InspiredResearch Summer 2021 Issue 18

News from the Department of Computer Science, University of Oxford

Satellite Hacking:
Researching Cyber Space

Read more – p20

Oxygen Delivery in Tumours:
New predictive model created by international team – p13

COVID-19 and increases in cyber-attacks:
How criminals have exploited the pandemic – p16

WatchDog:
New tech to protect vulnerable users against telephone fraud – p24

University of Oxford

Department of Computer Science

compscioxford CompSciOxford CompSciOxford

Inspired Research

is a twice-yearly newsletter published by the Department of Computer Science at the University of Oxford.

If you would like to learn more about anything you read in these pages, please get in touch: editorial@cs.ox.ac.uk

To subscribe to future issues, e-mail: editorial@cs.ox.ac.uk

To download previous issues, visit www.cs.ox.ac.uk/inspiredresearch

Editorial board

Contributors

Emma Dunlop,
Jack Jackson,
Francesca Margara,
Ines Marusic,
Tom Melham,
James Pavur,
Jan Pich,
Joe Pitt Francis,
Pericle Salvini,
Oliver Sampson,
Arianna Schuler Scott,
Claudine Tinsman,
Michael Wooldridge,
Jun Zhao

Photographs in the newsletter are used for illustrative purposes and may have been taken before COVID-19 restrictions came into force

CONTENTS

Letter from the Head of Department

As I write this I am in my final term as Head of Department, after seven years at the helm. It seems appropriate, therefore, to reflect on our journey as a department since I took over in 2014, and see how we have developed since then. The picture is, I think, quite remarkable.

First, we restructured our research groups into 10 areas, establishing three fundamentally new research themes: Artificial Intelligence & Machine Learning, Cyber-Physical Systems, and Human-Centred Computing. We obtained a staggering £74m of external research income over the period, and received £17m in philanthropic donations, including substantial donations for a planned new building and a new chair (the DeepMind professorship of AI – currently underway). We hired Sir Tim Berners-Lee, inventor of the World-Wide Web, and thirteen other academics besides; 12 of our staff were awarded the title of full professor. One of us received the ACM Turing Award (the highest international honour for a computer scientist); three were elected fellows of the Royal Society, and a further three were made fellows of the ACM; five received the Lovelace Medal from the British Computer Society (the highest UK honour for a computer scientist). We have received endless other awards besides, for work ranging from the logical foundations of computing to computational simulations of drugs to reduce animal testing.

We have substantially grown our undergraduate base, with 11 completely new tutorial fellowships created in the period, and a further two agreed. Applications to our undergraduate taught programmes have continued to rise year-on-year, to the point where we are now receiving more than 20 applicants for every place on our single-honours computer science degree. *Twenty applicants for every place!* Our doctoral programme has also continued to grow: we have awarded 242 doctoral degrees since 2014, nearly twice as many as in the equivalent period preceding this. We currently receive some 400 applications annually for our doctoral programme, and typically offer about 50 places.

Activity around the commercialisation of research has expanded hugely. Since 2014, our spinout companies have raised over £50m in investment, and several have been acquired by major international companies, including GitHub, Meltwater, and Waymo (following their acquisition of Latent Logic, Waymo established a research lab in Oxford, the first research base for this company outside the USA).

External confirmation of our quality comes from many sources. In the *Times Higher Education World University Subject Rankings*, we were placed 1st in the world for Computer Science in two out of the last three rankings. The *QS World University Subject Rankings* placed us 7th in the world for Computer Science and Information Systems in both 2017 and 2018, 6th in 2019, and 5th in 2020.

I could go on, but I really don't think I need to: the picture is clear. I am proud to have been head of such a vibrant and active department at such an extraordinary time for our discipline. I think Oxford is the most exciting place to be a computer scientist in Europe right now, and I am pleased to be leaving my role as Head of Department in such rude good health. My successor, Professor Leslie Goldberg, will take over on 1 October 2021, and I know she has a raft of exciting new ideas for advancing the department. The next seven years are shaping up to be every bit as exciting as the past seven.

