Prof. Emiliano De Cristofaro

Professor of Computer Science
Department of Computer Science and Engineering
University of California, Riverside
351 Winston Chung Hall, Riverside, CA 92521

Homepage: emilianodc.com
Email: me@emilianodc.com
LinkedIn: emilianodc
Google Scholar: 1wfzUuEAAAAJ

[CV Last Updated: June 11, 2025]

Research Interests

- Security and Privacy Enhancing Technologies
- Trustworthy Machine Learning
- Internet Measurement, CyberSafety, Online Harms

Education

- **PhD in Networked Systems**, University of California, Irvine (Advisor: Gene Tsudik)
  Dissertation: *Sharing Sensitive Information with Privacy*
  Fall 2007 – Summer 2011
- **BSc Honors** (5-year program) in Computer Science, *summa cum laude*, University of Salerno, Italy
  Fall 2000 – Summer 2005

Employment

- **July 2023–ongoing: University of California, Riverside (UCR)**
  - Full Professor (Step IV)
  - *Funding*: Cisco Research Gift, Privacy-Friendly Collaborative Threat Mitigation (PI, $50,000), ARL (co-I, TBA)
- **October 2013 – June 2023: University College London (UCL)**
  - (Full) Professor of Security and Privacy Enhancing Technologies (since October 2019)
  - Reader/Associate Professor (October 2017 – September 2019)
  - Senior Lecturer (October 2013 – September 2017)

  Roles:
  - Head of UCL's Information Security Research Group (September 2018–August 2022)
  - Director of the Academic Center of Excellence in Cyber Security Research (January 2019–June 2023)
  - Technology Advisor to Information Commissioner's Office (May 2019–May 2022)
  - Faculty Fellow and Leader of the Privacy in Machine Learning Interest Group at the Alan Turing Institute, UK's National Institute for Data Science and Artificial Intelligence (October 2018–September 2021)
  - Director of the MSc in Information Security (2015–2018)

  Grants and Funding (PI/co-PI):
  - Google, Privacy-Friendly Distributed Misbehavior Detection, (PI, total funding $70,000)
  - Alan Turing Institute & Accenture, A Framework for Quantifying the Privacy/Utility Trade-off in Generative Model based Synthetic Data (co-PI, total funding £150,000)
  - UKRI National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online,"REPHRAIN" (co-PI, leadership team, total funding £6,864,055, UCL funding: £799,682)
  - EU H2020 MSCA-ITN, Privacy & Usability Innovative Training Network, "Privacy & Us" (PI, total funding €3,376,517, UCL funding: €546,575)
  - EU H2020 MSCA-RISE, Enhancing Security and Privacy in the Social Web, "ENCASE" (PI, total funding: €2,160,000, UCL funding: €310,500)
  - Xerox University Affairs Committee Award and Research Councils UK IMPACT Award, "Secure Collaborative Analytics" (PI, total funding: £120,000)
  - Microsoft Research & EPSRC Case Studentship, "Privacy in Distributed Learning" (PI, total funding £120,000)
  - Amazon Research Awards, "Studying and Mitigating Inference Attacks on Collaborative Federated Learning" (PI, total funding, $100,000)

- Alan Turing Institute & GCHQ, "Evaluating Privacy-Preserving Generative Models In The Wild" (PI, total funding £70,000)
- Google Faculty Research Award, "Enabling Progress in Genomic Research via Privacy-Preserving Data Sharing" (PI, $70,000)
- Nokia Bell Labs Faculty Donation, "Privacy in Generative Models" (PI, total funding €40,000)
- Royal Society Netwon Fund Grant, "Usable Cryptographic Authentication" (co-PI, total funding: £30,000)

Grants and Funding (co-I):

- EPSRC iSense Exploratory Grant, "A technical framework for enabling and supporting data donors for medical research" (co-I, £120,000)
- Alan Turing Institute & GCHQ, "Privacy And Trust In The Decentralised Web' (co-I, total funding £70,000)

- **September 2011 – September 2013: PARC (a Xerox company);** Member of Research Staff
  - Internal and commercial projects: secure and privacy-preserving analytics; security and privacy in healthcare and genomics; security and privacy in future Internet architectures; usable enterprise security
  - US Government projects: PI on DoE-funded National Electric Sector Cybersecurity Organization Resource program (2011–2013); co-I on several NSF, DARPA, and IARPA funded projects

- **September 2007 – August 2011: University of California, Irvine;** Graduate Student Research Assistant
  - IARPA's Automatic Privacy Protection (APP) program; co-designed and implemented the fastest protocols among the four teams participating in the program
  - Co-authored several academic publications on secure information sharing and co-designed the first protocol for privacy-preserving testing on whole human genomes
  - Teaching assistant for undergraduate and graduate security classes

- **June – September 2010: Nokia Research Center, Lausanne;** PhD Intern
  - Worked with Dr. Imad Aad and Dr. Valtteri Niemi; designed, implemented, and evaluated several protocols for security and privacy protection in smartphone applications.
  - Co-authored one US patent and one paper published in the top pervasive computing conference (PERCOM)

- **September – December 2009: INRIA Rhone Alpes, Grenoble, France;** PhD Intern
  - Worked with Dr. Claude Castelluccia, discovered and demonstrated an inference attack to reconstruct search history of Google users (published at PETS)
  - Designed and implemented a system for protecting long-term privacy of published data (published at ICNP)

- **June – September 2008: NEC Europe Research Lab, Heidelberg, Germany;** PhD Intern
  - Worked with Dr. Westhoff, designed and implemented a framework for resilient data aggregation in sensor networks
  - Co-authored one paper published in the top wireless security conference (WiSec)

- **January 2006 – August 2007: University of Salerno, Italy;** Research Assistant
  - Worked with Prof. C. Blundo, Prof. G. Persiano, and Prof. V. Auletta, co-authored several academic papers
  - Research assistant on EU-funded Ecrypt and Aeolus projects

Awards

- *IEEE S&P 2025, Distinguished Paper Award.* For the paper "The Inadequacy of Similarity-based Privacy Metrics: Privacy Attacks against "Truly Anonymous" Synthetic Datasets," with Georgi Ganev, May 2025
- *ACM Distinguished Member (Class of 2025).* Recognized for "contributions to privacy-enhancing technologies and internet measurement."
- *ACM WebSci 2023, Best Paper Award.* For the paper "Understanding the Use of e-Prints on Reddit and 4chan's Politically Incorrect Board," with Satrio Baskoro Yudhoatmojo and Jeremy Blackburn, April 2023
- *ACM CCS 2022, Honorable Mention.* For the paper "Why So Toxic? Measuring and Triggering Toxic Behavior in Open-Domain Chatbots," with Wai Man Si, Jeremy Blackburn, Gianluca Stringhini, Savvas Zannettou, and Yang Zhang, November 2022
- *ACM CSCW 2021, Honorable Mention.* For the paper "Do Platform Migrations Compromise Content Moderation? Evidence from r/The_Donald and r/Incels," with Manoel Horta Ribeiro, Shagun Jhaver, Savvas Zannettou, Jeremy Blackburn, Gianluca Stringhini, and Robert West, October 2021

