TRUST & TECHNOLOGY INITIATIVE

Exploring the dynamics of trust and distrust around internet technologies, society and power.

www.trusttech.cam.ac.uk
www.twitter.com/CamTrustTech

UNIVERSITY OF CAMBRIDGE

Contents

Introducing the Initiative ***2***

Get in touch ***4***

Get involved ***4***

Executive Committee ***5***

Steering Committee ***7***

Cambridge Perspectives on Trust & Technology ***16***

What if Uber Goes Under? 16

Empowering Trust and Security from Hardware 19

S-Money 20

Lex Ex Machina: From Rule of Law to Legal Singularity 22

Is Digital Security by Design Possible? 24

Institutions, Technology and Trust 26

Compliant and Accountable Systems 29

Smart Urbanism and Mental Health in Singapore 31

Introducing the Initiative

The Trust & Technology Initiative brings together and drives forward interdisciplinary research from Cambridge and beyond to:

- Explore the dynamics of trust and distrust in relation to internet technologies, society and power
- Better inform trustworthy design and governance of next generation tech at the research and development stage
- Promote informed, critical, and engaging voices supporting individuals, communities and institutions in light of technology's increasing pervasiveness in societies.

The Initiative is unique in considering the interplays and feedback loops between technology fundamentals, societal impact and governance of next generation systems at the research and development stage. Our particular ability to connect cutting edge deep technology with social science and humanities expertise enables dynamic exploration of emergent use cases, and for us to envisage and experiment with realistic future scenarios.

A network around trust, technology, society and power

As a network, the Initiative is a 'big tent,' bringing people together, facilitating collaboration, and engaging industry, civil society, government, and the public, across:

- Relationships and interplays between technology and society; the legal, ethical and political frameworks impacting both trust and technology, and innovative governance, in areas such as transport, critical infrastructure, identity, manufacturing,

healthcare, financial systems and networks, communications systems, internet of things
- The nature of trust and distrust; trust in technology, and trust through technology; the many dimensions of trust at individual, organisational and societal levels
- Rigorous technical foundations, for resilient, secure and safe computer systems, including data and communications platforms, artificial intelligence, and robotics

What the Trust & Technology Initiative does

- Connects the research community around trust and technology
- Catalyses new collaborative projects and activities
- Builds capacity and strengthens knowledge transfer
- Influences national and international research and policy agendas
- Acts as a helpful gateway to Cambridge for external partners

How we work

The Trust & Technology Initiative team proactively engages researchers and partners, and uses creative ways to bring together diverse participants and enable effective discussion and collaboration. We help interdisciplinary research ideas to emerge, and can support proposal development and securing resources. The Initiative also creates content to bridge between disciplines and sectors, and seeks new ways to connect researchers and enable prototyping and testing of ideas.

We are interested in more than just research collaborations, and are exploring what value the Initiative can offer potential partner organisations, including networking and brokering support, workshops and roundtables, strategic reports, and other services.

Get in touch

- Website: www.trusttech.cam.ac.uk
- Twitter: @CamTrustTech
- Mailing list: bit.ly/CamTrustTechList
- Email: admin@trusttech.cam.ac.uk

Get involved

We're developing a variety of ways to get more involved with the Trust & Technology Initiative. If you'd like to work with us in some way, please email us at admin@trusttech.cam.ac.uk, including a few sentences about your research and interests and how they relate to Trust & Technology, and whether you'd like to play an active part in our work (for instance, organising events, writing blog posts, etc). We'll be in touch to discuss options.

All are welcome to contribute to the Trust & Technology Initiative's Zotero library of interesting papers and articles. Find the library here: http://bit.ly/camtrusttechlibrary.

Executive Committee

Prof. Simon Moore, Co-Chair

Department of Computer Science and Technology

Professor Simon Moore is a Professor of Computer Engineering at the University of Cambridge Computer Laboratory in England, where he undertakes research and teaching in the general area of computer design with particular interests in secure and rigorously-engineered computer architecture. Professor Moore is the senior member of the Computer Architecture research group.

Dr Jat Singh, Co-Chair

Department of Computer Science and Technology

Dr Jat Singh is based at the Dept. Computer Science & Technology (Computer Laboratory), where he leads the Compliant and Accountable Systems research group. The group considers the intersections of computer science and law -- exploring means for better aligning technology with legal concerns, and vice-versa. He also co-chairs the Trust & Technology Initiative, which drives research exploring the dynamics of trust and distrust in relation to internet technologies, society and power. Jat is a Fellow of the Alan Turing Institute, the UK's national institute for data science and AI, and is active in the tech-policy space, having served on advisory councils for the UK Government and the Financial Conduct Authority.

Dr Jennifer Cobbe, Coordinator

Department of Computer Science and Technology

Dr Jennifer Cobbe is the Coordinator of the Trust & Technology Initiative and a researcher in the Department of Computer Science and Technology. Her research looks at the intersection of new and emerging technologies, law, and society from an interdisciplinary perspective. She is interested in legal responses to new and emerging technologies (typically but not exclusively AI/machine learning), tech industry business models, and platform power; technical means for improving legal compliance and accountability of complex systems; and theoretical approaches to privacy, surveillance, and emerging tech. Jennifer is part of the Microsoft Cloud Computing Research Centre and a member of the Law Committee of the IEEE's Global Initiative on Ethics of Autonomous and Intelligent Systems.

