Yves-Alexandre de Montjoye

http://deMontjoye.com

Current positions

Imperial College London, United Kingdom

Associate Professor of Applied Mathematics and Computer Science (UK: Reader), 2022-now
Associate Professor of Applied Mathematics and Computer Science (UK: Senior Lecturer), 2020-2022
Assistant Professor (UK: Lecturer), 2017-2020

Head of the Computational Privacy Group, Dept. of Computing
Director of the Algorithmic Society Lab, Data Science Institute

European Commission, Brussels, Belgium

Special Adviser on AI, Privacy, and Data Protection to Commissioner Reynders (Justice), 2020-2023

Belgian Data Protection Authority, Brussels, Belgium

Parliament-appointed member, 2019-2024

Royal Academy of Science, Letters and Fine Arts of Belgium, Brussels, Belgium

Member of the Technology and Society Class (Collegium), 2022-

Previous positions

European Commission, Brussels, Belgium

Special Adviser to Commissioner Vestager (Competition), 2018-2019

Massachusetts Institute of Technology, Cambridge, MA

Research Affiliate, *Media Lab*, 2017-2019
Research Scientist, *Media Lab*, 2016-2017
Post-doctoral researcher, *Media Lab*, 2015-2016

Harvard University, Cambridge, MA

Post-doctoral researcher, *Harvard IQSS and Computer Science*, 2015-2016
Supervision: Latanya Sweeney, Gary King

The Boston Consulting Group, Boston, MA

Intern, Strategic Analytics (now BCG Gamma), Summer 2014

Education

Massachusetts Institute of Technology, Cambridge, MA

Ph.D., *Media Lab*, 2010-2015
Thesis: "Computational Privacy: Towards Privacy-Conscientious Uses of Metadata"
Committee: Alex (Sandy) Pentland (Advisor), Gary King, and Alessandro Acquisti

Université catholique de Louvain, Belgium

M.Sc. in Applied Mathematics, 2007-2009
Major in Discrete Mathematics and Computer Science
Thesis: "Stability in society: Parameters for the persistence of social network"
Advisors: Vincent D. Blondel and Nathan Eagle
Visiting researcher at the Santa Fe Institute, NM

Katholieke Universiteit Leuven, Belgium
M.Sc. Mathematical Engineering, 2007-2009

École Centrale Paris, France
Centralien (M.Sc.), 2005-2007

Université catholique de Louvain, Louvain-La-Neuve, Belgium
B.Sc. in engineering, 2003-2006

Publications

Total number of citations: 7500+, H-index: 26
http://scholar.google.com/citations?user=LVJtdoEAAAAJhl=en

Journal papers

[24] Rocher, L., Tournier, A.J. and de Montjoye, Y.-A., 2023. Adversarial competition and collusion in algorithmic markets. **Nature Machine Intelligence**, pp.1-8.

[23] Houssiau F., Liénart T., Hendrickx J., and de Montjoye, Y.-A., 2023. Web privacy: a Formal Adversarial Model for Query Obfuscation **IEEE Transactions on Information Forensics and Security**.

[22] Houssiau F., Sapieżyński P., Radaelli L., Shmueli E., and de Montjoye, Y.-A., 2023. Detrimental Network Effects in Privacy: A Graph-theoretic Model for Node-based Intrusions **Cell Patterns**, 4(1), p.100662.

[21] Tournier, A. J. and de Montjoye, Y.-A., 2022. Expanding the attack surface: Robust profiling attacks threaten the privacy of sparse behavioral data. **Science Advances**, 8(33), eabl6464.

[20] Creţu A.-M., Monti F., Marrone S., Dong X., Bronstein M., and de Montjoye, Y.-A., 2022. Interaction data are identifiable even across long periods of time. **Nature Communications**, 13(313).
Also presented at the ACM CSS PPML 2021 and the NeurIPS PriML 2021 workshops.

[19] Houssiau F, Rocher L, and de Montjoye, Y.-A., 2022. On the difficulty of achieving DP in practice: user-level guarantees in aggregate location data **Nature Communications** (Matters Arising), 13(29)

[18] Chatalic A., Schellekens V., Houssiau F., de Montjoye, Y.-A., Jacques L. and Gribonval R. Compressive Learning with Privacy Guarantees. **Information and Inference**, Oxford University Press (OUP), 10.1093/imaiai/iaab005.

[17] Farzanehfar, A., Houssiau, F. and de Montjoye, Y.-A., 2021. The risk of re-identification remains high even in country-scale location datasets. **Cell Patterns**, 2(3), p.100204.

[16] de Montjoye, Y.-A., Ramadorai, T., Valletti, T. and Walther, A., 2020. Privacy, adoption, and truthful reporting: A simple theory of contact tracing applications. **Economics Letters**, 198, p.109676.

