David R. Choffnes

Northeastern University
Khoury College of Computer Sciences
Boston, Massachusetts 02115
United States of America

choffnes@ccs.neu.edu
https://david.choffnes.com

EDUCATION

06/2010 **Doctor of Philosophy** in Computer Science
Northwestern University, Evanston, Illinois
Thesis: *Service-Level Network Event Detection from Edge Systems*
Advisor: Fabián E. Bustamante

12/2006 **Master of Science** in Computer Science
Northwestern University, Evanston, Illinois
Advisor: Fabián E. Bustamante

05/2002 **Bachelor of Arts** in Physics and French, awarded *magna cum laude*
Amherst College, Amherst, Massachusetts

PROFESSIONAL EXPERIENCE

7/2019 – Pres. **Associate Professor**
Khoury College of Computer Sciences, Northeastern University, Boston, Mass.

7/2021 – Pres. **Executive Director, Cybersecurity and Privacy Institute**
Cybersecurity and Privacy Institute, Northeastern University, Boston, Mass.

10/2020 – 6/2021 **Security Architect**
Akamai Technologies, Cambridge, Mass.

9/2013 – 6/2019 **Assistant Professor**
College of Computer and Information Science, Northeastern University, Boston, Mass.

6/2010 – 8/2013 **Post-Doctoral Scholar (NSF/CRA Computing Innovations Fellow)**
University of Washington, Department of CSE, Seattle, Washington
Mentors: Tom Anderson and Arvind Krishnamurthy

6/2009 – 9/2009 **Research Intern**
AT&T Labs – Research, Florham Park, New Jersey

6/2007 – 9/2007 **Research Intern**
IBM T. J. Watson Research Lab, Hawthorne, New York

8/2002 – 7/2004 **Editor and author**
Deitel & Associates, Maynard, Massachusetts

HONORS AND AWARDS

2023 Best Paper (IMC 2023)
2023 Runner-up Best Student Paper (PETS 2023)
2021 ACM Senior Member
2019 Community Contribution Award (IMC 2019)
2018 DNSSEC paper (USENIX Security 2018) selected for the IRTF's Applied Networking Research Prize
2018 NSF CAREER Award
2018 Best of CCR Award for FreeBasics paper (presented at SIGCOMM 2018)
2018 Cisco Network Security Best Paper Award (NDSS 2018)
2018 QUIC paper (IMC 2017) selected for the IRTF's Applied Networking Research Prize
2017 IEEE Cybersecurity Award for Innovation
2017 USENIX Security Distinguished Paper Award
2010-2012 NSF/CRA Computing Innovations Fellowship
2010 EECS Outstanding Dissertation Award, Northwestern University

SELECTED PRESS COVERAGE

4/2023 I was quoted by Reuters in a story about Tesla vehicle cameras capturing sensitive footage of unwitting bystanders.
8/2022 Our work on identifying biases in automatic transcription services was covered by Consumer Reports.
5/2021 Our work on blocking unnecessary connections from IoT devices (`https://moniotrlab.ccis.neu.edu/pets21/`) was covered by Consumer Reports.
2/2020 Our work on systematically revealing misactivations of smart speakers and the implications of what they record (`https://moniotrlab.ccis.neu.edu/smart-speakers-study/`) appeared in the New York Times, USA Today, Vox, Fortune, and others.
9/2019 Our work on revealing users' sensitive information exposed by IoT devices was covered by The Financial Times, VICE, and others.
9/2018 Bloomberg covered our analysis of ISP throttling behavior before and after the new FCC order that permits it. Also covered by the Boston Globe, Gizmodo, Geekwire, the Verge, and other international publications such as Le Monde and Figaro.
7/2018 Coverage of our work (published at PETS 2018) on apps that spy on you. Covered by more than 200 news outlets, including Gizmodo, USA Today, WIRED, the Recode podcast (interviewed by Kara Swisher), Fox 25 Boston, Denver 7 News, The Register, and other publications worldwide. We responsibly disclosed to Google and others, they took action to mitigate this privacy risk.
1/2018 Our Wehe app for detecting net neutrality violations received substantial international attention, in large part due to Apple rejecting our app and then later reversing its decision based on public backlash. Our work was subsequently covered by dozens of news outlets, and a piece about net neutrality featuring this work appeared on VICE News' TV show.

11/2017 Article about my team's net neutrality research appeared on the PBS Newshour website, CBS News website, among others. I was also interviewed by The Takeaway (NY Times / PRI production) on a segment that aired nationally on November 21st.

11/2015 The ReCon project, which reveals and controls how personal information is leaked from mobile devices, was covered by the Boston Globe, Northeastern News, Christian Science Monitor, New Scientist, Science Codex, NBC News, MSN News, El Mundo, Le Matin, among others.

TEXTBOOKS

[1] Harvey Deitel, Paul Deitel, David Choffnes, and Chriti Kelsey. *Simply C++ : An Application-Driven Tutorial Approach*. Prentice Hall, 2005.

[2] Harvey Deitel, Paul Deitel, and David Choffnes. *Operating Systems*. Prentice Hall, Third edition, 2004.

REFEREED JOURNAL AND MAGAZINE PUBLICATIONS

[1] Michelle N. Meyer, John Basl, David Choffnes, Christo Wilson, and David M. J. Lazer. Enhancing the ethics of user-sourced online data collection and sharing. *Nature Computational Science*, 3(8), 2023.