Dr Ella McPherson

Department of Sociology

Dr Ella McPherson is the Department of Sociology's Lecturer in the Sociology of New Media and Digital Technology as well as the Anthony L. Lyster Fellow in Sociology at Queens' College. She is also Co-Director of the Centre of Governance and Human Rights, where she leads the research theme on human rights in the digital age. Ella's research focuses on symbolic struggles surrounding the media in times of transition, whether democratic or digital. She is particularly interested in the implication of these struggles for the formation, evaluation and contestation of truth-claims. Her current research, which has

been funded by an ESRC Future Research Leader fellowship as well as by the Isaac Newton Trust, is on human rights fact-finding in the digital age. Ella also leads The Whistle, an academic startup supported by an EU Research and Innovation Horizon 2020 grant, which aims to support the collection and verification of human rights information for evidence.

Steering Committee

Dr Anne Alexander

Centre for Research in the Arts, Social Sciences and Humanities

Dr Anne Alexander is Director of the Learning Programme at Cambridge Digital Humanities, a network of researchers at the University of Cambridge who are interested in how the use of digital tools is transforming scholarship in the humanities and social sciences. Her research interests include ethics of big data, activist media in the Middle East and the political economy of the Internet. She is a member of the Data Ethics Group at the Alan Turing Institute and a member of the Steering Group of the Trust and Technology Strategic Research Initiative.

Dr Richard Clayton

Department of Computer Science and Technology

Dr Richard Clayton is a security researcher in the Computer Laboratory of the University of Cambridge and the Director of the Cambridge Cloud Cybercrime Center, working in the field of work in the field of "security economics". He has research interests in email spam, fake bank "phishing" websites, and other Internet wickedness. As an expert in these areas, he is a regular speaker and media commentator. He has also

assisted the APIG and APComms all-party groups of MPs in their inquiries into Internet issues, and he acted as the "specialist adviser" for the House of Lords Science and Technology Committee's two inquiries into "Personal Internet Security".

Dr Rob Doubleday

Centre for Science and Policy

Dr Rob Doubleday has been Executive Director of the Centre for Science and Policy at the University of Cambridge since 2012. Previously Rob established CSaP's research programme. His research interests include the role of science, evidence and expertise in contemporary societies, in particular the relationship between scientific advice, public policy and democracy. In 2010 Rob spent a year on secondment to the Government Office for Science, working on policies to promote engagement between academia and government. Prior to this Rob was the principal investigator of a three-year Wellcome Trust funded project that studied the policy and public dimensions of nanotechnologies. Rob has degrees in Chemistry (Imperial College, London) and Science and Technology Policy (SPRU, University of Sussex). He has a PhD in Geography and Science & Technology Studies from University College London and studied at the Harvard Kennedy School on a Fulbright Scholarship. Rob is also a Senior Research Associate in the Department of Geography at Cambridge.

Dr David Erdos

Centre for Intellectual Property and Information Law

Dr David Erdos is Deputy Director of the Centre for Intellectual Property and Information Law (CIPIL) and University Senior Lecturer in Law and

the Open Society in the Faculty of Law. He is also WYNG Fellow in Law at Trinity Hall. David's current research explores the nature of Data Protection especially as it intersects with the right to privacy, freedom of expression, freedom of information and freedom of research. This work intersects with debates on internet governance generally including, in particular, the liability and responsibility of "intermediary" actors such as Facebook and Google. David's work has been published widely in leading legal and socio-legal journals including the Cambridge Law Journal, the Common Market Law Review, Public Law and the Journal of Law and Society.

Dr Tanya Filer

Bennett Institute for Public Policy

Dr Tanya Filer leads the Digital State Project at the Bennett Institute for Public Policy. Her work focuses on GovTech (government technology) innovation ecosystems, and on digital government more broadly. Amid rapid technological change and deepening inequality, she seeks to understand how governments can better engage digital and emerging technologies, including for improved service provision and more meaningful forms of citizen participation. Tanya has published numerous articles and chapters including in Information, Communication & Society, International Journal of Politics, Culture and Society, Journal of Iberian and Latin American Studies, and the edited volume Conspiracy Theories and the People Who Believe Them (OUP, 2019). She also runs Tech States, the Institute's interview series featuring leading international voices on government and technology.

Prof Jennifer Gabrys

Department of Sociology

Professor Jennifer Gabrys is Chair in Media, Culture and Environment, a post she began in October 2018. Previously, she was Professor in the Department of Sociology at Goldsmiths, University of London, where she continues to have an affiliation as honorary Visiting Professor. She has also been a visiting Research Fellow at the Digital Cultures Research Lab in the Centre for Digital Cultures, Leuphana University of Lüneburg, Germany. Since 2013, she has been the Principal Investigator on the ERC-funded project 'Citizen Sense' -- a pioneering investigation into the public engagement with environmental sensing technologies and citizen-data generation in both urban and rural locations in the US and the UK. Gabrys has been awarded an ERC Proof of Concept grant, 'AirKit' (2018-2019), to further develop Citizen Sense research. The Citizen Sense project has received multiple awards, including the John Ziman award for public engagement in science and technology awarded by the European Association for the Study of Science and Technology (EASST) in 2018.