- *ACM CSCW 2021, Impact Recognition Award.* For the paper "I'm a Professor, which isn't usually a dangerous job: Internet-Facilitated Harassment and its Impact on Researchers," with Periwinkle Doerfler, Andrea Forte, Gianluca Stringhini, Jeremy Blackburn, and Damon McCoy, October 2021
- *ACM CyberSafety 2019, Best Paper Award.* For the paper "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web" with Savvas Zannettou, Tristan Caulfield, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn, May 2019
- *ACM IMC 2018, Distinguished Paper Award.* For the paper "On the Origins of Memes by Means of Fringe Web Communities," with Savvas Zannettou, Tristan Caulfield, Jeremy Blackburn, Michael Sirivianos, Gianluca Stringhini, and Guillermo Suarez-Tangil, October 2018
- *NDSS 2018, Distinguished Paper Award.* For the paper "Knock Knock, Who's There? Membership Inference on Aggregate Location Data," with Apostolos Pyrgelis and Carmela Troncoso, February 2018
- *5th Data Protection by Design Award.* Award issued by the Catalan Data Protection authority and the Parliament of Catalonia, for work with Luca Melis and George Danezis, June 2017
- *PARC Excellence Award.* Outstanding research performance in 2012, only 1 awarded per group
- *UC Irvine's Dissertation Fellowship*, Fall 2010 ($10,000), only 1 awarded per department
- *UC Irvine's Dean's Fellowship.* 4-year PhD financial support (2007–2011), only 5 awarded per department
- *Summa Cum Laude Honors*, University of Salerno, Italy, top 1% in graduating class

Top Publications

1. Georgi Ganev and Emiliano De Cristofaro
The Inadequacy of Similarity-based Privacy Metrics: Privacy Attacks against "Truly Anonymous" Synthetic Datasets
46th IEEE Symposium on Security and Privacy (S&P 2025)
Distinguished Paper Award
2. Meenatchi Sundaram Muthu Selva Annamalai, Igor Bilogrevic, Emiliano De Cristofaro
Beyond the Crawl: Unmasking Browser Fingerprinting in Real User Interactions
34th The Web Conference (WWW 2025)
3. Meenatchi Sundaram Muthu Selva Annamalai, Emiliano De Cristofaro
Nearly Tight Black-Box Auditing of Differentially Private Machine Learning
Thirty-Eighth Annual Conference on Neural Information Processing Systems (NeurIPS 2024)
4. Georgi Ganev, Kai Xu, Emiliano De Cristofaro
Graphical vs. Deep Generative Models: Measuring the Impact of Differentially Private Mechanisms and Budgets on Utility
31st ACM Conference on Computer and Communications Security (ACM CCS 2024), to appear
5. Meenatchi Sundaram Muthu Selva Annamalai, Georgi Ganev, Emiliano De Cristofaro
"What do you want from theory alone?" Experimenting with Tight Auditing of Differentially Private Synthetic Data Generation
33st USENIX Security Symposium (USENIX Security 2024)
6. Alexandros Efstratiou, Marina Efstratiou, Satrio Yudhoatmojo, Jeremy Blackburn, Emiliano De Cristofaro
"Here's Your Evidence": False Consensus in Public Twitter Discussions of COVID-19 Science
27th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2024)
7. Meenatchi Sundaram Muthu Selva Annamalai, Igor Bilogrevic, Emiliano De Cristofaro
FP-Fed: Privacy-Preserving Federated Detection of Browser Fingerprinting
31st Network and Distributed System Security Symposium (NDSS 2024)
8. Mohammad Naseri, Yufei Han, Emiliano De Cristofaro
BadVFL: Backdoor Attacks in Vertical Federated Learning
45th IEEE Symposium on Security and Privacy (S&P 2024)
9. Mohammad Hammas Saeed, Kostantinos Papadamou, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini
TUBERAIDER: Attributing Coordinated Hate Attacks on YouTube Videos to their Source Communities
18th International AAAI Conference on Web and Social Media (ICWSM 2024)
10. Pujan Paudel, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, Gianluca Stringhini
LAMBRETTA: Learning to Rank for Twitter Soft Moderation
44th IEEE Symposium on Security & Privacy (S&P 2023)

11. Alexandros Efstratiou, Jeremy Blackburn, Tristan Caulfield, Gianluca Stringhini, Savvas Zannettou, Emiliano De Cristofaro
Non-Polar Opposites: Analyzing the Relationship Between Echo Chambers and Hostile Intergroup Interactions on Reddit
17th International AAAI Conference on Web and Social Media (ICWSM 2023)
12. Mohammad Naseri, Yufei Han, Enrico Mariconti, Yun Shen, Gianluca Stringhini, Emiliano De Cristofaro
CERBERUS: Exploring Federated Prediction of Security Events
29th ACM Conference on Computer and Communications Security (ACM CCS 2022)
13. Wai Man Si, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, Savvas Zannettou, Yang Zhang
Why So Toxic? Measuring and Triggering Toxic Behavior in Open-Domain Chatbots
29th ACM Conference on Computer and Communications Security (ACM CCS 2022)
14. Alexandros Efstratiou and Emiliano De Cristofaro
Adherence to Misinformation on Social Media Through Socio-Cognitive and Group-Based Processes
25th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2022)
15. Georgi Ganev, Bristena Oprisanu, Emiliano De Cristofaro
Robin Hood and Matthew Effects – Differential Privacy Has Disparate Impact on Synthetic Data
39th International Conference on Machine Learning (ICML 2022)
16. Yugeng Liu, Rui Wen, Xinlei He, Ahmed Salem, Zhikun Zhang, M. Backes, Emiliano De Cristofaro, Mario Fritz, Yang Zhang
ML-Doctor: Holistic Risk Assessment of Inference Attacks Against Machine Learning Models
31st USENIX Security Symposium (USENIX Security 2022)
17. Haris Bin Zia, A. Raman, I. Castro, I. Anaobi, Emiliano De Cristofaro, N. Sastry, Gareth Tyson
Toxicity in the Decentralized Web and the Potential for Model Sharing
ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2022)
18. M. Hammas Saeed, Shiza Ali, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini
TROLLMAGNIFIER: Detecting State-Sponsored Troll Accounts on Reddit
43th IEEE Symposium on Security & Privacy (S&P 2022)
19. Mohammad Naseri, Jamie Hayes, Emiliano De Cristofaro
Local and Central Differential Privacy for Robustness and Privacy in Federated Learning
29th Network and Distributed System Security Symposium (NDSS 2022)
20. Bristena Oprisanu, Georgi Ganev, Emiliano De Cristofaro
On Utility and Privacy in Synthetic Genomic Data
29th Network and Distributed System Security Symposium (NDSS 2022)
21. Max Aliapoulios, Antonis Papasavva, Cameron Ballard, Emiliano De Stringhini, Savvas Zannettou, and Jeremy Blackburn
The Gospel According to Q: Understanding the QAnon Conspiracy from the Perspective of Canonical Information
16th International AAAI Conference on Web and Social Media (ICWSM 2022)
22. Kostantinos Papadamou, Savvas Zannettou, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Michael Sirivianos
"It is just a flu": Assessing the Effect of Watch History on YouTube's Pseudoscientific Video Recommendations
16th International AAAI Conference on Web and Social Media (ICWSM 2022)
23. Periwinkle Doerfler, Andrea Forte, Emiliano De Cristofaro, Gianluca Stringhini, Jeremy Blackburn, and Damon McCoy
"I'm a Professor, which isn't usually a dangerous job": Internet-Facilitated Harassment and its Impact on Researchers
24th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2021)
Impact Recognition Award
24. Manoel Horta Ribeiro, Shagun Jhaver, Savvas Zannettou, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Robert West
Do Platform Migrations Compromise Content Moderation? Evidence from r/The_Donald and r/Incels