[2] Arash Molavi Kakhki, Samuel Jero, David Choffnes, Alan Mislove, and Cristina Nita-Rotaru. Taking a long look at QUIC: An approach for rigorous evaluation of rapidly evolving transport protocols. *Communications of the ACM*, 62(7), 2019.

[3] Fan Zhou, Kaushik Chowdhury, and David Choffnes. Janus: A multi-TCP framework for application-aware optimization in mobile networks. *IEEE IEEE Transactions on Mobile Computing*, 2019.

[4] Liang Zhang, David Choffnes, Tudor Dumitraş, Dave Levin, Alan Mislove, Aaron Schulman, and Christo Wilson. Analysis of ssl certificate reissues and revocations in the wake of heartbleed. *Communications of the ACM*, 61(3), 2018.

[5] Quirin Scheitle, Taejoong Chung, Jens Hiller, Oliver Gasser, Johannes Naab, Roland van Rijswijk-Deij, Oliver Hohlfeld, Ralph Holz, Dave Choffnes, Alan Mislove, and Georg Carle. A First Look at Certification Authority Authorization (CAA). *ACM SIGCOMM Computer Communications Review (CCR)*, April 2018.

[6] Jing'an Xue, David Choffnes, and Jilong Wang. CDNs meet CN: An empirical study of CDN deployments in China. In *IEEE Access*, volume 5, December 2017.

[7] Rijurekha Sen, Sohaib Ahmad, Amreesh Phokeer, Zaid Ahmed Farooq, Ihsan Ayyub Qazi, David Choffnes, and Krishna P. Gummadi. Inside the walled garden: Deconstructing facebook's free basics program. *SIGCOMM CCR*, 47(5), 2017.

[8] Ashwin Rao, Arash Molavi Kakhki, Abbas Razaghpanah, Anke Li, David Choffnes, Arnaud Legout, Alan Mislove, and Phillipa Gill. Meddle: Enabling transparency and control for mobile internet traffic. *Journal of Technology Science (JoTS)*, October 2015.

[9] Arnau Gavalda, David Choffnes, John Otto, Mario Sanchez, Fabian Bustamante, Luis A. N. Amaral, Jordi Duch, and Roger Guimera. Impact of heterogeneity and socio-economic factors on massive decentralized sharing ecosystems. *Proceedings of the National Academy of Sciences (PNAS)*, October 2014.

[10] Mario A. Sánchez, John S. Otto, Zachary S. Bischof, David R. Choffnes, Fabian E. Bustamante, Balachander Krishnamurthy, and Walter Willinger. A measurement experimentation platform at the internet's edge. *IEEE/ACM Trans. Netw.*, 23(6):1944–1958, 2015.

[11] Kai Chen, David R. Choffnes, Rahul Potharaju, Yan Chen, Fabian E. Bustamante, Dan Pei, and Yao Zhao. Where the sidewalk ends: Extending the internet AS graph using traceroutes from P2P users. *IEEE Trans. Computers*, 63(4):1021–1036, 2014.

[12] Ao-Jan Su, David R. Choffnes, Aleksandar Kuzmanovic, and Fabián E. Bustamante. Drafting behind akamai: inferring network conditions based on CDN redirections. *IEEE/ACM Trans. Netw.*, 17(6):1752–1765, 2009.

[13] David R. Choffnes, Mark Astley, and Michael J. Ward. Migration policies for multi-core fair-share scheduling. *Operating Systems Review*, 42(1):92–93, 2008.

REFEREED CONFERENCE PUBLICATIONS

[1] Daniel J. Dubois, Nicole Holliday, Kaveh Waddell, and David Choffnes. Fair or fare? understanding automated transcription error bias in social media and videoconferencing platforms. In *Proc. of ICWSM*, 2024.

[2] Vadim Safronov, Anna Maria Mandalari, Daniel J. Dubois, David Choffnes, and Hamed Haddadi. Sunblock: Cloudless protection for iot systems. In *Passive and Active Measurement (PAM) Conference*, 2024.

[3] Aniketh Girish, Tianrui Hu, Vijay Prakash, Daniel J. Dubois, Srdjan Matic, Danny Yuxing Huang, Serge Egelman, Joel Reardon, Juan Tapiador, David Choffnes, and Narseo Vallina-Rodriguez. In the room where it happens: Characterizing local communication and threats in smart homes. In *Proc. of IMC*, 2023.

[4] Tianrui Hu, Daniel J. Dubois, and David Choffnes. Behaviot: Measuring smart home iot behavior using network-inferred behavior models. In *Proc. of IMC*, 2023.

[5] Hongying Dong, Hao Shu, Vijay Prakash, Yizhe Zhang, Muhammad Talha Paracha, David Choffnes, Santiago Torres-Arias, Danny Yuxing Huang,

and Yixin Sun. Behind the scenes: Uncovering tls and server certificate practice of iot device vendors in the wild. In *Proc. of IMC*, 2023.

[6] Zeinab Shmeis, Muhammad Abdullah, Pavlos Nikolopoulos, Katerina Argyraki, David Choffnes, and Phillipa Gill. Localizing traffic differentiation. In *Proc. of IMC*, 2023.

[7] Umar Iqbal, Pouneh Nikkhah Bahrami, Rahmadi Trimananda, Hao Cui, Alexander Gamero-Garrido, Daniel J. Dubois, David Choffnes, Athina Markopoulou, Franziska Roesner, and Zubair Shafiq. Tracking, profiling, and ad targeting in the alexa echo smart speaker ecosystem. In *Proc. of IMC*, 2023.