Dr Julian Huppert

Intellectual Forum, Jesus College

Dr Julian Huppert is the Founding Director of the Intellectual Forum, which is aimed at covering the widest range of academic interests across the College. His background is as a scientist, working on unusual structures of DNA. In particular, DNA of particular sequences can form four-stranded knot-like structures called G-quadruplexes, which can function as genomic switches, turning genes on and off. His work used biophysical and computational methods to predict the formation of these structures, and has led to the identification of a large number of

possible anti-cancer drug targets. After five years away as the MP for Cambridge, his research focus changed to look at science and technology policy, including the challenges of privacy in the digital age. He has also worked on how to best use evidence in public policy making – a perennial challenge.

Prof Adrian Kent

Department of Applied Mathematics and Theoretical Physics

Professor Adrian Kent is Professor of Quantum Physics in the Department of Applied Mathematics and Theoretical Physics and a Distinguished Visiting Research Chair at Perimeter Institute for Theoretical Physics. His research interests span the foundations of physics and technological applications of quantum information. He pioneered the use of relativistic signalling constraints in cryptography, and co-authored research that sparked the field of “device-independent” quantum cryptography, which gives users security guarantees even when their devices may have been designed by a malicious supplier. More recently, he has developed “supermoney”, a form of token that gives users privacy and issuers security against fraud and is faster and more flexible than any existing technology. He has a strong interest in how we most effectively channel science and technological developments to shape our future in positive directions and to reduce catastrophic threats, and is a member of the scientific advisory board of the Cambridge Centre for the Study of Existential Risk.

Prof John Naughton

Centre for Research in the Arts, Social Sciences and Humanities

Professor John Naughton is a Senior Research Fellow at CRASSH, Emeritus Professor of the Public Understanding of Technology at the Open University, Director of the Wolfson Press Fellowship Programme and the Technology columnist of the London *Observer*. By background a systems engineer, he is an historian of the Internet whose main research interests lie in the network's impact on society. He has written extensively on technology and its role in society; his most recent book, *From Gutenberg to Zuckerberg: what you really need to know about the Internet,* is published by Quercus. He was co-director of the *Technology and Democracy* and *Conspiracy and Democracy* research projects at CRASSH. His most recent work and publications have focussed on surveillance capitalism and the power and responsibilities of technology corporations.

Prof Daniel Ralph

Judge Business School

Professor Daniel Ralph is Professor of Operations Research at Cambridge Judge Business School, and is part of the School's Operations & Technology Management subject group. Professor Ralph is a member of the Australian Mathematical Society, INFORMS, the Mathematical Optimization Society and SIAM. He was Editor-in-Chief of *Mathematical Programming (Series B)* from 2007-2013 and has served on the editorial boards of *Mathematics of Operations Research* and the *SIAM Journal on Optimization*

Dr Manj Sandhu

Department of Medicine

Dr Manj Sandu's research focuses on the integration of principles and procedures underlying population genetics and epidemiology. Together with current and emerging genome-wide technologies, this approach provides unparalleled opportunities to identify the biological mechanisms underlying the development of complex diseases and traits. His work has largely centred on the genetic basis of cardiometabolic traits and diseases, particularly lipid metabolism and coronary artery disease, and the use of genetic tools for causal inference. More recently, he has begun developing epidemiological resources to explore genomic diversity and its impact on infectious and cardiometabolic risk factors and diseases in Sub-Saharan African populations, as part of a public health and epidemiological research programme.

Dr Simone Schnall

Department of Psychology

Dr Simone Schnall is the Director of the Cambridge Body, Mind and Behaviour Laboratory and Fellow of Jesus College. By combining insights and methods from social psychology and cognitive science her research explores how thoughts and feelings interact. She aims to understand how people make judgments and decisions about other people, and about physical properties of the world. For example, Schnall's research has examined the role of bodily influences in the context of, first, moral judgments and behaviours, and second, perceptions of the spatial environment. Current research topics include judgments and decisions in moral and legal contexts, perceptions of the physical environment, and risky behaviours in finance (e.g., risk

management in banks). In general the work seeks to understand why people often think and behave in seemingly surprising ways, and how to capitalize on insights from behavioural science to encourage adaptive choices in everyday life.

Dr Phillip Stanley-Marbell

Department of Engineering

Dr Phillip Stanley-Marbell is a University Lecturer in the Internet of Things in the Department of Engineering. Phillip's research exploits the structure of signals in the physical world and the flexibility of human perception to make computation more efficient. His research focuses on designing hardware architectures, algorithms, and programming language constructs that use an understanding of the physical world and the flexibility of sensing systems to improve the efficiency of computing systems that interact with nature. His research results range from fundamental theory, to algorithms, programming languages, and compiler tools. Phillip frequently build printed circuit board and FPGA prototypes to validate concepts.

Dr Adrian Weller

Department of Engineering

Dr Adrian Weller is a senior research fellow in machine learning at the University of Cambridge. Adrian is Programme Director for AI at The Alan Turing Institute (national institute for data science and AI), where he is also a Turing Fellow leading a group on Fairness, Transparency and Privacy. He is a senior research fellow at the Leverhulme Centre for the Future of Intelligence (CFI) leading work on Trust and Transparency; the David MacKay Newton research fellow at Darwin College; and an advisor

to the Centre for Science and Policy (CSaP), and the Centre for the Study of Existential Risk (CSER). Adrian serves on the boards of several organizations, including the Centre for Data Ethics and Innovation (CDEI). Previously, Adrian held senior positions in finance. He continues to be an angel investor and advisor.