Professor Michael Wooldridge
Head of Department of Computer Science
June 2021

NEWS

MPLS Impact Awards 2021: winners and commendations announced

Each year the Mathematical, Physical and Life Sciences division (MPLS) runs a competition which recognises the impact of research undertaken by researchers. Impact Awards are open to MPLS researchers at all career stages – from DPhil students to senior academics. Nominations are made across four impact categories: commercial, social, early career and public engagement with research. The Department of Computer Science has done exceptionally well this year.

Associate Professor Kasper Rasmussen won the Commercial Impact category, for his research on 'Resolution of Multiple Critical Design Flaws in Bluetooth Standard'. Kasper lead research on weaknesses in wireless protocols which uncovered critical flaws in multiple parts of the Bluetooth standard (as implemented in billions of devices worldwide), demonstrating how both the Bluetooth session key establishment and the authentication procedures can be completely compromised. The research team coordinated with key industry bodies to disclose each vulnerability, allowing them to be remedied before they could be abused. The work led to changes to the Bluetooth Core Specification, and to mitigations applied by major manufacturers.

Professor Michael Wooldridge, Head of the Department of Computer Science, said: 'Kasper and his colleagues discovered a jaw dropping bug in the Bluetooth protocol, used by hundreds of millions of people every day. Their discovery necessitated a change to the protocol, and firmware updates for billions of devices. It is wonderful work, and one of the clearest examples of impact I've seen during my seven years as head.'

Members of the department were also awarded commendations in the Commercial Impact category as follows:

Professor Georg Gottlob: Efficient Web Data Extraction and Knowledge Processing via Datalog
Georg's research at Oxford has led to fundamental advances in efficient reasoning languages and their application to web data extraction and management. Systems developed as part of this research led to two spinout companies, Wrapidity and DeepReason.ai.

Professors Bernardo Cuenca Grau, Ian Horrocks, Boris Motik: Enabling Applications of Ontologies in Healthcare and in Industry via Reasoning Systems
The researchers have developed state-of-the-art reasoning systems that represent important advances in exploiting the potential of semantic technologies for complex data and knowledge applications. Their open source reasoning tools are enabling applications of ontologies in areas as diverse as global healthcare IT and large-scale infrastructure design. They have also developed and commercialized RDFox, a high-performance knowledge graph and semantic reasoning engine, through the spinout company Oxford Semantic Technologies (OST).

Professor Niki Trigoni: Improving Workforce Efficiency in Hospitals via Infrastructure-Free Indoor Localisation
Niki's research group developed a frictionless infrastructure-free indoor positioning solution based on smartphones, which avoids the significant cost and effort required to deploy existing indoor location-tracking solutions. The patented technology underpins the spinout Navenio, founded by Niki in 2015. Navenio has applied the technology in multiple NHS trusts to build a workforce tracking and tasking solution.

Professor Michael Wooldridge wins 2021 Outstanding Educator Award

The Association for the Advancement of Artificial Intelligence (AAAI) and the Symposium on Educational Advances in Artificial Intelligence (EAAI) have announced that the 2021 AAAI/EAAI Outstanding Educator award was given to Professor Michael Wooldridge of the University of Oxford and The Alan Turing Institute.

The AAAI/EAAI Outstanding Educator was established in 2016 to recognise a person (or group of people) who has (have) made major contributions to AI education that provide long-lasting benefits to the AI community.

Michael received this award for outstanding global leadership in AI education and public awareness, including publishing broadly adopted books and textbooks, establishing the European Agent Systems Summer School, and inspiring public dialogue on AI and multi-agent systems.

'I'm extremely grateful, and it's an unexpected honour,' Michael said of the award at the beginning of his invited talk at EAAI-21, titled 'Talking to the Public about AI'. During his talk, Michael focused on his experiences talking to a variety of non-specialist audiences about Artificial Intelligence. He shared what he learned about how the field is perceived, and his recommendations for how best to communicate excitement about the progress we've made, where we are, and where we are going.

The talk is publicly available on the EAAI-21 conference website. The award consists of a certificate, a US $1,000 honorarium, a one-year AAAI membership, and a conference registration to the EAAI/AAAI conference, where the award was conferred.