24th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2021)
Honorable Mention
Media Coverage: WaPo, El Pais, The Brink, Wired

25. Kostantinos Papadamou, Savvas Zannettou, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Michael Sirivianos
"How over is it?" Understanding the Incel Community on YouTube
24th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2021)
26. Chen Ling, Ihab AbuHilal, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini
Dissecting the Meme Magic: Understanding Indicators of Virality in Image Memes
24th ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2021)
Media Coverage: Input Mag
27. Anaobi Ishaku, Igancio Castro, Aravindh Raman, Haris Bin Zia, Emiliano De Cristofaro, N. Sastry, Gareth Tyson
Throwing the Baby out with the Bathwater: Exploring Moderation in the Decentralised Web
17th International Conference on emerging Networking EXperiments and Technologies (ACM CoNext 2021)
28. Antonis Papasavva, Jeremy Blackburn, Gianluca Stringhini, Savvas Zannettou, and Emiliano De Cristofaro
"Is it a Qoincidence?": An Exploratory Study of QAnon on Voat
30th The Web Conference (WWW 2021)
Media Coverage: WaPo, El Pais, The Brink, Wired
29. Max Aliapoulios, Emmi Bevensee, Jeremy Blackburn, Emiliano De Cristofaro, Gianluca Stringhini, and Savvas Zannettou
A Large Open Dataset from the Parler Social Network
15th International AAAI Conference on Web and Social Media (ICWSM 2021)
Media Coverage: USA Today, The Conversation, Business Insider-1, Business Insider-2
30. Yuping Wang, Fatemeh Tahmasbi, Jeremy Blackburn, Barry Bradlyn, Emiliano De Cristofaro, David Magerman, Savvas Zannettou, and Gianluca Stringhini
Understanding the Use of Fauxtography on Social Media
15th International AAAI Conference on Web and Social Media (ICWSM 2021)
31. Manoel Horta Ribeiro, Jeremy Blackburn, Barry Bradlyn, Emiliano De Cristofaro Gianluca Stringhini, Summer Long, Stephanie Greenberg, and Savvas Zannettou
The Evolution of the Manosphere Across the Web
15th International AAAI Conference on Web and Social Media (ICWSM 2021)
Media Coverage: Newsweek, MIT Tech, Daily Mail
32. Apostolos Pyrgelis, Carmela Troncoso, and Emiliano De Cristofaro
Measuring Membership Privacy on Aggregate Location Time-Series
ACM International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS 2020)
33. Antonis Papasavva, Savvas Zannettou, Emiliano De Cristofaro, Gianluca Stringhini, Jeremy Blackburn
Raiders of the Lost Kek: 3.5 Years of Augmented 4chan Posts from the Politically Incorrect Board
14th International AAAI Conference on Web and Social Media (ICWSM 2020)
34. Savvas Zannettou, Barry Bradlyn, Tristan Caulfield, Emiliano De Cristofaro, Gianluca Stringhini, and Jeremy Blackburn
Characterizing the Use of Images in State-Sponsored Information Warfare Operations by Russian Trolls on Twitter
14th International AAAI Conference on Web and Social Media (ICWSM 2020)
35. Alexandros Mittos, Savvas Zannettou, Jeremy Blackburn, and Emiliano De Cristofaro
"And We Will Fight For Our Race!" A Measurement Study of Genetic Testing Conversations on Reddit and 4chan
14th International AAAI Conference on Web and Social Media (ICWSM 2020)
36. Aravindh Raman, Sagar Joglekar, Emiliano De Cristofaro, Nishanth Sastry, Gareth Tyson
Challenges in the Decentralized Web: The Mastodon Case
19th ACM Internet Measurement Conference (IMC 2019)
37. Enrico Mariconti, Guillermo Suarez-Tangil, Jeremy Blackburn, Emiliano De Cristofaro, Nicolas Kourtellis, Ilias Leontiadis, Jordi Luque Serrano, and Gianluca Stringhini

"You Know What to Do": Proactive Detection of YouTube Videos Targeted by Coordinated Hate Attacks
22nd ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW 2019)

38. Luca Melis, Congzheng Song, Emiliano De Cristofaro, and Vitaly Shmatikov
Exploiting Unintended Feature Leakage in Collaborative Learning
40th IEEE Symposium on Security & Privacy (S&P 2019)

39. Vincent Primault, Vasileios Lampos, Ingemar Cox, and Emiliano De Cristofaro
Privacy-Preserving Crowd-Sourcing of Web Searches with Private Data Donor
28th The World Wide Web Conference (WWW 2019)

40. Savvas Zannettou, Tristan Caulfield, Jeremy Blackburn, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Guillermo Suarez-Tangil
On the Origins of Memes by Means of Fringe Web Communities
18th ACM Internet Measurement Conference (IMC 2018)
Distinguished Paper Award

