Institution: Goldsmiths, University of London		
Unit of Assessment: 21, Sociology		
Title of case study: Protecting Privacy: Using sociological research to design algorithmic security systems		
Period when the underpinning research was undertaken: 2013 - onwards		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s): Daniel Neyland	**Role(s) (e.g. job title):** Professor	**Period(s) employed by submitting HEI:** 2012-present
Period when the claimed impact occurred: August 2013 - onward		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Neyland's research on the privacy and surveillance implications of algorithmic technology has been translated into a set of ethical principles that have informed the design and development of new security systems for industry partners, including SEA, operator of Milan Linate Airport and RENFE, operator of the Spanish State Railway. Algorithms automate complex forms of decision making, but this requires data collection, storage and analysis on an unprecedented scale, raising questions of surveillance and privacy. Drawing on Neyland's research, five large technology developments have reduced potential harms, and risks of harm, through intrusive surveillance that would have undermined individual and collective privacy of large sections of the population. Neyland's advice made members of the IT, transport and security industry more aware of privacy risks, changing their design behaviour and the capacity of the technologies they developed.

2. Underpinning research

Algorithmic systems are now a ubiquitous feature of contemporary life, automating many everyday decision-making processes by drawing together huge amounts of data. By collecting, storing and processing data on an unprecedented scale, operating without human intervention and producing consequential decisions for large sections of the population, these systems raise significant privacy and surveillance concerns (R1, R4). These concerns are made most apparent in locations such as airports and train stations where digital video data on tens of millions of passengers is collected and analysed by algorithmic systems to decide automatically, for example, who counts as a security risk (R2). These systems have remained largely unaccountable as they are closed, proprietary technologies, often not accessible to, or well understood by, regulators (R3). Neyland's research thus involves unprecedented access to the design and development of algorithmic systems and plays a vital role in rendering these systems accountable.

In a three year project entitled 'Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance' (ADDPRIV, 2011-2014), Neyland carried out an ethnographic study (with support from Dr. Inga Kroener and Dr. Patrick Murphy; see R1) of the development of an algorithmic surveillance system to be deployed by RENFE (Spanish state railway with 262 million passenger journeys in 2018) and SEA (owner and operator of Milan Linate airport with 9.2 million passenger journeys in 2018). Unlike conventional fieldwork, that might seek to retain

distance from participants, this ethnography was designed to deliver practical outcomes by helping computer scientists (from Kingston and Gdansk Universities, working with Hewlett Packard, RENFE and SEA) to produce a new surveillance system that would respect privacy by cutting down on data storage and by making automated, algorithmic decision-making, accessible and accountable to data protection authorities (R2).

Building on a fieldwork method developed in his previous projects, Neyland's research created three ethical principles to guide the design of the new surveillance technology and reverse the privacy-intrusive features commonly associated with algorithms (R2, R3). The principles were to: 1) reduce the scope of data made visible; 2) reduce the amount of data stored; and 3) to create an automated basis for managing system accountability (R5). The reach and significance of this impact has been developed in further industry-academic collaborations such as VideoSense and Eyes of Things and by feeding into policy discussions.

3. References to the research

R1. D. Neyland (2019) *The Everyday Life of an Algorithm* (London: Palgrave) https://www.palgrave.com/us/book/9783030005771 [Open Access]
R2. D. Neyland (2016) 'Bearing Account-able Witness to the Ethical Algorithmic System' *Science, Technology and Human Values*, 41(1): 50-76 DOI: https://doi.org/10.1177/0162243915598056 [Submitted to REF2]
R3. D. Neyland and N. Mollers (2016) 'Algorithmic IF…THEN rules and the conditions and consequences of power,' *Information, Communication and Society,* 20(1): 45-62 DOI: https://doi.org/10.1080/1369118X.2016.1156141 [Available on Request]
R4. D. Neyland (2015) 'On Organizing Algorithms' *Theory, Culture and Society* 32(1): 119-32 DOI: https://doi.org/10.1177/0263276414530477 [Available on Request]
R5. D. Neyland (2018) 'Something and Nothing: On algorithmic deletion, accountability and value'. *Science and Technology Studies* 31(4) DOI: https://doi.org/10.23987/sts.56744 [Open Access]

These publications are all peer reviewed and are products of EU FP7 funded research project ADDPRIV (grant no. 261653), Project Partner; EU Contribution to Goldsmiths EUR156,240 (Feb 2011-March 2014)

4. Details of the impact

To translate ethnographic research into ethical design practice, in ADDPRIV Neyland developed a design method for developing ethical algorithmic systems. This involved establishing an ethics board, which in ADDPRIV comprised: Jan Philipp Albrecht (MEP and one of the original authors of the General Data Protection Regulation), two national Data Protection Authorities (DPAs), two privacy academics and two members of privacy-focused civil liberty groups. Neyland presented to the ethics board his developing study of the algorithmic system (R2) to show how the system made sense of spaces such as Linate airport and RENFE train stations, how it was expected to work with operators' everyday competences for securing those spaces and how successfully the system met the project's ethical principles. In place of buying into the claims made on behalf of algorithms by other members of the project team or in popular and academic discussions of algorithms (R4), Neyland could present the system itself, how it worked and its future trajectory of development. In response, members of the ethics board used Neyland's presentations, along with demonstrations of the technology to open up the algorithmic system to a form of

accountability by raising questions which fed back into the ongoing project and the design of the system, and which could be included in public project reports.