Dr Jess Whittlestone

Leverhulme Centre for the Future of Intelligence

Dr Jess Whittlestone is a research associate at the Leverhulme Centre for the Future of Intelligence, focused on AI policy. She is particularly interested in how we can build appropriate levels of trust in AI systems amongst policymakers and the general public, and how to avoid harmful misperceptions of the capabilities and risks of AI. Jess has a PhD in Behavioural Science from the University of Warwick, and a first class degree in Mathematics and Philosophy from Oxford University. In her PhD, she argued that confirmation bias is not necessarily as "irrational" as it seems, with implications for how we think about the strengths and weaknesses of human reasoning. Previously, Jess worked for the Behavioural Insights Team, where she advised various government departments on improving their use of behavioural science, evidence, and evaluation methods, with a particular focus on foreign policy and security.

Cambridge Perspectives on Trust & Technology

In the run up to our symposium, we asked researchers from Cambridge to give us their thoughts on trust and technology. This is what they said.

Full versions of articles, with references where appropriate, are available on our website.

What if Uber Goes Under?

Dr Jennifer Cobbe
Trust & Technology Initiative

The popular taxi (or, in startup parlance, "ride-sharing") company Uber has been making headlines recently, having lost $5.24 billion in three months of 2019 alone[1]. For most companies, this would be a grave situation. Uber, however, is not most companies, and it doesn't seem overly concerned about its balance sheet. That's because heavy losses are part of its long-term strategy. Bankrolled by tens of billions of dollars in venture capital, it hopes to run at a loss to undercut the competition and drive them out of business[2].

---

[1] Rushe, Dominic. 2019. Uber sees biggest-ever quarterly loss: $5bn in three months. *The Guardian*. Available at https://www.theguardian.com/technology/2019/aug/08/uber-quarterly-earnings-loss-stocks-shares [accessed 13/09/2019].
[2] Horan, Herbert. 2019. Uber's Path of Destruction. *American Affairs* 3(2). Available at https://americanaffairsjournal.org/2019/05/ubers-path-of-destruction [accessed 13/09/2019].

Establishing a monopoly would bring huge financial rewards for Uber (and its investors), but it's a high-risk strategy. To succeed, Uber must sustain heavy losses for many years while systematically seeking to shape regulatory and financial incentives in its favour. Trying to keep costs as low as possible, it aggressively fights any attempts to recognise its drivers as workers and to extend to them even the most basic of workers' rights and employment benefits.

Uber's plan has already paid off in places, devastating the local taxi market in some American cities[3]. And, seduced by the possibility of cheaper (VC-subsidised) transport, some civic governments are even playing along. The Canadian town of Innisfil, for example, has contracted with Uber to provide public transport for its citizens in place of local bus services[4]. As local taxis face extinction and bus services are gradually replaced, those who rely on them – the elderly, those with disabilities, and others – are at risk of being left with little choice but to use Uber.

But what happens if Uber's monopolisation strategy fails – if its losses pile up and its pockets aren't as deep as they need to be. What if Uber goes under? In towns like Innisfil or in places where local taxis have been forced out of the market, Uber's demise would leave a vacuum, with no obvious replacement. Anyone who has come to rely on its services (whether by choice or necessity) would be out of luck.

---

[3] Goldstein, Michael. 2018. Dislocation and Its Discontents: Ride-Sharing's Impact On The Taxi Industry. *Forbes*. Available at https://www.forbes.com/sites/michaelgoldstein/2018/06/08/uber-lyft-taxi-drivers/#27acff5259f0 [accessed 13/09/2019].

[4] Cecco, Leyland. 2019. The Innisfil experiment: the town that replaced public transit with Uber. *The Guardian*. Available at https://www.theguardian.com/cities/2019/jul/16/the-innisfil-experiment-the-town-that-replaced-public-transit-with-uber [accessed 13/09/2019].

Uber is just one example of the risks of embracing a new technocapitalist elite motivated by short-term thinking and the desire to dominate markets in pursuit of profit and shareholder value. In Louisville, Kentucky, Google was contracted by the city to provide cheap fibre optic broadband to poorer areas where internet access was limited. It wasn't long before the cables – buried only two inches below the road surface to save money – became exposed and damaged. When Google decided that repairing the cables (and the roads) would mean that the service wouldn't be as profitable as they would like, they decided to abandon Louisville altogether, leaving the city to clean up the mess[5].

There are lessons here. We need to think more about the sustainability of tech-driven services, about alternative ways of doing things, about questions of power, profit, and trust – and, yes, about regulating where necessary. And we should be wary of allowing corporations to influence regulatory and policy decisions about the markets they're trying to 'disrupt' in their favour. Tech can offer great benefits, but the current paradigm risks enriching only companies, not empowering people. By considering more carefully our relationship with new and emerging technologies how best to realise their benefits, we as a society can move closer to the point where technology works for everyone.

[5] Raymond, Adam K. 2019. When Google Fiber abandons Your City as a Failed Experiment. *Gizmodo*. Available at https://gizmodo.com/when-google-fiber-abandons-your-city-as-a-failed-experi-1833244198 [accessed 13/09/2019].

Empowering Trust and Security from Hardware

Dr Franck Courbon
Department of Computer Science and Technology

Hundreds of microns thick, several millimetre wide, computer chips are everywhere and the heart of the devices we rely on every day. While their unit cost is very small (some tens of pence), they actually need to sustain a full spectrum of attacks, from software to hardware-based such as side-channel, fault and invasive attacks. On one hand, less critical data are stored on embedded devices and calculations may be directly performed on encrypted data. On the other hand, various hardware root of trust and technology/architecture (including countermeasures) are assumed secure.