For more information aaai.org/

Projects funded by the EPSRCs Impact Acceleration Account

A number of projects from the Department of Computer Science have recently been awarded funding from Oxford's Engineering and Physical Sciences Research Council (EPSRC) Impact Acceleration Account (IAA), which provides support to accelerate and amplify the impact arising from research that falls within the EPSRC's remit. Those receiving funding most recently from the IAA at the Department of Computer Science have included:

Professor Michael Benedikt, for an IAA Partnerships project, 'From reasoning to neuro-symbolic AI for knowledge graphs and vision'. The project, in collaboration with industry partner Samsung AI Center Cambridge, will explore how neuro-symbolic AI can enhance the performance of symbolic reasoning systems for applications such as knowledge graph querying and scene recognition.

Alfonso Bueno-Orovio, for the project 'In silico clinical trials for precision medicine in genetic heart disease', which aims to integrate modelling and simulation technologies developed in Oxford research within the drug assessment pipeline of industry partner MyoKardia (recently acquired by Bristol Meyers Squibb). As part of this Doctoral Impact IAA award, current DPhil student Francesca Margara will spend time on secondment at MyoKardia in California.

Professor Tom Melham, together with collaborators Professor Rebecca Williams and Václav Janeček in the Law Faculty, for a project that will scale up the Oxford LawTech Education Programme (OLTEP). This research-led, non-degree education offering aims to amplify the positive impact of digital technology in the legal sector, and to meet the urgent professional learning needs of today's lawyers. The training programme, which has already been successfully piloted – with participation by over 700 UK lawyers – will help to foster technological innovation and shape digital leadership in tomorrow's law firms and public sector organisations.

You can read more about the collaboration with the Law Faculty on page 8.

Professor Georg Gottlob joint winner of 2021 Alonzo Church Award

Professor Georg Gottlob (together with co-authors Christoph Koch, Reinhard Pichler, Klaus U. Schulz, and Luc Segoufin) has won the prestigious Alonzo Church Award. The award was made for fundamental work on logic-based web data extraction and querying tree-structured data.

The Alonzo Church Award for Outstanding Contributions to Logic and Computation was established in 2015 by the Association for Computing Machinery (ACM) Special Interest Group for Logic and Computation (SIGLOG), the European Association for Theoretical Computer Science (EATCS), the European Association for Computer Science Logic (EACSL), and the Kurt Gödel Society (KGS). The award is for an outstanding contribution represented by a paper or small group of papers within the past 25 years. Professor Samson Abramsky, Professor Luke Ong, and Lecturer Hanno Nickau (together with their co-authors) won the same award in 2017.

News in brief

The *Times Higher Education* 2021 league table features the University of Oxford as one of the best universities in the UK for Computer Science! The article can be viewed here: bit.ly/3pYqnIo

Sir Nigel Shadbolt spoke at the launch of the Ethics in AI institute. The talk can be seen here: bit.ly/35sjl5d

Professor Marta Kwiatkowska gave this year's British Computer Society Lovelace lecture, titled 'Probabilistic model checking for the data-rich world' in May. The talk is available online at bit.ly/3wmPW85

Professor Niki Trigoni's Navenio has been chosen to join the exclusive Tech Nation Upscale 6.0 programme. The full article can be read here: bit.ly/3iJHmwp

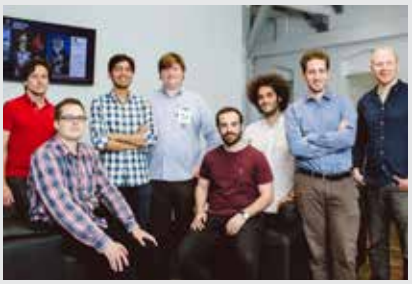
Julià Camps has been awarded an Engineering and Physical Sciences Research Council Doctoral Prize to increase the impact of his DPhil, titled Bayesian inference and Machine learning methods for the advanced analysis of electrocardiographic signals. This prize includes nine months of salary for Julià to stay as a postdoctoral researcher in the Computational Cardiovascular research group at the University of Oxford.