[15] Rocher, L., Hendrickx, J.M. and de Montjoye, Y.-A., 2019. Estimating the success of re-identifications in incomplete datasets using generative models. **Nature Communications**, 10(1), p.3069.

[14] Mulders D., de Bodt C., Bjelland J., Pentland A. S., Verleysen M., de Montjoye Y.-A., 2019. Inference of node attributes from social network assortativity. **Neural Computing and Applications**, pp.1-21.

[13] de Montjoye Y.-A., Gambs S., Blondel Y., Canright G., de Cordes N., Deletaille S., Engø-Monsen K., Garcia-Herranz M., Kendall J., Kerry C., Krings G., Letouze E., Luengo-Oroz M., Oliver N., Rocher L., Rutherford A., Smoreda Z., Steele J., Wetter E., Pentland A., Bengtsson L., 2018. On the privacy-conscientious use of mobile phone data. **Nature SData**, 5.

[12] Kondor, D., Hashemian, B., de Montjoye, Y.-A and Ratti, C., 2018. Towards matching user mobility traces in large-scale datasets. **IEEE Transactions on Big Data**

[11] Taquet, M., Quoidbach, J., de Montjoye, Y.-A. Desseilles, M. and Gross, J.J., 2016. Hedonism and the choice of everyday activities. **Proceedings of the National Academy of Sciences**, 113(35)

[10] Jahani, E., Sundsøy, P., Bjelland, J., Bengtsson, L. and de Montjoye, Y.-A., 2017. Improving official statistics in emerging markets using machine learning and mobile phone data. **EPJ Data Science**, 6(1)

[9] Steele, J.E., Sundsøy, P.R., Pezzulo, C., Alegana, V.A., Bird, T.J., Blumenstock, J., Bjelland, J., Engø-Monsen, K., de Montjoye, Y.-A., Iqbal, A.M. and Hadiuzzaman, K.N., 2017. Mapping poverty using mobile phone and satellite data. **Journal of The Royal Society Interface**, 14(127), p.20160690.

[8] de Montjoye, Y.-A., Rocher, L. and Pentland, A.S., 2016. bandicoot: A python toolbox for mobile phone metadata. **Journal of Machine Learning Research**, 17, pp.1-5.

[7] de Montjoye Y.-A., Radaelli, L. and Singh, V.K., 2015. Unique in the shopping mall: On the reidentifiability of credit card metadata. **Science**, 347(6221), pp.536-539.

[6] de Montjoye, Y.-A., Stopczynski, A., Shmueli, E., Pentland, A. and Lehmann, S., 2014. The strength of the strongest ties in collaborative problem solving. **Nature SRep**, 4, p.5277.

[5] de Montjoye, Y.-A., Shmueli, E., Wang, S.S. and Pentland, A.S., 2014. openpds: Protecting the privacy of metadata through safeanswers. **PloS ONE**, 9(7), p.e98790.

[4] Taquet, M., Quoidbach, J., de Montjoye, Y.-A. and Desseilles, M., 2014. Mapping collective emotions to make sense of collective behavior. **Behavioral and Brain Sciences**, 37(1), pp.102-103.

[3] de Montjoye Y.-A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D., 2013. Unique in the crowd: The privacy bounds of human mobility. **Nature S.Rep.**, 3, p.1376.

[2] de Montjoye, Y.-A., Wang, S.S. and Pentland A., 2012. On the Trusted Use of Large-Scale Personal Data. **IEEE Data Eng. Bull.** 35(4), pp.5-8.

[1] Good, B.H., de Montjoye, Y.-A. and Clauset, A., 2010. Performance of modularity maximization in practical contexts. **Physical Review E**, 81(4), p.046106.

Conferences papers

[13] Jain, S., Cretu, A.M., Cully, A. and de Montjoye, Y.-A., 2023, May. Deep perceptual hashing algorithms with hidden dual purpose: when client-side scanning does facial recognition. In 2023 IEEE Symposium on Security and Privacy (pp. 234-252). **IEEE S&P** (oral presentation)

[12] Creţu, A-M*, Houssiau F*, Cully A. and de Montjoye, Y.-A., 2022. QuerySnout: Automating the Discovery of Attribute Inference Attacks against Query-Based Systems. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (pp. 623-637). **ACM CCS** (oral presentation)

[11] Gadotti, A., Houssiau, F., Annamalai, M.S.M.S. and de Montjoye, Y.-A., 2022. Pool Inference Attacks on Local Differential Privacy: Quantifying the Privacy Guarantees of Apple's Count Mean Sketch in Practice. 31st USENIX Security Symposium **USENIX Security** (oral presentation).