Within the Department of Computer Science and Technology Security Group, with the need to understand weaknesses to improve matters, we also characterise low-level hardware features. A recent access to a multi-million pounds lab facilities will further help such hardware security research. From sample preparation (mechanical/chemical/plasma) to microscopy imaging (optical/electron/laser), in-depth silicon level analysis is added to our previous side-channel and fault attacks/testing capabilities. This initiative is interdisciplinary and includes various materials, chemistry, physics, electrical engineering and computer science aspects. While starting to gather large datasets, we are building in-house post-processing tools before exploring possible countermeasures. We complete such capabilities with access to state-of-the-art Focused Ion Beam (FIB) and XRAY facilities for nanometre scale integrated circuit modification and imaging.

At last, we are keen to announce the creation of a dedicated hardware

security teaching class for our postgraduate students, with unique data to play with and practicals to resolve.

Contact Franck: franck.courbon@cl.cam.ac.uk

S-Money

Prof Adrian Kent
Department of Applied Mathematics and Theoretical Physics

Together with my colleague Damian Pitalua-Garcia, I've been working on the theory and proof of concept implementation of "S-money"[1] -- a new type of money that allows users to make decisions based on information arriving at different locations and times. It also has the advantage of being secure against any code-breaking attacks, including possible new attacks using quantum computers. S-money gets its security from the combined power of quantum theory (roughly, from the fact that unknown quantum states can't be copied) and relativity (from the fact that signals can't be sent faster than light). It's designed allow faster and more flexible responses than any existing financial technology, by allowing instant authentication without any need to cross-check across a network that the money hasn't been duplicated and presented elsewhere – something that will likely be crucial as transactions become more automated and more time-critical. S-money could ultimately even make it possible to conduct commerce across the Solar System and beyond, without long time lags –though obviously this is a very long term (and perhaps optimistic) aspiration!

[1] Kent, Adrian. 2019. S-Money: virtual tokens for a relativistic economy. *Proceedings of the Royal Society* A 475 20190170.

At the heart of the scheme is a different way of conceptualizing money. S-money isn't something you can generally hold in one place, nor does it generally follow definite paths through space and time. One way of thinking about it is as something that "materialises" at a certain point in space and time, where the space and time coordinates of that point depend on real-time incoming data around (or beyond) the Earth.

Other researchers have developed theoretical frameworks for so-called "quantum money". This uses the properties of quantum information in a theoretically elegant way, but is presently technologically impractical, because it requires the long-term storage of quantum systems in a fixed state. In comparison, S-money needs a lot of fast information processing but no new technologies. Damian and I are working with colleagues in the UK Quantum Communications Hub to understand how feasible S-money is with current off-the-shelf computer technology.

One arguable advantage of quantum and relativistic cryptography is that they offer security that in some ways is more evidently trustworthy: the schemes are provably secure so long as the currently understood laws of physics are correct. Of course, though, users can't generally trust that a commercially available cryptosystem achieves (or even is designed to achieve) theoretically ideal security. Another long-term research project I've been interested in is designing and analysing so-called "device-independent" cryptographic schemes, which self-certify their security without relying on trust in the devices. These can significantly enhance trustworthiness but – long story short – are not perfect: all the known schemes still rely on some extra assumptions.

There's a broader question about these and other emerging quantum technologies: their benefits are well publicized, but we should also be asking whether they pose qualitatively new societal or even existential risks. I've begun working with colleagues in the Leverhulme Centre for the Future of Intelligence on a horizon-scanning project looking into this.

Lex Ex Machina: From Rule of Law to Legal Singularity

Dr Christopher Markou
Faculty of Law

Advances in Artificial Intelligence (AI), Machine Learning (ML) and data science are rekindling interest in applying computation to more aspects of legal process and decision-making. This is particularly evident through the development of various AI-leveraging LegalTech applications to assist with legal practice and business, law enforcement, and the prediction of case outcomes, among other things. The use of algorithmic decision-making (ADM) systems to replicate, and in some cases: replace, human judges and other decision-makers has, however, preoccupied the attention of the public, media, and scholars. Powles and Nissenbaum suggest that the 'seductive diversion' of solving the 'bias problem' makes the totalisation of AI in society contingent on solving narrow computational puzzles and 'ethics washing' away hard questions, bad business practices and worse ideas. Not more fundamental questions about the compatibility of autonomous systems with the rule of law, deliberative democracy, and ultimately: should we be building them at all?

While technical concerns about bias and transparency are clearly important, they should not detract from the fact that 'legal authority' is increasingly expressed and enforced algorithmically. As technology continues to replicate and replace more aspects of legal process and decision-making, the question becomes: is law computable? As a social system, legal norms, concepts, categories and reasoning are socially constructed. Can these be sufficiently captured by computation? If so, to what extent? What are the path-dependent and lock-in effects? But law also has an anthropological role, one aspect of which is safeguarding

against the potentially harmful and de-humanising effects of science and technology on the individual and society. To what extent can ‘legal authority’ or the ‘rule of law’ remain legitimate in the algorithmic language of 1’s and 0’s rather than through juridical reasoning expressed through natural language?

