutherford, R. A Botha, and M. S Olivier. Towards Hippocratic Log files. In *Proceedings of the Fourth Annual Information Security South Africa Conference (ISSA2004)*, Midrand, South Africa, June/July 2004. Published electronically.

[108] S. Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1996.

[109] V. Seničar, B. Jerman-Blažič, and T. Klobučar. Privacy-enhancing technologies: approaches and development. *Comput. Stand. Interfaces*, 25(2):147–158, 2003.

[110] C. Shields. Responder Anonymity and Anonymous Peer-to-Peer File Sharing. In *ICNP '01: Proceedings of the Ninth International Conference on Network Protocols*, page 272, Washington, DC, USA, 2001. IEEE Computer Society.

[111] D. J. Solove. Conceptualizing Privacy. *California Law Review*, 90:1087, 2002.

[112] D. J. Solove. "I've Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*, 44:745, 2007.

[113] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications. In *Proceedings of the ACM SIGCOMM '01 Conference*, San Diego, California, August 2001.

[114] R. Thibadeau. A Critique of P3P: Privacy on the Web, August 2000.

[115] J. J. Thomson. The Right to Privacy. *Philosophy and Public Affairs*, 4(4):295–314, 1975.

[116] V. Bellotti and A. Sellen. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93)*, pages 77–92. Kluwer, 1993.

[117] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A Digital Watermark. In *ICIP (2)*, pages 86–90, 1994.

[118] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In *In Proceedings of the Second UNIX Workshop on Electronic Commerce*, pages 29–40. USENIX Association, 1996.

[119] S. Warren and L. Brandeis. The Right to Privacy. *Harward Law Review*, 4:193–220, 1890.

[120] A. F. Westin. *Privacy and Freedom*. Atheneum, New York, 1967.

[121] C. K. Wilbur and Y. Zhu. Click Fraud. *Marketing Science*, 28(2):293–308, 2009.

[122] J. Wright, S. Stepney, J. A. Clark, and J. L. Jacob. Designing Anonymity - A Formal Basis for Identity Hiding. Internal Yellow Report, York University, York, UK, December 2004.

[123] M. Wright, M. Adler, B. N. Levine, and C. Shields. Defending Anonymous Communication Against Passive Logging Attacks. In *Proc. IEEE Symposium on Security and Privacy (Oakland)*, pages 28–41, May 2003.

[124] M. K. Wright, M. Adler, B. N. Levine, and C. Shields. An Analysis of the Degradation of Anonymous Protocols. In *Proc. ISOC Symposium Network and Distributed System Security (NDSS)*, pages 38–50, February 2002.

[125] M. K. Wright, M. Adler, B. N. Levine, and C. Shields. The Predecessor Attack: An analysis of a threat to anonymous communications systems. *ACM Trans. Inf. Syst. Secur.*, 7(4):489–522, 2004.

[126] G. Zacharia and P. Maes. Trust management through reputation mechanisms. *Applied Artificial Intelligence*, 14(19):881 – 907, 2000.

[127] B. Zhao, J. Kubiatowicz, and A. D. Joseph. Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing. Technical Report UCB/CSD-01-1141, University of California Berkeley, Electrical Engineering and Computer Science Department, April 2001.

[128] Y. Zhu, L. Xiong, and C. Verdery. Anonymizing user profiles for personalized web search. In *WWW*, pages 1225–1226, 2010.