[8] Anna Maria Mandalari, Hamed Haddadi, Daniel J. Dubois, and David Choffnes. Protected or porous: A comparative analysis of threat detection capability of iot safeguards. In *Proc. of IEEE S&P*, 2023.

[9] Monica Kowalczyk, Johanna T. Gunawan, David Choffnes, Daniel J Dubois, Woodrow Hartzog, and Christo Wilson. Understanding dark patterns in home iot devices. In *Proc. of CHI*, 2023.

[10] Amogh Pradeep, Alvaro Feal, Julien Gamba, Ashwin Rao, Martina Lindorfer, Narseo Vallina-Rodriguez, and David Choffnes. Not your average app: A large-scale privacy analysis of android browsers. In *Proc. of PETS*, 2023.

[11] Amogh Pradeep, Muhammad Talha Paracha, Protick Bhowmick, Ali Davanian, Abbas Razaghpanah, Taejoong Chung, Martina Lindorfer, Narseo Vallina-Rodriguez, Dave Levin, and David Choffnes. A comparative analysis of certificate pinning in Android & iOS. In *Proc. of IMC*, 2022.

[12] Kevin Vermeulen, Ege Gurmericliler, Italo Cunha, David Choffnes, and Ethan Katz-Bassett. Internet scale reverse traceroute. In *Proc. of IMC*, 2022.

[13] Kentrell Owens, Johanna Gunawan, David Choffnes, Pardis Emami-Naeini, Tadayoshi Kohno, and Franziska Roesner. Exploring deceptive design patterns in voice interfaces. In *Proc. of EuroUSEC*, 2022.

[14] Narmeen Shafqat, Daniel J. Dubois, David Choffnes, Aaron Schulman, Dinesh Bharadia, and Aanjhan Ranganathan. ZLeaks: Passive inference attacks on zigbee based smart homes. In *Proc. of ANCS*, 2022.

[15] Amogh Pradeep, Hira Javaid, Ryan Williams, Antoine Rault, David Choffnes, Stevens Le Blond, and Bryan Ford. Moby: A blackout-resistant anonymity network for mobile devices. In *Proc. of PETS*, 2022.

[16] Muhammad Talha Paracha, Daniel Dubois, Narseo Vallina-Rodriguez, and David Choffnes. IoTLS: Understanding TLS usage in consumer IoT devices. In *Proc. of IMC*, 2021.

[17] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. A comparative study of dark patterns across mobile and web modalities. In *Proc. of CSCW*, 2021.

[18] Xiao Zhang, Tanmoy Sen, Zheyuan Zhang, Tim April, Balakrishnan Chandrasekaran, David Choffnes, Bruce M. Maggs, Haiying Shen, Ramesh K. Sitaraman, and Xiaowei Yang. AnyOpt: Predicting and optimizing IP anycast performance. In *Proc. of ACM SIGCOMM*, 2021.

[19] Ruimin Sun, Alejandro Mera, Long Lu, and David Choffnes. SoK: Attacks on industrial control logic and formal verification-based defenses. In *Proc. of IEEE European Security and Privacy*, 2021.

[20] Anna Maria Mandalari, Daniel J. Dubois, Roman Kolcun, Muhammad Talha Paracha, Hamed Haddadi, and David Choffnes. Blocking without Breaking: Identification and Mitigation of Non-Essential IoT Traffic. In *Proc. of the Privacy Enhancing Technologies Symposium (PETS)*, 2021.

[21] Said Jawad Saidi, Anna Maria Mandalari, Roman Kolcun, Hamed Haddadi, Daniel J. Dubois, David Choffnes, Georgios Smaragdakis, and Anja Feldmann. A Haystack Full of Needles: Scalable Detection of IoT Devices in the Wild. In *Proc. of the Internet Measurement Conference (IMC)*, 2020.

[22] Daniel Dubois, Roman Kolcun, Anna Mandalari, Muhammad Talha Paracha, David Choffnes, and Hamed Haddadi. When speakers are all ears: Characterizing misactivations of IoT smart speakers. In *Proc. of PETS*, 2020.

[23] Muhammad Talha Paracha, Balakrishnan Chandrasekara, David Choffnes, and Dave Levin. A deeper look at web content availability and consistency over HTTP/S. In *Network Traffic Measurement and Analysis Conference*, 2020.

[24] Thijs van Ede, Riccardo Bortolameotti, Andrea Continella, Jingjing Ren, Daniel J. Dubois, Martina Lindorfer, David Choffnes, Maarten van Steen, and Andreas Peter. FlowPrint: Semi-supervised mobile-app fingerprinting on encrypted network traffic. In *Proc. of NDSS*, 2020.

[25] Jingjing Ren, Daniel J. Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. *Proc. of IMC*, 2019.

[26] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, Roland van Rijswijk-Deij, John P. Rula, and Nick Sullivan. Rpki is coming of age: A longitudinal study of rpki deployment and invalid route origins. *Proc. of IMC*, 2019.

[27] Fangfan Li, Arian Niaki, David Choffnes, Phillipa Gill, and Alan Mislove. A large-scale analysis of deployed traffic differentiation practices. In *Proc. of ACM SIGCOMM*, 2019.

[28] Taejoong Chung, Jay Lok, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, John P. Rula, Nick Sullivan, and Christo Wilson. Is the web ready for OCSP Must Staple? In *Proc. of IMC*, 2018.