These questions become all the more acute in light of predictions of a forthcoming ‘legal singularity’—a hypothetical point where the functional capabilities of AI vastly exceed those of human judges and lawyers. In this world of a 'legal singularity' the law is said to exist in a perpetual state of equilibrium between facts and norms. However, the legal singularity is also a proposal for eliminating juridical reasoning as the basis for dispute resolution and the allocation of rights, responsibilities and power. Will this world of a legal singularity be one that even needs lawyers, judges, and indeed, the legal system as we currently understand it?

On December 13th I am hosting a conference at Jesus College entitled Lex Ex Machina that will bring together legal academics with researchers in STEM, the social sciences, policy makers, LegalTech developers and civil society organisations to explore these questions and what computable law means for the autonomy, authority, and legitimacy of the legal system as a social institution. Moving beyond narrow technical questions about bias and explainability, this workshop features contributions from leading interdisciplinary researchers that bridges technical and legal expertise, to examine questions at the intersection of law and computation.

Find out more: www.lexexmachina.org
Contact Christopher: cpm49@cam.ac.uk

Is Digital Security by Design Possible?

Prof Simon Moore
Department of Computer Science and Technology

As one of his last acts as Secretary of State for Business, Energy and Industrial Strategy, Greg Clark signed off on a new UK Industry Strategy Challenge Fund: Digital Security by Design. This £70m challenge fund is expected to be matched by funding of up to £117 million from industry. While a significant investment, it is dwarfed by the annual revenue of major big tech companies (Apple: $229b, Samsung $211b, Amazon $177b, Alphabet $110b, Microsoft $90b, Intel $62b, ARM $1.4b, etc.), so can it make a difference? I believe that it can because big tech. companies are driven to make money, often with short-sighted attention on earnings for the next quarter. Moreover, these companies operate in particular sectors with engineers working for these companies focusing their attention on improvement within these sectors: so, software companies improve the software and hardware companies improve the hardware, but rarely the two work on global optimisations/improvements. Even vertically integrated companies like Apple license processor technology or buy processor chips from ARM (for mobile phones) and Intel (for laptops and desktops).

The Common Vulnerabilities and Exposures (CVE) database records publicly known vulnerabilities and fixes. The number of CVE reports is growing at an alarming rate, fuelled by ever growing software systems that present an increasingly large attack surface, and mass connection of devices to the internet providing a conduit for attacks. I conjecture that we need a radical approach to reverse this alarming trend.

To fundamentally reduce the attack surface, we need to apply the *principle of least privilege*: code should be divided into compartments

with each compartment being given the least amount of privilege needed to perform its task. This fundamental approach is based on a 1960s idea, yet it is only deployed to a limited extent today; for example, each tab in web browser is run in a separate compartment but for performance reasons once there are thirty or so tabs open, tabs share compartments, potentially allowing your Facebook page to interfere with your online banking. Ideally not only would each tab have its own component, but each element needed to render the page should be in a compartment: every image and every fragment of JavaScript should be in a separate compartment. But today's hardware does not efficiently support this model, so software does not attempt to perform fine grained compartmentalisation. Since software does not perform fine grained compartmentalisation, hardware vendors do not optimise for it. This chicken and egg scenario has been played out for over a decade, with no signs of fundamental improvements being made by industry that fails to address fundamental challenges that require changes across the hardware and software divide.

Ransomware attacks are on the rise, paralysing critical public-sector functions. For example, WanaCry had a devastating impact on the NHS, taking down computer systems, which resulted in patients not being treated when medical records and test results became unavailable. The initial attack vector used is documented as CVE-2017-0145: Windows SMB Remote Code Execution Vulnerability. This is yet another example of a memory safety bug, specifically CWE-20: Improper Input Validation, that results in a buffer overflow. The buffer overflow vulnerability was first documented in 1972 and yet modern systems are still vulnerable. Our analysis indicates that much software vulnerable to buffer overflow at a machine code level (i.e. what a contemporary processor runs) is not inherently vulnerable at a source code level (i.e. what the human programmer wrote). The very process of transforming the human readable program code into machine code has introduced the vulnerability by failing to preserve the semantic intent the programmer

had when describing data structures. This leads us to the ideal of the *principle of intentional use*: processors need to be able to run software the way the programmer intended, not the way the attacker tricked it. Implementing the principle of intentional use also demands changes to both hardware and software.

To conclude, I am excited by the UK Digital Security by Design initiative and believe that there is a real opportunity to fundamentally advance hardware and software to efficiently embody the principle of least privilege and the principle of intentional use.

Institutions, Technology and Trust

Prof John Naughton
Centre for Research in the Arts Social Sciences and Humanities

A central question for researchers in this field is whether traditional concepts of 'trust' — which are rooted in ideas about the trustworthiness of *persons* — can be applied to *institutions* (government, regulators, legislatures, newspapers), or to *artefacts* (i.e. technologies).[1]The evolution of an increasingly networked world is throwing up interesting case studies which suggest that both issues of trustworthiness are coming to be inextricably linked.