41. Apostolos Pyrgelis, Carmela Troncoso, Emiliano De Cristofaro
Knock Knock, Who's There? Membership Inference on Aggregate Location Data
25th Network and Distributed System Security Symposium (NDSS 2018)
Distinguished Paper award

42. Savvas Zannettou, Jeremy Blackburn, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini
Understanding Web Archiving Services and Their (Mis)Use on Social Media
12th International AAAI Conference on Web and Social Media (ICWSM 2018)

43. Bristena Oprisanu and Emilliano De Cristofaro
AnoniMME: Bringing Anonymity to the Matchmaker Exchange Platform for Rare Disease Gene Discovery
26th ISCB Conference on Intelligent Systems for Molecular Biology (ISMB 2018)

44. S. Zannettou, T. Caulfield, E. De Cristofaro, N. Kourtellis, I. Leontiadis, M. Sirivianos, G. Stringhini, J. Blackburn
The Web Centipede: Understanding How Web Communities Influence Each Other Through the Lens of Mainstream and Alternative News Sources
17th ACM Internet Measurement Conference (IMC 2017)

45. G. Hine, J. Onaolapo, E. De Cristofaro, N. Kourtellis, I. Leontiadis, R. Samaras, G. Stringhini, J. Blackburn
Kek, Cucks, and God Emperor Trump: A Measurement Study of 4chan's Politically Incorrect Forum and Its Effects on the Web
11th International AAAI Conference on Web and Social Media (ICWSM 2017)
Best Paper Runner-Up

46. E. Mariconti, L. Onwuzurike, P. Andriotis, E. De Cristofaro, G. Ross, G. Stringhini
MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Models
24th Network and Distributed System Security Symposium (NDSS 2017)

47. L. Melis, G. Danezis, E. De Cristofaro
Efficient Private Statistics with Succinct Sketches
23rd Network and Distributed System Security Symposium (NDSS 2016)

48. A. Chaabane, T. Chen, M. Cunche, E. De Cristofaro, A. Friedman, M.A. Kaafar
Censorship in the Wild: Analyzing Web Filtering in Syria
14th ACM Internet Measurement Conference (IMC 2014)
Best Paper runner-up

49. E. De Cristofaro, A. Friedman, G. Jourjon, M.A. Kaafar, M.Z. Shafiq
Paying for Likes? Understanding Facebook Like Fraud Using Honeypots
14th ACM Internet Measurement Conference (IMC 2014)

50. E. De Cristofaro, C. Soriente, G. Tsudik, A. Williams
Hummingbird: Privacy at the time of Twitter
IEEE Symposium on Security and Privacy (S&P 2012)

51. P. Baldi, R. Baronio, E. De Cristofaro, P. Gasti, G. Tsudik
Countering GATTACA: Efficient and Secure Testing of Fully Sequenced Human Genomes
ACM Conference on Computer and Communications Security (CCS 2011)

52. E. De Cristofaro, J. Kim, and G. Tsudik
Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model
IACR Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2010)

Other Publications

53. Ben Treves, Emiliano De Cristofaro, Michalis Faloutsos, Yue Dong
VIKI: Systematic Cross-Platform Profile Inference of Tech Users
17th ACM Web Science Conference (WebSci 2025)

54. Georgi Ganev, Meenatchi Sundaram Muthu Selva Annamalai, Sofiane Mahiou, Emiliano De Cristofaro
Understanding the Impact of Data Domain Extraction on Synthetic Data Privacy
Will Synthetic Data Finally Solve the Data Access Problem? (ICLR 2025 Workshop)

55. Georgi Ganev, Meenatchi Sundaram Muthu Selva Annamalai, Emiliano De Cristofaro
The Elusive Pursuit of Reproducing PATE-GAN: Benchmarking, Auditing, Debugging
Transactions on Machine Learning Research (TMLR), Feb 2025

56. Emiliano De Cristofaro
Synthetic Data: Methods, Use Cases, and Risks
IEEE Security and Privacy Magazine – Special Issue on Synthetic Realities, 2024

57. Satrio Baskoro Yudhoatmojo, Emiliano De Cristofaro, Jeremy Blackburn
Understanding the Use of e-Prints on Reddit and 4chan's Politically Incorrect Board
15th ACM Web Science Conference 2023 (WebSci 2023)
Best Paper Award

58. Utkucan Balci, Chen Ling, Emiliano De Cristofaro, Megan Squire, Gianluca Stringhini, Jeremy Blackburn
Beyond Fish and Bicycles: Exploring the Varieties of Online Women's Ideological Spaces
15th ACM Web Science Conference 2023 (WebSci 2023)

59. Yuping Wang, Savvas Zannettou, Jeremy Blackburn, Barry Bradlyn, Emiliano De Cristofaro, and Gianluca Stringhini
A Multi-Platform Analysis of Political News Discussion and Sharing on Web Communities
2021 IEEE International Conference on Big Data (IEEE BigData 2021)

60. Emiliano De Cristofaro
A Critical Overview of Privacy in Machine Learning
IEEE Security & Privacy Magazine, Volume 19, Issue 4, July-August 2021

61. Shiza Ali, Mohammad Hammas Saeed, Esraa Aldreabi, Jeremy Blackburn, Emiliano De Cristofaro, Savvas Zannettou, and Gianluca Stringhini
Understanding the Effect of Deplatforming on Social Networks
13th ACM Web Science Conference (ACM WebSci 2021)

62. Alexandros Mittos, Savvas Zannettou, Jeremy Blackburn, and Emiliano De Cristofaro
Analyzing Genetic Testing Discourse on the Web Through the Lens of Twitter, Reddit, and 4chan
ACM Transactions on the Web (TWEB), Volume 13, Issue 4, August 2020

63. Matt Wixey, Shane Johnson, and Emiliano De Cristofaro
On the Feasibility of Acoustic Attacks Using Commodity Smart Devices
IEEE Workshop on the Internet of Safe Things (co-located with IEEE S&P 2020)

64. Bristena Oprisanu, Christophe Dessimoz, and Emiliano De Cristofaro
How Much Does GenoGuard Really Guard? An Empirical Analysis of Long-Term Security for Genomic Data
18th ACM CCS Workshop on Privacy in the Electronic Society (WPES 2019)

65. Hassan Jameel Asghar, Emiliano De Cristofaro, Guillaume Jourjon, Dali Kaafar, Laurent Mathy, Luca Melis, Craig Russell, and Mang Yu
Fast Privacy-Preserving Network Function Outsourcing
Computer Networks, Vol. 163, 2019

66. Despoina Chatzakou, I. Leontiadis, J. Blackburn, Emiliano De Cristofaro, G. Stringhini, A. Vakali, and N. Kourtellis
Detecting Cyberbullying and Cyberaggression in Social Media
ACM Transactions on the Web (TWEB), Vol. 13, No. 3, 2019

67. Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn
Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web
4th Workshop on Computational Methods in CyberSafety, Online Harassment and Misinformation (ACM CyberSafety 2019)
Best Paper Award
68. Lucky Onwuzurike, Enrico Mariconti, Panagiotis Andriotis, Emiliano De Cristofaro, Gordon Ross, and Gianluca Stringhini
MaMaDroid: Detecting Android Malware by Building Markov Chains of Behavioral Models (Extended Version)
ACM Transactions on Privacy and Security (ACM TOPS), Volume 22, Issue 2, April 2019
69. Jamie Hayes, Luca Melis, George Danezis, Emiliano De Cristofaro
LOGAN: Membership Inference Attacks Against Generative Models
Proceedings on Privacy Enhancing Technologies, Vol. 2019, Issue 1 (PoPETS 2019)
70. Alexandros Mittos, Bradley Malin, and Emiliano De Cristofaro
Systematizing Genome Privacy Research: A Privacy-Enhancing Technologies Perspective
Proceedings on Privacy Enhancing Technologies, Vol. 2019, Issue 1 (PoPETS 2019)
71. Luca Melis, Apostolos Pyrgelis, Emiliano De Cristofaro
On Collaborative Predictive Blacklisting
ACM SIGCOMM's Computer Communication Review (CCR), Vol. 48, No. 5, Oct. 2018
72. Juan Echeverria, Emiliano De Cristofaro, Nicolas Kourtellis, Ilias Leontiadis, Gianluca Stringhini, Shi Zhou
LOBO -– Evaluation of Generalization Deficiencies in Twitter Bot Classifiers
2018 Annual Computer Security Applications Conference (ACSAC 2018)
73. Gergely Acs, Luca Melis, Claude Castelluccia, Emiliano De Cristofaro (Extended Version)
Differentially Private Mixture of Generative Neural Networks
IEEE Transactions on Knowledge and Data Engineering (TKDE 2018)
74. Neema Kotonya, Paolo De Cristofaro, Emiliano De Cristofaro
Of Wines and Reviews: Measuring and Modeling the Vivino Wine Social Network
IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2018)
75. Lucky Onwuzurike, Mario Almeida, Enrico Mariconti, Jeremy Blackburn, Gianluca Stringhini, Emiliano De Cristofaro
A Family of Droids–Android Malware Detection via Behavioral Modeling: Static vs Dynamic Analysis
16th Annual Conference on Privacy, Security and Trust 16th Annual Conference on Privacy, Security and Trust (PST 2018)
76. Andrea Cerulli, Emiliano De Cristofaro, Claudio Soriente
Nothing Refreshes Like a RePSI: Reactive Private Set Intersection
16th International Conference on Applied Cryptography and Network Security (ACNS 2018)
77. G. Acs, L. Melis, C. Castelluccia, E, De Cristofaro
Differentially Private Mixture of Generative Neural Networks
17th IEEE International Conference on Data Mining series (ICDM 2017)
78. Apostolos Pyrgelis, Carmela Troncoso, Emiliano De Cristofaro
What Does The Crowd Say About You? Evaluating Aggregation-based Location Privacy
17th Privacy Enhancing Technologies Symposium (PETS 2017)
79. M. Ikram, L. Onwuzurike, S. Farooqi, E. De Cristofaro, A. Friedman, G. Jourjon, D. Kaafar, M.Z. Shafiq
Measuring, Characterizing, and Detecting Facebook Like Farms
ACM Transactions on Privacy and Security (ACM TOPS 2017)
80. D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, G. Stringhini, A. Vakali
Hate is not binary: Studying abusive behavior of #GamerGate on Twitter
28th ACM Conference on Hypertext and Social Media (ACM HyperText 2017)
81. D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, G. Stringhini, A. Vakali
Mean Birds: Detecting Aggression and Bullying on Twitter
9th International ACM Web Science Conference (ACM WebSci 2017)

82. S. Farooqi, M. Ikram, E. De Cristofaro, A. Friedman, G. Jourjon, M.A. Kaafar, M.Z. Shafiq
Characterizing Key Stakeholders in an Online Black-Hat Marketplace
12th IEEE/APWG Symposium on Electronic Crime Research (eCrime 2017)

83. D. Chatzakou, N. Kourtellis, J. Blackburn, E. De Cristofaro, G. Stringhini, A. Vakali
Measuring #GamerGate: A Tale of Hate, Sexism, and Bullying
2nd WWW Workshop on Computational Methods for CyberSafety (CyberSafety 2017)

84. S. Sajadmanesh, S. Jafarzadeh, S.A. Ossia, H.R. Rabiee, H. Haddadi, Y. Mejova, M. Musolesi, E. De Cristofaro, G. Stringhini
Kissing Cuisines: Exploring Worldwide Culinary Habits on the Web
26th International World Wide Web Conference Web Science Track (WWW 2017)

85. H. Haddadi, R. Nithyanand, S. Khattak, M. Javed, N. Vallina-Rodriguez, M. Falahrastegar, J.E. Powles, E. De Cristofaro, S.J. Murdoch
The Adblocking Tug-of-War
USENIX ;login: Magazine, Winter 2016, Vol. 41, No. 4 (;login: 2016)

86. Apostolos Pyrgelis, E. De Cristofaro, G. Ross
Privacy-Friendly Mobility Analytics using Aggregate Location Data
24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL 2016)

87. E. De Cristofaro, K. Liang, Y. Zhang
Privacy-Preserving Genetic Relatedness Test
3rd International Workshop on Genome Privacy and Security (GenoPri 2016)

88. R. Nithyanand, S. Khattak, M. Javed, N. Vallina-Rodriguez, M. Falahrastegar, J. E. Powles, E. De Cristofaro, H. Haddadi, S.J. Murdoch
Ad-Blocking and Counter Blocking: A Slice of the Arms Races
6th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2016)

89. H. Asghar, L. Melis, C. Soldani, E. De Cristofaro, M.A. Kaafar, L. Mathy
SplitBox: Toward Efficient Private Network Function Virtualization
3rd ACM SIGCOMM Workshop on Hot Topics in Middleboxes and Network Function Virtualization (HotMiddleBox 2016)

90. L. Melis, H. Asghar, E. De Cristofaro, D. Kaafar
Private Processing of Outsourced Network Functions: Feasibility and Constructions
1st ACM Workshop on Security in Software Defined Networks & Network Function Virtualization (SDNNFVSEC 2016)