[29] Elleen Pan, Jingjing Ren, Martina Lindorfer, Christo Wilson, and David Choffnes. Panoptispy: Characterizing audio and video exfiltration from Android applications. In *Proc. of PETS*, 2018.

[30] John P. Rula, Fabian E. Bustamante, James Newman, Arash Molavi Khaki, and David Choffnes. Mile high WiFi: A first look at in-flight Internet connectivity. In *Proc. of WWW*, 2018.

[31] Jingjing Ren, Martina Lindorfer, Daniel Dubois, Ashwin Rao, David R. Choffnes, and Narseo Vallina-Rodriguez. Bug fixes, improvements, ... and privacy leaks - a longitudinal study of PII leaks across Android app versions. In *Proc. of NDSS*, 2018.

[32] Samuel Jero, Endadul Hoque, David Choffnes, Alan Mislove, and Cristina Nita-Rotaru. Automated attack discovery in TCP congestion control using a model-guided approach. In *Proc. of NDSS*, 2018.

[33] Arash Molavi Kakhki, Samuel Jero, David Choffnes, Alan Mislove, and Cristina Nita-Rotaru. Taking a long look at QUIC: An approach for rigorous evaluation of rapidly evolving transport protocols. In *Proc. of IMC*, 2017.

[34] Fangfan Li, Abbas Razaghpanah, Arash Molavi Kakhki, Arian Akhavan Niaki, David Choffnes, Phillipa Gill, and Alan Mislove. lib·erate, (n): A library for exposing (traffic-classification) rules and avoiding them efficiently. In *Proc. of IMC*, 2017.

[35] Taejoong Chung, Roland Rijswijk-Deij, David Choffnes, Alan Mislove, Christo Wilson, Dave Levin, and Bruce M. Maggs. Understanding the role of registrars in DNSSEC deployment. In *Proc. of IMC*, 2017.

[36] Brian Goodchild, Yi-Ching Chiu, Haonan Lu, Rob Hansen, Matt Calder, David Choffnes, Wyatt Lloyd, Matthew Luckie, and Ethan Katz-Bassett. The record route option is an option! In *Proc. of IMC*, 2017.

[37] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. A longitudinal, end-to-end view of the DNSSEC ecosystem. In *Proc. of USENIX Security*, 2017.

[38] James Larisch, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. CRLite: a scalable system for pushing all TLS revocations to browsers. In *Proc. of IEEE S&P*, 2017.

[39] Stevens Le Blond, Cédric Gilbert, Utkarsh Upadhyay, Manuel Gomez Rodriguez, and David Choffnes. A broad view of the ecosystem of socially engineered exploit documents. In *Proc. of NDSS*, 2017.

[40] Fangfan Li, Arash Molavi Kakhki, David Choffnes, Phillipa Gill, and Alan Mislove. Classifiers unclassified: An efficient approach to revealing ip-traffic classification rules. In *Proc. of IMC*, 2016.

[41] Christophe Leung, Jingjing Ren, David Choffnes, and Christo Wilson. Should you use the app for that? comparing the privacy implications of web- and app-based online services. In *Proc. of IMC*, 2016.

[42] Taejoong Chung, David Choffnes, and Alan Mislove. Tunneling for transparency: A large-scale analysis of end-to-end violations in the internet. In *Proc. of IMC*, 2016.

[43] Rijurekha Sen, Hasnain Ali Pirzada, Amreesh Phokeer, Zaid Ahmed Farooq, Satadal Sengupta, David Choffnes, and Krishna P. Gummadi. Inspecting the free bridge across the digital divide: Assessing the quality of facebook's free basics service. In *Proc. of IMC*, 2016.

[44] Taejoong Chung, Yabing Liu, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, and Christo Wilson. Measuring and applying invalid SSL certificates: The silent majority. In *Proc. of IMC*, 2016.

[45] Frank Cangialosi, Taejoong Chung, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. Measurement and analysis of private key sharing in the ssl ecosystem. In *Proc. of CCS*, 2016.

[46] Jingjing Ren, Ashwin Rao, Martina Lindorfer, Arnaud Legout, and David R. Choffnes. ReCon: Revealing and controlling privacy leaks in mobile network traffic. In *Proc. of ACM MobiSys*, 2016.

[47] Arash Molavi Kakhki, Abbas Razaghpanah, Anke Li, Hyungjoon Koo, Rajesh Golani, David R. Choffnes, Phillipa Gill, and Alan Mislove. Identifying traffic differentiation in mobile networks. In *Proc. of IMC*, 2015.

[48] Yabing Liu, Will Tome, Liang Zhang, David R. Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Aaron Schulman, and Christo Wilson. An end-to-end measurement of certificate revocation in the web's PKI. In *Proc. of IMC*, 2015.

[49] Ruwaifa Anwar, Haseeb Niaz, David R. Choffnes, Ítalo S. Cunha, Phillipa Gill, and Ethan Katz-Bassett. Investigating interdomain routing policies in the wild. In *Proc. of IMC*, 2015.

[50] Stevens Le Blond, David R. Choffnes, William Caldwell, Peter Druschel, and Nicholas Merritt. Herd: A scalable, traffic analysis resistant anonymity network for voip systems. In *Proc. of ACM SIGCOMM*, 2015.

[51] Ashkan Nikravesh, Hongyi Yao, Shichang Xu, David R. Choffnes, and Zhuoqing Morley Mao. Mobilyzer: An open platform for controllable mobile network measurements. In *Proc. of ACM MobiSys*, 2015.