Consider the case of Uber and Airbnb. These are online platforms which (respectively) put providers of mobility and accommodation services in

[1] Nickel, Philip J, Franssen, Maarten, and Kroes, Peter. 2010. Can We Make Sense of the Notion of Trustworthy Technology?. *Knowledge, Technology, and Policy* 23(3-4): 429-444. Available at https://link.springer.com/article/10.1007/s12130-010-9124-6 [accessed 13/09/2019].

touch with buyers who wish to avail of them. But what exactly are Uber and Airbnb selling? The conventional answer is: rides and rooms. But, as Henderson and Churi argue,[2] this is too simplistic. Uber doesn't own any cars or employ any drivers[3] and so is not really in the taxi business. "Instead, it sells a passenger the information she needs to trust a stranger to give her a ride. Specifically, it provides information on all nearby people willing to offer a ride and all nearby people seeking a ride, then efficiently matches passengers and drivers". Trustworthiness is supposedly delivered by a five-star rating system on both passengers and drivers. On this analysis, the competitors of Uber are not traditional taxi firms but the municipal regulators who license taxi operators and thereby ensure that these operators are fit and proper persons to carry passengers and are therefore trustworthy. Much the same analysis can be applied to Airbnb.

Another case study is provided by Facebook. Over the last two years the company has been beset by a series of scandals[4] involving data breaches, exploitation of its various services by political extremists and political actors (domestic and foreign). Controversies about these scandals — especially the revelations about Cambridge Analytica's

[2] Henderson, Todd M and Churi, Salem. 2019. *The Trust Revolution*. Cambridge University Press.
[3] Though the question of whether drivers should be regarded as employees is contested in some jurisdictions.
[4] Mahdawi, Arwa. Is 2019 the year you should finally quit Facebook?. *The Guardian*. Available at https://www.theguardian.com/commentisfree/2018/dec/21/quit-facebook-privacy-scandal-private-messages [accessed 13/09/2019].

exploitation of user data — initially appeared to have dented users' trust in Facebook, but it's not clear[5] whether it led many to stop using it.[6] But when Facebook launched its Libra cryptocurrency project in July 2019, the proposed design[7] suggested that the company understood that it suffered from a trust deficit. The currency would be 'stable' — backed by a basket of currencies and security instruments managed by an 'association' of up to 100 other organisations of which Facebook would be only one. Libra was a cryptocurrency because that would ensure that Facebook was not in control of the validation of transactions.[8] And although the company would create its own Calibra wallet, other organisations would be free to create competing wallets. So — the argument ran — the currency project would not be dominated by Facebook.

---

[5] Sterling, Greg. After a week of crisis and mea culpas, assessing the threats and exposure. *Marketing Land*. Available at https://marketingland.com/after-a-week-of-crisis-and-mea-culpas-from-facebook-assessing-the-threats-and-exposure-236937 [accessed 13/09/2019].

[6] A Pew survey conducted in 2019 found that 69% of Americans continue to use the service, three quarters of whom visit the site at least once a day. On the other hand, 54% of adult users have adjusted their privacy services following the Cambridge Analytica revelations. See Gramlich, John. 2019. 10 facts about Americans and Facebook. Pew Research Centre. Available at https://www.pewresearch.org/fact-tank/2019/05/16/facts-about-americans-and-facebook [accessed 13/09/2019].

[7] Libra. 2019. *The Libra Blockchain*. Available at https://libra.org/en-US/white-paper/#the-libra-blockchain [accessed 13/09/2019].

[8] In fact, Libra — unlike, say, Bitcoin — is based on a "permissioned" blockchain: transactions are validated not by mining but by designated 'validators'. Whereas 'pure' blockchains avoid the need for a central validating authority by essentially de-centralising the task (thereby solving the 'trust' problem), Libra deals with the trust issue by nominating a set of up to 100 validators, all of whom are members of the Libra Association. See Halpern, Sue. 2019. Facebook's audacious pitch for a global cryptocurrency. *New Yorker*. Available at https://www.newyorker.com/tech/annals-of-technology/facebooks-audacious-pitch-for-a-global-cryptocurrency [accessed 13/09/2019].

These arguments cut no ice with the Congressional Committee which grilled[9] the Facebook executive leading the Libra project. The general tone of the Hearing was, as the ranking Democrat on the Committee put it, that it was 'delusional' for Facebook to think that people would trust it with "their hard-earned money". So Facebook's strategy for addressing its trust deficit by both technical (blockchain) and institutional (Libra Association) means appeared to have stumbled at the first regulatory hurdle. It will be interesting to see how this pans out.

Compliant and Accountable Systems

Dr Jat Singh
Department of Computer Science and Technology

Data-driven technology increasingly underpins everyday life. But what happens when it fails? Who is, or should be, responsible, given the complexity of these systems and their supply-chains? How do we hold those responsible to account when things do go wrong? What is needed to govern the development and use of technologies so that they better accord with social values?

These socio-technical questions are particularly pertinent as systems become more pervasive and complex; technical environments increasingly data driven, autonomous and physical; and as the grand visions of smart cities, the Internet of Things, and of course, "AI" become a reality.

---

[9] CNBC. 2019. *Facebook's David Marcus testifies before Senate on Libra cryptocurrency* [video]. Available at https://www.youtube.com/watch?v=xUQpmEjgFAU [accessed 13/09/2019].

In line with this, technology and its impact on society are the subject of much public discussion and regulatory attention – the EU's General Data Protection Regulation is a prominent example. There is growing demand for better accountability regarding the technology that influences everyday life, not least given the scandals now being reported almost daily.

Addressing issues of accountability and legal compliance of new and emerging technologies can help ensure that those technologies are built and deployed in alignment with social norms, that they remain appropriate and fit for purpose, and that those responsible can be held to account as and when necessary.