[10] Jain S., Creţu A.-M. and de Montjoye, Y.-A., 2022. Adversarial Detection Avoidance Attacks: Evaluating the robustness of perceptual hashing-based client-side scanning. **USENIX Security**. (oral presentation) Also presented as extended abstract at the AI Village@DEF CON 29, HotPETs 2021, NeurIPS PriML 2021 workshop, and at the Conference on Applied Machine Learning in Information Security (CAMLIS 2021)

[9] Rocher, L., Muthu, M.S., and de Montjoye, Y.-A., 2021, The Observatory of Anonymity: A Reactive Tool to Understand Re-Identification Risks in 89 countries. In The World Wide Web Conference (**WWW**). ACM.

[8] Gadotti, A.*, Houssiau, F.*, Rocher, L.*, Livshits, B., and de Montjoye, Y.-A., 2019. When the signal is in the noise: The limits of Diffix's sticky noise. 28th USENIX Security Symposium **USENIX Security** (oral presentation)

[7] Jain, S., Bensaid, E. and de Montjoye, Y.-A., 2019. UNVEIL: Capture and Visualise WiFi Data Leakages. In The World Wide Web Conference (**WWW**) (pp. 3550-3554). ACM.

[6] Schellekens, V., Chatalic, A., Houssiau, F., de Montjoye, Y.-A., Jacques, L. and Gribonval, R., 2019, May. Differentially Private Compressive K-means. IEEE International Conference on Acoustics, Speech and Signal Processing (**ICASSP**) (pp. 7933-7937)

[5] Felbo, B., Sundsøy, P., Lehmann, S. and de Montjoye, Y.-A., 2017. Modeling the Temporal Nature of Human Behavior for Demographics Prediction. European Conference on Machine Learning and Principles and Practice of Knowledge Discovery (**ECML-PKDD**) (pp. 140-152). Springer.

[4] Sundsøy, P., Bjelland, J., Iqbal, A.M. and de Montjoye, Y.-A., 2014. Big data-driven marketing: how machine learning outperforms marketers' gut-feeling. International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction (**SBP**) (pp. 367-374). Springer, Cham.

[3] de Montjoye, Y.-A.*, Quoidbach, J.*, Robic, F.* and Pentland, A.S.*, 2013, April. Predicting personality using novel mobile phone-based metrics. International conference

on social computing, behavioral-cultural modeling, and prediction (**SBP**) (pp. 48-55). Springer, Berlin, Heidelberg.

[2] de Montjoye, Y.-A., Haria, J., Cebrian, M. and Pentland, A., 2011, October. The Need for Champions for Approximate Social Search. **IEEE SocialCom** (pp. 231-234). IEEE.

[1] Eagle, N., de Montjoye, Y.-A. and Bettencourt, L.M.A., 2009, Community computing: Comparisons between rural and urban societies using mobile phone data. **IEEE SocialCom** (Vol. 4, pp. 144-150). IEEE.

Workshop papers

[3] Houssiau, F., Schellekensn, V., Chatalic, A. Annamraju, S. K., and de Montjoye, Y.-A., M2M: A general method to perform various data analysis tasks from a differentially private sketch. **STM22** The 18th International Workshop on Security and Trust Management (co-located w/ ESORICS'22)

[2] Schellekens, V., Chatalic, A., Houssiau, F., de Montjoye, Y.-A., Jacques, L. and Gribonval, R. 2019. Compressive k-means with differential privacy. **SPARS** Signal Processing with Adaptive Sparse Structured Representations Workshop (pp. 1-2).

[1] Mulders, D., De Bodt, C., Bjelland, J., Pentland, A.S., Verleysen, M. and de Montjoye, Y.-A., 2017. Improving individual predictions using social networks assortativity. International Workshop on Self-Organizing Maps and Learning Vector Quantization, Clustering and Data Visualization (**WSOM**+)

Book chapters

Toole, J. L., de Montjoye, Y.-A., González, M.C. and Pentland, A.S., 2015. Modeling and understanding intrinsic characteristics of human mobility. Social Phenomena: From Data to Models (pp. 15-35). Springer, Cham.

Policy & opinions

Maynard, T., Baldassarre, L.*, de Montjoye, Y.A.*, McFall, L.* and Óskarsdóttir, M.*, 2022. AI: Coming of age?. Annals of Actuarial Science, pp.1-5.

de Montjoye, Y.A. and Taquet, M., 2019. Anonymity takes more than protecting personal details. Nature, 574, p.176.

Crémer J.*, de Montjoye Y.-A.* and Schweitzer H.*, 2019. Competition Policy for the digital era. Report to EC Competition Commissioner Vestager.

de Montjoye Y.-A., Farzanehfar A., Hendrickx J. and Rocher L., Solving Artificial Intelligence's Privacy Problem. Facts Reports (Special Issue 17 pp.80-83) and Data Science Institute White Paper, February 2018

de Montjoye, Y.A., Pentland A.S. 2015. Assessing data intrusion threats—Response. Science, 348(6231), pp.195-195.