[52] Xing Xu, Yurong Jiang, Tobias Flach, Ethan Katz-Bassett, David R. Choffnes, and Ramesh Govindan. Investigating transparent web proxies in cellular networks. In *Passive and Active Measurement (PAM) Conference*, 2015.

[53] Liang Zhang, David R. Choffnes, Dave Levin, Tudor Dumitras, Alan Mislove, Aaron Schulman, and Christo Wilson. Analysis of SSL certificate reissues and revocations in the wake of heartbleed. In *Proc. of IMC*, 2014.

[54] Kyriakos Zarifis, Tobias Flach, Srikanth Nori, David R. Choffnes, Ramesh Govindan, Ethan Katz-Bassett, Zhuoqing Morley Mao, and Matt Welsh. Diagnosing path inflation of mobile client traffic. In *Passive and Active Measurement (PAM) Conference*, 2014.

[55] Ashkan Nikravesh, David R. Choffnes, Ethan Katz-Bassett, Zhuoqing Morley Mao, and Matt Welsh. Mobile network performance from user devices: A longitudinal, multidimensional analysis. In *Passive and Active Measurement (PAM) Conference*, 2014.

[56] Umar Javed, Ítalo Cunha, David R. Choffnes, Ethan Katz-Bassett, Thomas E. Anderson, and Arvind Krishnamurthy. Poiroot: investigating the root cause of interdomain path changes. In *Proc. of ACM SIGCOMM*, pages 183–194, 2013.

[57] Stevens Le Blond, David R. Choffnes, Wenxuan Zhou, Peter Druschel, Hitesh Ballani, and Paul Francis. Towards efficient traffic-analysis resistant anonymity networks. In *Proc. of ACM SIGCOMM*, pages 303–314, 2013.

[58] Mario A. Sánchez, John S. Otto, Zachary S. Bischof, David R. Choffnes, Fabián E. Bustamante, Balachander Krishnamurthy, and Walter Willinger. Dasu: Pushing experiments to the internet's edge. In *definition*, pages 487–499, 2013.

[59] Ethan Katz-Bassett, Colin Scott, David R. Choffnes, Ítalo Cunha, Vytautas Valancius, Nick Feamster, Harsha V. Madhyastha, Thomas E. Anderson, and Arvind Krishnamurthy. LIFEGUARD: practical repair of persistent route failures. In *Proc. of ACM SIGCOMM*, pages 395–406, 2012.

[60] John S. Otto, Mario A. Sánchez, David R. Choffnes, Fabián E. Bustamante, and Georgos Siganos. On blind mice and the elephant: understanding the network impact of a large distributed system. In *Proc. of ACM SIGCOMM*, pages 110–121, 2011.

[61] David R. Choffnes, Fabián E. Bustamante, and Zihui Ge. Crowdsourcing service-level network event monitoring. In *Proc. of ACM SIGCOMM*, pages 387–398, 2010.

[62] Kai Chen, David R. Choffnes, Rahul Potharaju, Yan Chen, Fabian E. Bustamante, Dan Pei, and Yao Zhao. Where the sidewalk ends: extending

the internet as graph using traceroutes from P2P users. In *Proc. of ACM CoNEXT*, pages 217–228, 2009.

[63] David R. Choffnes and Fabian E. Bustamante. On the effectiveness of measurement reuse for performance-based detouring. In *Proc. of IEEE INFOCOM*, pages 693–701, 2009.

[64] David R. Choffnes and Fabián E. Bustamante. Taming the torrent: a practical approach to reducing cross-isp traffic in peer-to-peer systems. In *Proc. of ACM SIGCOMM*, pages 363–374, 2008.

[65] Ao-Jan Su, David R. Choffnes, Fabián E. Bustamante, and Aleksandar Kuzmanovic. Relative network positioning via CDN redirections. In *Proc. of ICDCS*, pages 377–386, 2008.

[66] Ao-Jan Su, David R. Choffnes, Aleksandar Kuzmanovic, and Fabián E. Bustamante. Drafting behind akamai (travelocity-based detouring). In *Proc. of ACM SIGCOMM*, pages 435–446, 2006.

REFEREED WORKSHOP PUBLICATIONS

[1] David Choffnes. A case for personal virtual networks. In *Proc. of HotNets*, 2016.

[2] Fan Zhou, Kaushik Chowdhury, and David Choffnes. Janus: Network and application-aware multi-TCP optimization engine. In *INFOCOM Poster Session*, 2016.

[3] Arash Molavi Kakhki, Fangfan Li David R. Choffnes, Alan Mislove, and Ethan Katz-Bassett. BingeOn under the microscope: Understanding T-Mobile's zero-rating implementation. In *SIGCOMM Internet-QoE Workshop*, 2016.

[4] John P. Rula, Fabian E. Bustamante, and David R. Choffnes. When IPs fly: A case for redefining airline communication. In *Proc. of HotMobile*, 2016.

[5] Ashwin Rao, Justine Sherry, Arnaud Legout, Walid Dabbout, Arvind Krishnamurthy, and David Choffnes. Meddle: Middleboxes for increased transparency and control of mobile traffic. In *Proc. of CoNEXT 2012 Student Workshop*, 2012.

[6] Ethan Katz-Bassett, David R. Choffnes, Ítalo Cunha, Colin Scott, Thomas E. Anderson, and Arvind Krishnamurthy. Machiavellian routing: improving internet availability with BGP poisoning. In *Proc. of HotNets*, page 11, 2011.