NEWS

News in brief

Professor Niki Trigoni answers questions about Navenio, a spinout from the Department of Computer Science. You can see the written interview here: bit.ly/3xhq9yo

Department alumnus Yannis Assael has been featured in Forbes 30 under 30 list for Europe, in the Science and Healthcare section. Yannis is now a Senior Research Scientist at Google DeepMind, where he uses machine learning to address AI challenges. Yannis undertook both an MSc and his DPhil (PhD) in the Department of Computer Science. More here: bit.ly/2StJL3I



National Review had plenty of positive things to say in their review of Professor Michael Woolridge's book 'A brief history of Artificial Intelligence: what is it? where we are and where are we going': bit.ly/3vrh2dc

Professor Michael Wooldridge takes part in a podcast about AI for *The Economist*. Listen here: t.co/1q5MnW942O?amp=1

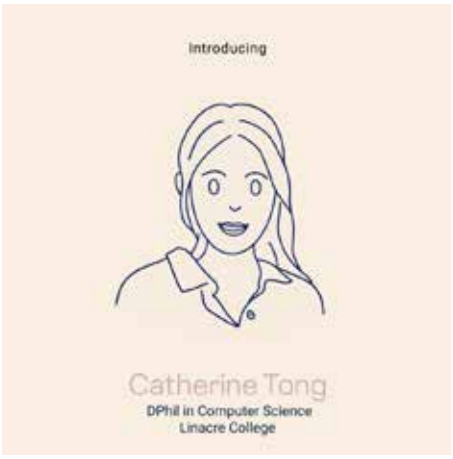
Many congratulations to Ani Calinescu and Joe Pitt-Francis, both of whom have been awarded the title of Associate Professor. Head of Department Michael Wooldridge commented 'I'm delighted to see you recognised in this way'.

We are thrilled that The Complete University Guide has ranked us as the top university in the UK for Computer Science, in their 2022 league tables.

Female Faces of Computer Science

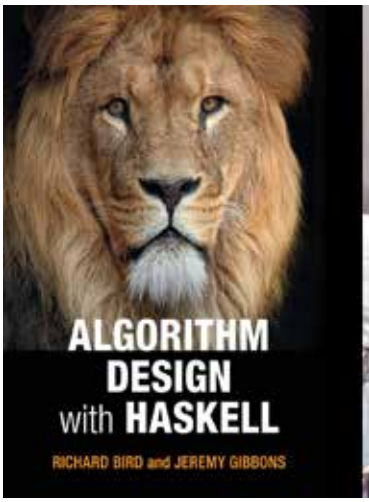
At the start of 2021 the Oxford Women in Computer Science Society, in collaboration with the Department of Computer Science, launched the #FemaleFacesofComputerScience campaign. This is the first collaborative campaign between the department and the society with the aim to inspire others looking to pursue a career in the field of Computer Science. The campaign highlights the achievements of some of our computer scientists at Oxford, all at various stages in their careers. It is centred on a series of interviews with some of our current computer scientists giving insight into the lives and contributions of so many accomplished women in the field of Computer Science.

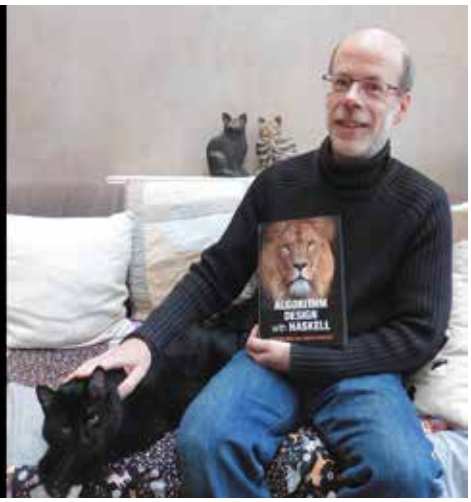
A selection of posts have been included below. You can see the full campaign here: instagram.com/compscioxford/



World Book Day

World Book Day is an annual event that most people associate with young kids dressing up as their favourite book character. However, it's also a day that celebrates authors, and the Oxford University community has a huge number of authors writing on a fascinating range of subjects. Members of the department took part in the University's #OxfordUniAuthors campaign, celebrating the books written by members of our Department with selfies on Twitter. Members of the department that took part include Professor Mike Wooldridge, Professor Tom Melham, Kiri Walden, Graham Lee, Professor Standa Živný and Professor Jeremy Gibbons, pictured here in his fantastically-styled Twitter selfie.