Towards this, the *Compliant and Accountable Systems research group* considers how to better align technology with legal and policy concerns, and vice-versa. The team, based at the Department of Computer Science & Technology (Computer Laboratory), is multi-disciplinary, with its members having backgrounds in computer science, law, and policy. Our research involves analyses and interventions—both technical and legal—in areas around governance, agency, empowerment, compliance, and accountability as they relate to new and emerging technologies. Some current research themes include: engineering for rights, centralisation vs decentralised data/compute, the reviewability of the design and use of machine learning, issues of online content distribution, and meaningful audit and interrogation of complex systems, to name a representative few.

Find out more about the group and its research: www.compacctsys.net

Smart Urbanism and Mental Health in Singapore

Aisha Sobey
Department of Architecture

Digital technologies are quickly being embedded in urban processes, yet there has been little investigation into the impact this is having on mental health and wellbeing. The ties between environment and mental health have been demonstrated[1], but the way space and life is conceptualised is being challenged by digitisation. New facets to life such as online communication, surveillance and data collection create new ways of experiencing space which spatial theory must engage with to adequately understand the digitally mediated age. To investigate the role of smart urbanism in mental health outcomes, this research will combine the discursive lens of 'fourthspace': "the intersection of the digital, real and imagined worlds"[2] with Lefebvre's perception of public spaces[3], to offer a way of conceptualising the different dimensions of space and separation between policy aims and lived experience.

---

[1] Goldhagen, Sarah. 2017. Welcome to your world: How the Built Environment Shapes Our Lives. New York: Harper Collins Publishers; Goldhagen, Sarah. 2018. What is Human-Centered Design? Should Anyone Care?. *Journal of Urban Design and Mental Health* 5(2). Available at: https://www.urbandesignmentalhealth.com/journal-5---human-centered-design.html [Accessed 29 Aug. 2019]; Gruebner, Oliver, Rapp, Michael, Adli, Mazda, Kluge, Ulrike, Galea, Sandra. and Heinz, Andreas. 2017. Cities and Mental Health. *Deutsches Aerzteblatt International*. Available at https://www.aerzteblatt.de/int/archive/article/186433/Cities-and-mental-health [accessed 13/09/2019].
[2] Kong, Lily and Woods, Orlando. 2018. The ideological alignment of smart urbanism in Singapore: Critical reflections on a political paradox. *Urban Studies* 55(4): 679-701.
[3] Lefebvre, Henri. 1991. *The production of space*. Oxford: Blackwell.

In a recent study looking at spatial interventions in NY public schools to improve mental wellbeing, they found that from the fifteen schools that had interventions, those with the most robust community partnerships, engagement and context specific design, resonated best with the community in which they're situated and had the most impact[4]. It is only with the support of all three of Lefebvre's dimensions of space that the produced space had the desired outcome. Through applying this understanding of traditional, physical space, to fourthspace - a reconfiguration of space including the digital- the perceived, conceived, and lived experiences of the digitally mediated world can be separated highlighting important divisions between types of technologically mediated space. Policy areas understood through this framework, will then be assessed against the five ways to wellbeing[5], identified by the Institute for Development Studies: Connect, Be Active, Take Notice, Keep Learning, Give. These offer a way of discerning the positive and negative implications on mental health.

One key area which this research hopes to question, is how technological systems relate to trust, and feelings of autonomy in life which impacts on mental wellbeing. Sensors embedded into all aspects of life in a smart city, also create unimaginably large amounts of data. Where this is stored, who has access and how it is used creates vast asymmetries of information and the rationale behind decisions produced

---

[4] Peterman, Kelli, Jackson, Nivea, Ortiz-Rossi, Monica, Shaff, Jamie, Hernandez, Yianice, White, Takeesha, and Swenson, Theodora. 2018. Mental Health by Design: Fostering student emotional wellness in New York City high schools by improving and enhancing built environments. *Journal of Urban Design and Mental Health* 5(5). Available at: https://www.urbandesignmentalhealth.com/journal-5---nyc-school-design-for-mental-health.html [Accessed 29/08/2019].

[5] Aked, Jody, Marks, Nic, Cordon, Corrina, & Thompson, Sam. 2008. *Five ways to well-being: The evidence*. London: Report commissioned by the Foresight Project on Mental Capital and Well-being.

with this information can be exceedingly unclear. The “black box” effect[6] offers the illusion of technological neutrality to obfuscate decisions removing autonomy due to the disambiguation of outcomes, where the internal logic is not available for inspection or review. Caught in this web of unquestionable decisions, creates feelings of powerlessness in citizens and is expected to exacerbate a degeneration of mental wellbeing. Through considering the representational space using surveys and interviews, focussed on the digital natives, it will evidence the way these spaces are impacting on mental health. This research will focus on Singapore as its case study, using the highly advanced smart urbanism employed there, to answer “Will a smart urban future exacerbate mental health issues?”

Contact Aisha: as2713@cam.ac.uk

[6] Holzinger, Andreas, Palade, Vasile, Plass, Markus, Holzinger, Katharina, Crisan, Gloria Cerasela and Pintea, Camelia-M. 2017. A glass-box interactive machine learning approach for solving NP-hard problems with the human-in-the-loop. *Cornell University Computer Science Lab*. Available at: https://arxiv.org/abs/1708.01104 [Accessed 19/09/2019].