[7] Xiao Sophia Wang, David Choffnes, Patrick Gage Kelley, Ben Greenstein, and David Wetherall. Measuring and predicting web login safety. In *Proc. of ACM SIGCOMM Workshop on Measurements Up the STack (W-MUST)*, 2011.

[8] Zachary S. Bischof, John S. Otto, Mario A. Sanchez, John P. Rula, David R. Choffnes, and Fabián E. Bustamante. Crowdsourcing isp characterization to the network edge. In *Proc. of ACM SIGCOMM Workshop on Measurements Up the STack (W-MUST)*, 2011.

[9] David Wetherall, David R. Choffnes, Ben Greenstein, Seungyeop Han, Peter Hornyack, Jaeyeon Jung, Stuart E. Schechter, and Xiao Sophia Wang. Privacy revelations for web and mobile apps. In *Proc. of HotOS*, 2011.

[10] David R. Choffnes and Fabian E. Bustamante. Pitfalls for testbed evaluations of internet systems. *Computer Communication Review*, 40(2):43–50, 2010.

[11] David R. Choffnes, Jordi Duch, R. Dean Malmgren, Roger Guimerà, Fabián E. Bustamante, and Luis A. Nunes Amaral. Strange bedfellows: community identification in bittorrent. In *Proc. of IPTPS*, page 13, 2010.

[12] David R. Choffnes, Mario A. Sánchez, and Fabian E. Bustamante. Network positioning from the edge - an empirical study of the effectiveness of network positioning in P2P systems. In *Proc. of IEEE INFOCOM*, pages 291–295, 2010.

[13] David Choffnes and Fabián E. Bustamante. Exploiting emergent behavior for inter-vehicle communication. In *Proc. of Hot Topics in Autonomic Computing (HotAC)*, June 2007.

[14] David R. Choffnes and Fabián E. Bustamante. An integrated mobility and traffic model for vehicular wireless networks. In *Proc. Workshop on Vehicular Ad Hoc Networks (VANET)*, pages 69–78, 2005.

OTHER PRODUCTS

2017 Director of Technology for the *Harvest* documentary film, which appeared at the Aspen Film Festival, Toronto HotDocs Film Festival, Seattle International Film Festival, BAM Cinemafest, and Rooftop Films Summer Series. The film focuses on information gathered from my ReCon project.

GRANTS (ALL EXTERNAL, FUNDED)

ASPIRE Fund

2019–2020 *Shining a Light on Dark Patterns in Mobile Apps.* $75K, shared equally with Christo Wilson.

ARCEP

2017–2020 *Partnership for auditing net neutrality violations.* Contracts. $60K.

Comcast Innovation Fund

2023 *Internet Measurements to Empirically Characterize the Digital Divide.* Gift. $85K.

2018 *Personal Virtual Networks.* Gift. $71K.

2017 *Revealing and Controlling Privacy Leaks in Network Traffic.* Gift. $70K.

Consumer Reports

2022 *Understanding Profiling via Voice Assistants.* Collaborative Research. $40K.

2022 *Investigation of IoT Dark Patterns.* Collaborative Research. $40K.

2021 *Analysis of Automated Transcription Services.* Collaborative Research. $40K.

Data Transparency Lab

2015, 2018 DTL Grantee, *ReCon: Improving Transparency and Control of PII in Mobile Network Traffic.* Unrestricted gift. Primary Investigator, joint with Alan Mislove and Christo Wilson. $55K initially, $20K followup in 2018.

Department of Homeland Security Science & Technology

2017–2019 *Revealing and Controlling Privacy Leaks in Network Traffic.* Sole PI. $350K.

Google

2017 Google Research Award, *Monitoring and diagnosis of Internet QoE.* Unrestricted gift. Joint with Renata Teixeira (Inria). $62K ($31K to Northeastern).

2015 Google Research Award, *Identifying Traffic Differentiation in Mobile Networks.* Unrestricted gift. $56K.

National Science Foundation

10/23 – 09/27 CNS-2330066, *Research Infrastructure: Mid-scale RI-1 (M1:IP): SPHERE - Security and Privacy Heterogeneous Environment for Reproducible Experimentation.* Joint with Jelena Mirkovic (lead, USC). $18M, $3.4M to Northeastern.

10/23 – 09/25 CNS-2332541, *NeTS: Continuous Monitoring and Localization of Network Neutrality Violations.* Sole PI. $99K.

10/21 – 09/26 SES-2131929, *Midscale RI: Observatory for Online Human and Platform Behavior.* Joint with David Lazer (lead, Northeastern), Christo Wilson (Northeastern). $15.7M.

10/20 – 09/24 CNS-1955227, *SaTC: Frontiers: Collaborative: Protecting Personal Data Flow on the Internet.* Lead Northeastern PI, joint with Alan Mislove, Woody Hartzog (Northeastern), Athina Markopoulou (Project Lead, UC Irvine), Zubair Shafiq (UC Davis), Konstantinos Psounis (USC). $10M (total), $1.7M (Northeastern).

10/19 – 9/22 CNS-1909020, *BehavIoT: Modeling and Controlling Internet of Things Behavior Using Network-Inferred State Machines.* Sole PI. $498K.

9/2018 – 8/2023 CNS-1750253, *CAREER: Personal Virtual Networks.* Sole PI. $513K.