91. L. Onwuzurike and E. De Cristofaro
Experimental Analysis of Popular Smartphone Apps Offering Anonymity, Ephemerality, and End-to-End Encryption
1st NDSS Workshop on Understanding and Enhancing Online Privacy (UEOP 2016)

92. K. Krol, M.S. Rahman, S. Parkin, E. De Cristofaro, E. Vasserman
An Exploratory Study of User Perceptions of Payment Methods in the UK and the US
10th NDSS Workshop on Usable Security (USEC 2016)

93. J. Freudiger, E. De Cristofaro, A. Brito
Controlled Data Sharing for Collaborative Predictive Blacklisting
12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2015)

94. M. Nagy, T. Bui, E. De Cristofaro, N. Asokan, J. Ott, A.R. Sadeghi
How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length with Social PaL
8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2015)

95. L. Onwuzurike and E. De Cristofaro
Danger is my middle name: Experimenting with SSL Vulnerabilities in Android Apps
8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2015)

96. E. Ayday, E. De Cristofaro, J.P. Hubaux, G. Tsudik
Whole Genome Sequencing: Revolutionary Medicine or Privacy Nightmare
IEEE Computer Magazine, Vol. 48, No. 2, February 2015

Presented as a poster at Usenix Security 2013 and available on ArXiv under the title "The Chills and Thrills of Whole Genome Sequencing"

97. K. Krol, E. Philippou, E. De Cristofaro, M.A. Sasse
"They brought in the horrible key ring thing" – Analysing the Usability of Two-Factor Authentication in UK Online Banking
9th NDSS Workshop on Usable Security (USEC 2015)

98. G. Danezis and E. De Cristofaro
Fast and Private Genomic Testing for Disease Susceptibility
12th ACM CCS Workshop on Privacy in the Electronic Society (WPES 2014)

99. I. Bilogrevic, J. Freudiger, E. De Cristofaro, E. Uzun
What's the Gist? Privacy-Preserving Aggregation of User Profiles
19th European Symposium on Research in Computer Security (ESORICS 2014)

100. F. Beato, E. De Cristofaro, K.B. Rasmussen
Undetectable Communication: The Online Social Networks Case
12th IEEE Annual Conference on Privacy, Security and Trust (PST 2014)

101. C. Blundo, E. De Cristofaro, P. Gasti
EsPRESSo: Efficient Privacy-Preserving Evaluation of Sample Set Similarity
Journal of Computer Security, Vol. 22, No. 3, May 2014 (Submitted Oct 2012, Accepted Sep 2013)
Extended Abstract appeared in 7h ESORICS Workshop on Data Privacy Management (DPM 2012).

102. E. De Cristofaro
Genomic Privacy and the Rise of a New Research Community
IEEE Magazine on Security and Privacy, March/April 2014 Issue, Vol. 13, No. 1, 2014

103. E. De Cristofaro
An Exploratory Ethnographic Study of Issues and Concerns with Whole Genome Sequencing
8th NDSS Workshop on Usable Security (USEC 2014)

104. E. De Cristofaro, H. Du, J. Freudiger, G. Norcie
Two-Factor or not Two-Factor? A Comparative Usability Study of Two-Factor Authentication
8th NDSS Workshop on Usable Security (USEC 2014)

105. M. Nagy, E. De Cristofaro, A. Dmitrienko, N. Asokan, A.R. Sadeghi
Do I Know You? - Efficient and Privacy-Preserving Common Friend-Finder Protocols and Applications
29th Annual Computer Security Applications Conference (ACSAC 2013)

106. E. De Cristofaro, C. Soriente
Extended Capabilities for a Privacy-Enhanced Participatory Sensing Infrastructure (PEPSI)
IEEE Transactions on Information Forensics & Security. Vol.8, No. 12, 2013

107. E. De Cristofaro, S. Faber, G. Tsudik
Secure Genomic Testing with Size- and Position-Hiding Private Substring Matching
12th ACM CCS Workshop on Privacy in the Electronic Society (WPES 2013)

108. A. Chaabane, E. De Cristofaro, M.A. Kaafar, E. Uzun
Privacy in Content-Oriented Networking: Threats and Countermeasures
ACM SIGCOMM Computer Communication Review (CCR), 2013
Invited at ACM SIGCOMM 2013 as one of the two "Best CCR Papers."

109. G. Norcie, E. De Cristofaro, V. Bellotti
Bootstrapping Trust in Online Dating: Social Verification of Online Dating Profiles
Financial Cryptography and Data Security (FC) Workshop on Usable Security (USEC 2013)

110. A. Cardenas, R. Chow, E. De Cristofaro
Data Handling in the Smart Grid: Do We Know Enough?
IFIP International Conference on Critical Infrastructure Protection (CIP 2013)

111. E. De Cristofaro, C. Soriente
Participatory Privacy: Enabling Privacy in Participatory Sensing
IEEE Network. Vol. 27, No. 1. January 2013 (Submitted March 2011, Accepted January 2012.)

112. E. De Cristofaro, M. Manulis, B. Poettering
Private Discovery of Common Social Contacts
International Journal of Information Security (IJIS). Vol. 12, No. 1, 2013.
Extended abstract appeared in ACNS 2011

113. E. De Cristofaro, C. Soriente, G. Tsudik, A. Williams
Tweeting with Hummingbird: Privacy in Large-Scale Micro-Blogging OSNs
IEEE Data Engineering Bulletin. Vol. 35, Number 4, December 2012

114. E. De Cristofaro, P. Gasti, G. Tsudik
Fast and Private Computation of Set Intersection Cardinality
11th International Conference on Cryptology and Network Security (CANS 2012)

115. E. De Cristofaro, S. Faber, P. Gasti, Gene Tsudik
GenoDroid: Are Privacy-Preserving Genomic Tests Ready for Prime Times?
International Workshop on Privacy in Electronic Society (WPES 2012)

116. C. Blundo, E. De Cristofaro, P. Gasti
EsPRESSo: Efficient Privacy-Preserving Evaluation of Sample Set Similarity
International Workshop on Data Privacy Management (DPM 2012).

117. E. De Cristofaro and R. Di Pietro
Adversaries and Countermeasures in Privacy-Enhanced Urban Sensing Systems
IEEE Systems Journal, Special Issue on Security and Privacy of Complex Systems, 2012.