1.Protecting privacy for the public: research raises awareness of privacy issues resulting in the development of new ethical privacy-sensitive surveillance system

Neyland's method produced ethical insights appropriate and relevant to a new and emerging technology, setting out what would constitute an ethical, algorithmic system. This directly reduced the potential harm and risk of harm for such a system to invade the privacy of up to 271 million passenger journeys a year in Linate airport and RENFE train stations where the system was being developed and would in future be used. Neyland's research also raised awareness of privacy issues for the transport, IT and security industry and academic computer science partners in the project, altering their design behaviour and changing the capacity of the technology produced.

Using Neyland's ethical design method, the ADDPRIV project produced a new ethical, privacy sensitive surveillance system that automatically deletes data (reducing privacy concerns), limits the range of visible data (reducing surveillance concerns) and provides automated outputs to data protection authorities (enhancing system accountability). This new technology was the direct result of the research that Neyland carried out, the ethical design method that he set up and managed, and the design advice that this method produced and fed into the development of the technological system. This altered the design practices of Anova consulting, Hewlett Packard, SEA airport operator and RENFE railways, who were working in collaboration with technical teams from Kingston University, Trinity College Dublin and Gdansk University. As the ADDPRIV Project Co-ordinator states:

> "Daniel Neyland's role on the project was to work with the consortium to research and understand the ethical implications of the technology, to help feed ethical concerns into the design of the system and to set up and run an ethics advisory board. His role included providing a critical analysis of the potential ethical impacts and opportunities of the proposed ADDPRIV technology and solutions. This was with particular reference to the possible impacts that ADDPRIV may have on the privacy of individuals who would be subject to the ADDPRIV technology." (S1)

2.Achieving compliance: research ensures new algorithmic systems comply with GDPR

As a result of Neyland's work on ADDPRIV he has been invited to help design other algorithmic systems with surveillance capabilities. The broader reach of this impact now lies in providing demonstration technologies that the security and IT industry across Europe and beyond can see and follow.

Privacy enhancing surveillance systems that comply with the EU General Data Protection Regulation (GDPR) now exist because of Neyland's research. For example, Neyland contributed to the design of a range of new visual surveillance technologies in the Eyes of Things project (EU Horizon 2020, 2015-2018). As a result of Neyland's role on the ethics board, an algorithmic emotion recognition system, a front-door alarm system, an interactive museum guide and a life-logging camera being developed by Thales, Movidus, Evercam, Nviso and Awaibahad, in conjunction with UCLM, had to change the way they managed and stored data. Following lessons learnt in the ADDPRIV project, less secure data stores were replaced by more secure encrypted stores, the technologies automatically delete data at the end of its lifespan and the way in which experimental subjects were taken through technology trials, and what happened to

their data, was transformed on the basis of Neyland's advice. As the Eyes of Things project co-ordinator stated:

> "Daniel has contributed to the successful completion of the project by feeding ethical advice into the design and development of four new technologies… The ethical advice has been crucial for managing issues of notification and consent, data handling, data access, data storage and transmission. This has led to the development of encrypted data storage, the development of protocols for use of cloud-based facilities, ethics protocols for incorporating potentially vulnerable research subjects in technology trials and a process for shredding data. The project would not have been the same without this advice." (S2)

In a further project – VideoSense (2011-2015) – Neyland contributed to the design of algorithmic systems with surveillance capabilities being developed by Thales, Eurecom, and Isdefe, in collaboration with computer scientists from the University of Reading, Queen Mary's and the Technical University of Berlin. As a member of the Ethics Advisory Board of the VideoSense Centre of Excellence, Neyland raised awareness of privacy issues, which altered the design behaviour of computer scientists and the capacities of technologies produced. As the project co-ordinator stated, Neyland's role:

> "was to provide advice on the technical achievements of the project and how these could be attuned to ethical goals. Technological developments that the ethics board considered ranged from specific deployments – such as the use of video-analytics on data drawn from surveillance drones – through to the development and adoption of privacy standards for MPEG and JPEG." (S3)

Beyond these projects, Neyland has developed the reach of his work through providing further advice on privacy and surveillance issues to two more EU-funded projects FORTRESS (focused on disaster management and data handling) and CRISP (focused on privacy certification). Here Neyland was called upon to ensure the projects achieved GDPR compliance.

3.Influencing UK government debates on ethical data collection through algorithmic systems

As a result of the work detailed above, Neyland has also contributed evidence on the implications of privacy sensitive, algorithmic systems to the 'Algorithms in Decision-Making Inquiry' of the House of Commons Science and Technology Committee (2018). Neyland's evidence, along with his research on algorithms (with reference to R2), was quoted in the Committee's 2018 Report of the 4th session of the Inquiry (S4). Through direct citation to Neyland's work, the report highlights the importance of understanding transparency and accountability in algorithmic systems, noting that; 'Algorithm accountability is often framed in terms of openness and transparency, and the ability to challenge and scrutinise the decisions reached using algorithms.' Three of the Committee's main findings, published in the conclusions and recommendations of the Inquiry, were based on transparency and accountability in the development of algorithmic systems (S5).

5. Sources to corroborate the impact

S1 Factual Statement from user/beneficiary no. 1: Statement from Project Co-ordinator of ADDPRIV, 18.6.2018

S2 Factual Statement from user/beneficiary no. 2: Statement from Project Co-ordinator of Eyes of Things, 11.6.2018

S3 Factual Statement from user/beneficiary no. 3: Statement from Co-ordinator of VideoSense, 18.6.2018
S4 Report: Daniel Neyland Submission of Evidence to The Algorithms in Decision-Making Inquiry (ALG027, S4a) and research paper (R2) cited in, House of Commons Science and Technology Committee. 'Algorithms in decision making', Fourth Report of the Session, 2017-2019, 23/5/2018 p. 26-27
S5 Report: Commons Select Committee, Science and Technology, Conclusions and recommendations of the Algorithms in Decision-Making Inquiry: 23.5.2018