10/2016–9/2019 CNS-1617728, *NeTS: Small: A Principled Approach to Enabling Policy Transparency for Mobile Networks.* co-PI, with Alan Mislove (Northeastern). $299K.

9/2016 – 8/2019 SaTC-1618955, *TWC: Small: Enabling Practical Traffic Analysis Resistance for Anonymous Communication Systems*. Sole PI. $499K.

7/2016 – 6/2020 SaTC-1564143, *TWC: Medium: Collaborative Research: Measuring and Improving the Management of Today's PKI*. co-Primary Investigator, joint with Alan Mislove, Christo Wilson (Northeastern), Dave Levin, and Tudor Dumitras (UMD). $1.2M (total), $600K (Northeastern).

1/2015 – 1/2017 CNS-1405871: *CI-New: Collaborative Research: An Open Platform for Internet Routing Experimentation*. Primary Investigator, joint with Ethan Katz-Bassett (USC) and Nick Feamster (Princeton). $1M (total), $360K (Northeastern)

9/2013 – 9/2016 CNS-1318396, *NeTS: Small: Automated Diagnosis and Root Cause Analysis of Internet Problems*. Co-Primary Investigator, joint with Arvind Krishnamurthy (University of Washington). $499K (total), $131K (Northeastern)

PwC

2019–2021 Analysis of Industrial IoT Security Threats. $100K shared with Long Lu.

Raytheon

2014 Raytheon Corporation, *Large-Scale Attacks in Multi-Level Interdependent Networks: Emerging Threats, Mitigation, and Recovery*. Grant/contract. $100K shared with Guevara Noubir, Alan Mislove, Edmund Yeh, Ravi Sundaram.

Verizon

2017–2018 *Cellular video performance measurements*. Grant/contract. $55K shared with Alan Mislove.

Amazon.com

2018 Amazon Web Services Research Grant $35K

2014 Amazon Web Services in Education Research Grants (3). $25K (in total).

ADVISING

Ph.D. Students

08/2018 – Pres. Amogh Pradeep (Northeastern)

08/2019 – Pres. Johanna Gunawan (Northeastern)

08/2020 – Pres. Tianrui Hu (Northeastern)

Alumni

08/2018 – 2023 Muhammed Talha Paracha (Northeastern, now postdoc at Bochum)

08/2015 – 2020 Fangfan Li (Northeastern, now at Facebook)

08/2014 – 2019 Jingjing Ren (Northeastern, now at Netflix)

08/2014 – 2017 Arash Molavi Kakhki (co-advised with Alan Mislove, now at ThousandEyes)

Ph.D. Committees

Spring 2023 Norbert Ludant (Northeastern, committee member)

Fall 2022 Bahruz Jabiyev (Northeastern, committee member)

Spring 2020 Giri Venkatadri (Northeastern, committee member)

Fall 2019 Abbas Razaghpanah (Stony Brook, committee member)
Spring 2019 Muhammad Ahmad Bashir (Northeastern, committee member)
Fall 2018 Jingjing Ren (Northeastern, **main advisor**)
Fall 2017 Jaijin Cao (Northeastern, committee member)
Spring 2017 Arash Molavi Kakhki (Northeastern, **main advisor**), currently at ThousandEyes
Fall 2016 Yabing Liu (Northeastern, committee member), currently at Twitter
Fall 2016 Liang Zhang (Northeastern, committee member), currently at Google
Spring 2015 Aldo Cassola (Northeastern, committee member), currently Professor at Universidad San Francisco de Quito (Ecuador)

SERVICE TO THE DISCIPLINE/PROFESSION

Steering Committee

2024–2026 ACM Internet Measurement Conference (IMC)

General Chair

2018 ACM Internet Measurement Conference (IMC)

Program Committee Co-Chair

2022 Internet Measurement Conference (IMC)
2019 Passive and Active Measurement (PAM) Conference
2018 IRTF Applied Networking Research Workshop (co-located with IETF 102)
2016–2018 Internet-QoE Workshop (co-located with SIGCOMM (2016-2017), ICDCS (2018))
2016 MobiData Workshop (co-located with MobiSys)
2015 All Things Cellular (co-located with SIGCOMM)

Program Committee Member

2023 Workshop on Technology and Consumer Protection (ConPro)
201[4,6,7,9], 2020-21, '23 ACM Internet Measurement Conference (IMC)
2017, 2023 ACM Special Interest Group on Data Communication (SIGCOMM)
2022 Privacy Enhancing Technologies Symposium (PETS)
2021 ACM Computer and Communications Security (CCS)
2020, 2022 IEEE Security and Privacy (Oakland)
2017, 2020 USENIX Network Systems Design & Implementation (NSDI)
2014–2017, 2019 ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT)
2018 Network and Distributed System Security Symposium (NDSS)
2014, 2017 International Conference on Mobile Systems, Applications, and Services (MobiSys) [External PC for 2017]
2016–2017 Data Transparency Lab (DTL) Grant Program
2015, 2016 International Workshop on Traffic Monitoring and Analysis (TMA)
2015 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)
2012, 2013 Passive and Active Measurement Conference (PAM)

Associate Editor

2015–2017 SIGCOMM Computing Communications Review (CCR)

Organization Committee

2017 CoNEXT: Travel Grant Co-Chair

2016 IMC: Works-In-Progress Chair

2016 CoNEXT: Workshop Co-Chair

Poster Committee Chair

2014 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)