118. E. De Cristofaro and G. Tsudik
Experimenting with Fast Private Set Intersection
International Conference on Trust and Trustworthy Computing (TRUST 2012)

119. E. De Cristofaro, R. Di Pietro
Preserving Query Privacy in Urban Sensing Systems
International Conference on Distributed Computing and Networking (ICDCN 2012)

120. M. Almishari, E. De Cristofaro, K. El Defrawy, G. Tsudik
Harvesting SSL Certi□cate Data to Identify Web-Fraud
International Journal of Network Security. Vol. 14, No. 6, 2012

121. E. De Cristofaro
Sharing Sensitive Information with Privacy
University of California, PhD Dissertation, 2011

122. C. Castelluccia, E. De Cristofaro, A. Francillon, M.A. Kaafar
EphPub: Toward Robust Ephemeral Publishing
IEEE Conference on Network Protocols (ICNP 2011)

123. E. De Cristofaro, Y. Lu, G. Tsudik
Efficient Techniques for Privacy-Preserving Sharing of Sensitive Information
International Conference on Trust and Trustworthy Computing (TRUST 2011)

124. E. De Cristofaro, C. Soriente
PEPSI: Privacy Enhancing Participatory Sensing Infrastructure
ACM Conference on Wireless Security (WiSec 2011)

125. E. De Cristofaro, A. Durussel, I. Aad
Reclaiming Privacy for Smartphone Applications
IEEE International Conference on Pervasive Computing and Communications (PerCom 2011)

126. G. Ateniese, E. De Cristofaro, G. Tsudik
(If) Size Matters: Size-Hiding Private Set Intersection
IACR International Conference on Practice and Theory of Public Key Cryptography (PKC 2011)

127. C. Castelluccia, E. De Cristofaro, and D. Perito
Private Information Disclosure from Web Searches
Privacy Enhancing Technologies Symposium (PETS 2010)
Also appeared as a poster at IEEE Symposium on Security and Privacy (S&P 2010)

128. E. De Cristofaro and J. Kim
Some like it private: Sharing Confidential Information based on Oblivious Authorization
IEEE Security and Privacy, July-August, 2010

129. E. De Cristofaro and G. Tsudik
Practical Private Set Intersection Protocols with Linear Complexity
Financial Cryptography and Data Security (FC 2010)

130. V. Auletta, C. Blundo, A.De Caro, E. De Cristofaro, G.Persiano, and I.Visconti
Increasing Privacy Threats in the Cyberspace: the Case of Italian e-Passports
Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC 2010)

131. E. De Cristofaro, S.Jarecki, J.Kim, and G. Tsudik
Privacy-preserving Policy-based Information Transfer
Privacy Enhancing Technologies Symposium (PETS 2009)

132. E. De Cristofaro, X.Ding, and G. Tsudik
Privacy-preserving Querying in Sensor Networks
IEEE International Conference on Computer Communications and Networks (ICCCN 2009)

133. E. De Cristofaro, J.M.Bohli, and D.Westhoff
FAIR: Fuzzy-based Aggregation providing In-network Resilience for real-time WSNs
ACM Conference on Wireless Network Security (WiSec 2009)

134. C. Blundo, E. De Cristofaro, A.Del Sorbo, C.Galdi, and G.Persiano
A Distributed Implementation of the Certified Information Access Service
European Symposium on Research in Computer Security (ESORICS 2008)

135. C. Blundo, E. De Cristofaro, C.Galdi, and G.Persiano
Validating Orchestration of Web Services with BPEL and Aggregate Signatures
IEEE European Conference on Web Services (ECOWS 2008)

136. E. De Cristofaro
A Secure and Privacy-Protecting Aggregation Scheme for Sensor Networks
IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM 2007)

137. V. Auletta, C. Blundo, E. De Cristofaro, S.Cimato, and G. Raimato
Authenticated Web Services: A WS-Security Based Implementation
IFIP International Conference on New Technologies, Mobility, and Security (NTMS 2007)

138. C. Blundo and E. De Cristofaro
A Bluetooth-based JXME infrastructure
International Symposium on Distributed Objects, Middleware, and Applications (DOA 2007)

139. V. Auletta, C. Blundo, and E. De Cristofaro
A J2ME transparent middleware to support HTTP connections over Bluetooth
International Conference on Systems and Network Communications (ICSNC 2007)

140. V. Auletta, C. Blundo, E. De Cristofaro, and G. Raimato
A lightweight framework for Web Services invocation over Bluetooth
IEEE International Conference on Web Services (ICWS 2006)

141. V. Auletta, C. Blundo, E. De Cristofaro, and G. Raimato
Performance Evaluation for Web Services invocation over Bluetooth
ACM Conference on Modeling and Simulation of Wireless and Mobile Systems (MSWiM 2006)

Patents

- Method and Apparatus for Preserving Privacy for Appointment Scheduling.
US Patent US8667062. Co-inventors: Imad Aad, Valtteri Niemi, Anthony Durussel, Igor Bilogrevic, Jean-Pierre Hubaux
- Method and apparatus for performing distributed privacy-preserving computations on user locations.
US Patent US8954737B2. Co-inventors: Joan Melia Segui, Rui Zhang, Oliver Brdiczka, Ersin Uzun
- Methods for Selection of Collaborators for Online Threat Mitigation.
US Patent US9817977. Co-inventors: Julien Freudiger, Ersin Uzun, Alejandro Brito, Marshall Bern

- Method and Apparatus for Privacy and Trust Enhancing Sharing of Data for Collaborative Analytics.
  US Patent US9275237. Co-inventors: Julien Freudiger, Ersin Uzun, Alejandro Brito, Marshall Bern
- Portable Proxy For Security Management And Privacy Protection And Method Of Use.
  US Patent US9578062B2. Co-inventors: Julien Freudiger, Ersin Uzun, Golam Sarwar
- Methods for Centralized Privacy-Preserving Collaborative Threat Mitigation.
  US Patent US9477839B2. Co-inventors: Julien Freudiger, Ersin Uzun, Alejandro Brito, Marshall Bern
- Computer-Implemented System And Method For Verifying Online Dating Profiles.
  US Patent Application 20140156750. Co-inventors: Victoria Bellotti and Gregory Norcie
- Privacy-Sensitive Ranking of User Data.
  US Patent Application 20150371059. Co-inventors: Igor Bilogrevic, Julien Freudiger, Ersin Uzun
- Private and Distributed Computation of Probability Density Functions.
  US Patent Application 20150372808. Co-inventors: Igor Bilogrevic, Julien Freudiger, and Ersin Uzun