Member of the expert committee, Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics. European Union Agency for Network and Information Security (ENISA) report, December 2015, ISBN 978-92-9204-160-1

de Montjoye Y.-A., Kendall J., Kerry C. F., Enabling Humanitarian Use of Mobile

Phone Data. Issues in Technology Innovation, Brookings Center for Technology Innovation. (2014)

de Montjoye Y.-A., Hidalgo C. A., Pentland A., Il est temps de parler des métadonnées, Le Monde, June 27, 2013

Hidalgo C. A., de Montjoye Y.-A., Pentland A., Solution to NSA overreach - put people in charge of their own data, The Christian Science Monitor, June 11, 2013

Blogposts

Wong, A., Jain, S., Cretu, A.M. and de Montjoye, Y.-A., 2022. Deep perceptual hashing is not robust to adversarial detection avoidance attacks.

de Montjoye, Y.-A., Houssiau, F., Gadotti, A. and Guepin, F., 2020. Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask.

de Montjoye, Y.-A. and Houssiau, F., 2020. Can we fight COVID-19 without resorting to mass surveillance?.

Gadotti, A., Houssiau, F., Rocher, L. and de Montjoye, Y.-A., 2018. When the signal is in the noise: Exploiting Aircloak's Diffix anonymization mechanism.

de Montjoye, Y.-A., Houssiau, F., Sapieżyński, P. and Radaelli, L., 2018. Cambridge Analytica is only the beginning and you might have your friends to blame for it.

Others

Salah, A.A., Pentland, A., Lepri, B., Letouzé, E., Vinck, P., de Montjoye, Y.-A., Dong, X. and Dağdelen, Ö., 2018. Data for Refugees: The D4R Challenge on Mobility of Syrian Refugees in Turkey.

de Montjoye, Y.-A., Smoreda, Z., Trinquart, R., Ziemlicki, C. and Blondel, V.D., 2014. D4D-Senegal: the second mobile phone data for development challenge.

Patents

Rocher, L., Hendrickx, J.M. and de Montjoye, Y.-A., 2020. Assessing likelihood of re-identification, International Application PCT/GB2020/051498

Awards and committees

Member of the International Cyber Security Center of Excellence (INCS-CoE), 2022
Member of the PETs expert forum, Information Commissioner's Office, 2021
Member of the advisory group, The Forum (Imperial College), 2021-
Member of (UK) DCMS' Digital Markets Research Working Group under the Chief Economist, 2021
Member of the (UK) Geospatial Commission Oversight Group, 2021
Concurrence Antitrust Writing Awards (for Competition Policy for the digital era w/ Jacques Crémer and Heike Schweitzer), 2020
Member of the World Economic Forum's Data for Common Purpose Initiative (DCPI), 2020-2021
The [Imperial College] President's Awards for Excellence in Research, 2019
Member of the jury for the CNIL/INRIA award for research on privacy protection, 2016, 2017, 2018, 2019
Honorable Mention in the UN Global Pulse's Data For Climate Challenge, 2017
Member of the IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems, 2015-2018
Member of the World Economic Forum network on AI, IoT and the Future of Trust,

2016
Member of the OECD Advisory Group on Health Data Governance, 2015
Innovators under 35 for Belgium (TR35), 2015
Amazon Graduate Research Symposium (declined), 2014
MIT-Imperial Global Fellow, 2013
MIT Harold Horowitz Award, 2012
Fellow of the B.A.E.F. foundation (Firmin van Brée Fellow), 2010

PhD students

Yifeng Mao, TBD, 2022-
Vincent Guan, TBD, 2022-
Matthieu Meeus, TBD, 2022-
Bozhidar Stevanoski, Automating privacy attacks, 2021-
Florent Guepin, Membership inference attacks, 2021-
Ana-Maria Cretu, Adversarial machine learning, 2018-
Shubham Jain, Fairness in algorithmic decision-making, 2018-
Axel Oehmichen, Privacy-preserving data processing platforms, 2017-2019
Andrea Gadotti, Beyond de-identification: An adversarial approach to evaluate the practical guarantees of privacy-preserving systems for collecting and sharing data, 2017-2022
Florimond Houssiau, Adversarial Privacy: an attack-defence approach to modern privacy protection, 2017-2021
Arnaud Tournier, Adverse Effects of Learning Algorithms, 2017-2021
Ali Farzanehfar, The impact of technology on data collection, 2016-2021
Luc Rocher, Anonymization in the 21st Century: A Critical Examination of De-identification for Modern Large-Scale Data, 2015-2019 (co-supervised with Julien Hendrickx at UCLouvain)