Workshop Committee Member

2021 Consumer Protection (ConPro) Workshop

2013 Conference on Emerging Networking Experiments and Technologies (CoNEXT) Student Workshop

2011 SIGCOMM Workshop on Measurements "Up the Stack" (W-MUST)

2011 ACM MM '11 "Media transport and sharing"

Poster/Demo Committee Member

2021 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)

2013 Conference of the ACM Special Interest Group on Data Communication (SIGCOMM)

SOFTWARE ARTIFACTS

ReCon and Mon(IoT)r Lab

Revealing and controlling privacy leaks from mobile and IoT devices.
The mobile and IoT devices that surround our everyday lives enable great new technologies, but also come a great risks to our online privacy and security. In this project, we use machine learning and network traffic analysis to reliably infer when a user's personally identifiable information is exposed to other parties on the Internet. We further allow users to customize how such information is shared (or blocked) in the future. Our datasets have been downloaded several hundred times. `https://recon.meddle.mobi` `https://moniotrlab.ccs.neu.edu`

Wehe

Identifying net neutrality violations and empowering average users to audit their providers. Differentiation is the practice of giving different Internet service to different applications. For example, an ISP may give worse performance to YouTube (leading to rebuffering and lower quality video), but allow Netflix to stream video at full resolution without rebuffering events. This is generally considered a violation of network neutrality. We developed techniques to reliably identify when an ISP selectively gives different performance for different apps, and embedded this technology in iOS and Android apps that have seen more than 200,000 downloads. We are making our data available to consumers, regulators, and any other interested parties. In addi-

tion, we have developed strategies to evade such differentiation and continue to undertake research to more comprehensively avoid network interference.
https://wehe.meddle.mobi

Mobilyzer System for measuring Internet performance from mobile devices.
Mobilyzer is an open source library for measuring network performance on mobile platforms. You can measure your network's throughput and latency, as well as other useful network metrics. Mobilyzer also supports background measurements, server-scheduled measurements, and push-based measurements. The data is collected either anonymously or from your selected account, which allows you to see your own data. The user credentials collected are not shared outside of this site, and any data used in research projects in universities are anonymized before use.
http://www.mobilyzer-project.mobi/

Herd Practical, anonymous voice over IP (VOIP).
In the face of strong adversaries with widespread surveillance, existing privacy tools fail to provide the required anonymity or performance for interactive communication (e.g., VoIP). In this work, we are building a VoIP system that resists traffic analysis under a strong adversarial model, without sacrificing performance. We will be releasing the tool, along with source code, shortly.
https://anonymity.ccs.neu.edu/

SSL/PKI Security Understanding the security of the currently deployed public key infrastructure.
Central to the secure operation of a public key infrastructure (PKI) is the ability to revoke certificates. While much of users' security rests on this process taking place quickly, in practice, revocation typically requires a human to decide to reissue a new certificate and revoke the old one. Thus, having a proper understanding of how often systems administrators reissue and revoke certificates is crucial to understanding the integrity of a PKI. We are currently investigating how certificates are revoked, how these revocations are enforced by client software (browsers), what are the security implications of existing practices, and how we can improve the state of the art.
https://www.sslresearch.org/

Piigeon Extension for Firefox that reveals Web login safety before you submit your password.
Piigeon is a Firefox extension that records whether websites protect your username and password when you sign in. For most sites, the cursor will change, telling you whether your login is encrypted or if it could instead be intercepted. Over time a report of your password safety is created. Created by Xiao (Sophia) Wang.
http://piigeon.org/

Dasu An extension to the popular Vuze/Azureus BitTorrent client. Dasu is a dual-objective system providing ISP characterization (including the detection of network interference) and supporting Internet measurement experimenta-

tion.
Over 100,100 users as of December 2014.
http://www.aqualab.cs.northwestern.edu/projects/Dasu.html

SwarmScreen An extension to the popular Vuze/Azureus BitTorrent client to make it difficult to classify users' downloading behavior by looking at his/her connection patterns.
http://www.aqualab.cs.northwestern.edu/projects/SwarmScreen.html

NEWS A system for Network Early Warning System built by taking advantage of the natural P2P traffic. NEWS is implemented as plugin/extension for the BitTorrent Azureus client.
Over 56,000 users as of December 2014.
http://www.aqualab.cs.northwestern.edu/projects/NEWS.html

SideStep/DraFTP The SideStep service reuses CDN information to locate quality overlay paths in the Internet with minimum overhead. We also implemented DraFTP, and open-source FTP suite that uses SideStep to improve download performance.
http://www.aqualab.cs.northwestern.edu/projects/SideStep.html

Ono A plugin/extension for the Azureus client that implements our proposed CDN-based positioning for peer selection in the popular BitTorrent system.
Over 1,480,000 users as of December 2014.
http://www.aqualab.cs.northwestern.edu/projects/Ono.html

STRAW An integrated mobility and traffic model for Vehicular Ad-Hoc Networks (VANETs); STRAW is written for the JiST/SWANS discrete-event simulator.
http://www.aqualab.cs.northwestern.edu/projects/STRAW.html

SWANS++ An extension to the Jist/SWANS Discrete-event Simulator, including new/re-implementation of well-known protocols, mobility models and a steering/visualization tool.
http://aqualab.cs.northwestern.edu/projects/swansplus2.html

Ceratias Real-time visualization tool for the JiST/SWANS simulation platform. Also enables interaction with and online modification of the ongoing simulation, and can be detached/re-attached dynamically for performance.
http://sourceforge.net/projects/straw/