Service

- **PC/Track Co-Chair:** ACM CCS 2025 (Usability & Measurement), TTO 2020, ACM CCS 2018 (Privacy), WWW 2018 (Security & Privacy), GenoPri 2018, GenoPri 2015, PETS 2014, PETS 2013, HotPETs 2012
- **PC Member:** IEEE S&P 2026, IEEE S&P 2025, Usenix Security 2025, ACM CCS 2024, IEEE S&P 2023, NDSS 2023, WWW 2023, SIGMETRICS 2023, SIGMETRICS 2022, NDSS 2022, WWW 2022, PETS 2022 (Senior), IEEE S&P 2022, IEEE S&P 2021, SIGMETRICS 2021, SIGMETRICS 2020, IEEE S&P 2020, WWW 2020, Usenix Security 2020, ACM CCS 2019, NDSS 2020, NDSS 2019, ICWSM 2018, ACM CCS 2018, PETS 2018, ACM HyperText 2018, ICDCS 2018, IEEE EuroSP 2018, ACM CCS 2017, WWW 2017, NDSS 2017, PETS 2017, AsiaCCS 2017, WiSec 2016, IEEE S&P 2016, NDSS 2016, PKC 2016, PETS 2016, EuroUSEC 2016, GenoPri 2016, PPML 2016, USEC 2015, WPES 2015, IEEE S&P 2015, Financial Crypto 2015, WiSec 2014, WWW 2014, ICCCN 2014, GenoPri 2014, SESOC 2014, WPES 2014, SESOC 2013, CANS 2013, WISEC 2013, Financial Crypto 2013, CANS 2012, PETS 2012, WISEC 2012, DPM 2012, ICCCN 2012, WPES 2012, CCSW 2012, CANS 2011, ISC 2010
- **Journals:** Associated Editor for the Journal of Cybersecurity (Cryptography and Associated Topics, 2015–2018) and ACM Transactions of Privacy and Security (ACM TOPS, 2021–).
- **Funding:** NSERC (Canada), NSF SaTC (USA), PRIN (Italy), FWO (Belgium), EPSRC (UK), FWF (Austria)
- **Organization:** Dagstuhl Seminar on "PETs and AI: Privacy Washing and the Need for a PETs Evaluation Framework" (March 9–14, 2025); IEEE EuroSP 2018, General Co-Chair (April 24–26, 2018), Dagstuhl Seminar on "Cybersafety in Modern Online Social Networks" (September 10–13, 2017)

Keynotes (not updated since 2019)

- *Membership and Property Inference Attacks against Machine Learning Models*
  The Bright and Dark Sides of Computer Vision: Challenges and Opportunities for Privacy and Security (CV-COPS 2019)
  Long Beach, CA, June 2019
- *The Genomics Revolution: The Good, The Bad, and The Ugly – A Privacy Researcher's Perspective*
  Microsoft Faculty Summit 2016
  Microsoft Research, Redmond, USA, July 2016
- *The Genomics Revolution: The Good, The Bad, and The Ugly – A Privacy Researcher's Perspective*
  Privacy-aware Computational Genomics Keynote (PRIVAGEN 2015), Tokyo, September 2015
- *The Genomics Revolution: Innovation Dream or Privacy Nightmare?*
  HotSpot and TPDP 2015 Joint Keynote Talk, London, April 2015
- *Whole Genome Sequencing: Innovation Dream or Privacy Nightmare?*
  EPFL Summer Research Institute (SuRI), Lausanne, Switzerland, June 2013

Teaching

- **Teaching at UCR:** CS 163 Privacy (Spring 2025), CS 179F Project in Computer Science–Operating Systems (Winter 2025), CS 260 Privacy Seminar (Spring 2024), CS 254 Network Security (Winter 2024), CS 179F Project in Computer Science–Operating Systems (Fall 2023)

- **Teaching at UCL:** Security (BSc/MEng Computer Science, Winter 2023, Winter 2022), Introduction to Cryptography (MSc InfoSec, Fall 2014, Fall 2015, Fall 2016, Fall 2017), Computer Security II (MSc InfoSec, Winter 2014, Winter 2015, Winter 2016, Winter 2017, Winter 2018, Winter 2019, Winter 2020), Privacy Enhancing Technologies (MSc InfoSec, Winter 2019, Winter 2020)
- **Teaching Assistant:** Network Security (UC Irvine, 2011), Crypto Protocols (University of Salerno, Italy, 2006)
- **Coordinator:** Academic Centre of Excellence in Cyber Security Research (ACE-CSR) Distinguished Seminars Series (UCL, 2014–2020), PARC Privacy Lunch (2012–2013), PARC Security Reading Group (2011–2012)

Mentoring

- **Current Supervision at UCR**: Md. Olid Hasan Bhuiyan, Rohith Krishna Papani (PhD Advisor); Alexander Hickerson (PhD Co-Advisor);
- **Current Supervision at UCL**: Georgi Ganev, Meenatchi Sundaram Muthu Selva Annamalai (PhD Advisor);
- **Graduated PhD Students** (Main PhD Advisor): Luca Melis (2014–2018, now Research Scientist at Meta), Lucky Onwuzurike (2014–2018, now Senior Security Consultant at E&Y), Apostolos Pyrgelis (2015–2018, now Senior Researcher at RISE Research Institutes of Sweden), Alexandros Mittos (2015–2020, now Data Scientist at PS AI Labs), Bristena Oprisanu (2017–2021, now Research Scientist at Bitfount), Antonis Papasavva (2019–2024, now Post-Doctoral Researcher at UCL), Mohammad Naseri (2019–2024, now Research Scientist at Flower Labs), Alexandros Efstratiou (2020–2024, now Postdoctoral Researcher at University of Washington)
- **Post-doc Alumni**: Vincent Primault (2017–2018), Lukasz Olejnik (2016–2017), Konstantinos Papadamou (2021-2023);
- **PhD Committee**: Hélène Orsini (INRIA Rennes, 2025), Joonas Jälkö (Aalto University, 2023), Sina Sajadmanesh (EPFL, 2023), Federica Granese (Institut Polytechnique de Paris, 2023), César Sabater (INRIA, 2022), Nikolaos Lykousas (University of Pireaus, 2022), Raouf Kerkouche (INRIA, 2021), Ania Piotrowska (UCL, 2020), Tejas Kulkarni (Warwick University, 2019), Jaroslav Sedenka (Masaryk University, 2019), Marc Roeschlin (Oxford University, 2018), Ingolf Becker (UCL, 2018), Marc Roeschlin (Oxford University, 2018), Manu Drijvers (IBM/ETH, 2018), Jean-Louis Raisaro (EPFL, 2018), Saman Feghhi (Trinity College Dublin, 2017), Sharad Kumar (University of Cambridge, 2016), Iacovos Kirlappos (UCL, 2016), Iraklis Leontidas (EURECOM, 2015), Filipe Beato (KU Leuven, 2015), Lukasz Olejnik (INRIA, 2015), Gines Dolera Tormo (University of Murcia, 2014), Abdelberi Chaabane (INRIA, 2014), Miguel Malheiros (UCL, 2013