Xin Zhou awarded Oxford-Bristol Myers Squibb Fellowship

Congratulations to Xin Zhou, who has been awarded one of five Oxford-Bristol Myers Squibb fellowships. The fellowships (representing an investment of £3M) will support postdoctoral researchers and clinicians across five departments within the Medical Sciences Division and the Mathematical, Physical and Life Sciences Division, providing an opportunity for them to gain exposure to the field of commercial drug discovery and development.

Bristol Myers Squibb focus on the discovery, development and commercialisation of innovative therapies for patients with cancer, immune-inflammatory and other unmet medical needs.

Now in its 6th year, the Oxford-BMS Fellowship Programme stimulates new scientific discovery and translation and facilitates skills and people transfer between researchers at Oxford and Bristol Myers Squibb (BMS). Oxford's relationship with BMS continues to grow year on year, with the new Fellowships taking the total of Oxford-BMS Fellows to 28.

Fellows carry out a three-year postdoctoral research project and have a high level of support available through the direction and mentorship of BMS project leads. Both BMS and the University draw value from the

opportunity to facilitate the transfer of skills between researchers in academia and those in industry to stimulate new scientific discovery and translation. The Fellows also have opportunities to carry out research and utilise facilities at BMS labs in the US and Spain, in addition to accessing unique training opportunities.

Xin Zhou will carry out her project under the supervision of Professor Blanca Rodriguez in the Department of Computer Science. Blanca (Principal Investigator) comments, 'We are very excited about this new Oxford-BMS collaboration on modelling and simulation for target identification and evaluation in heart failure.'

Xin Zhou says, 'The Oxford-BMS fellowship will be a great opportunity for me to dive deeper into the scientific research of heart failure and to know more about target identification in drug development at BMS through working closely with my mentors.'

Cyber Security Alumni Network

A new alumni network is being launched to connect Oxford alumni working in (or interested in) the cyber security field – regardless of what you studied at Oxford. We are looking for alumni who have moved into the cyber security field, but who may not have necessarily undertaken a technical course at Oxford.

This reflects the multidisciplinary nature of the academic network, with academics in 20+ departments across the university from Engineering to Politics to Geography.

If alumni would like to be included in future conversations they can sign up to our mailing list by emailing: enquiries@cybersecurity.ox.ac.uk

More details can be found here: cybersecurity.ox.ac.uk/alumni

News in brief

Designed to support women seeking careers in technology, Booking.com's STEM scholarships have enabled 10 graduates from Europe to study Maths, Statistics and Computer Science at the University of Oxford. The company's chairwoman, Gillian Tans, updates us on their progress: lnkd.in/er9bWFd

Congratulations to Arianna Schuler Scott for winning the best poster prize at the Sprite+ Showcase Research Snapshots! The poster can be viewed here: bit.ly/3vsu0qS

Alumna Chao Mbogho has given an inspirational TEDTalk describing her career journey to the University of Oxford and her subsequent life as a computer scientist. Watch it here: bit.ly/3hWT5Hn

Professor Marina Jirotka took part as a speaker at an All-Party Parliamentary Group on Data Analytics round-table discussion called 'Rebuilding Trust in Algorithms'. During the event Marina said, 'There can be no one size-fits-all for establishing trust in algorithms... Trust lies in citizens' understanding in the purpose of the system and how their data is used being by organisations'.

Professor Sadie Creese was interviewed by BBC Radio 4 for an episode of 'The Briefing Room' about the threat of ransomware attacks. The episode covered what the attacks are, how they work, and how dangerous they could be. bbc.in/3paXXu6

At the intersection of Law and Computer Science

Through research-led design of an innovative master's-level course, academics from the Department of Computer Science and the Faculty of Law are closing the gaps in mindset, skill, and knowledge that exist between students from the two disciplines. Oxford's 'Law and Computer Science' course has attracted support from a range of senior industry mentors and sponsors. The research group behind the course is now developing a practice-oriented, online non-degree education programme and gathering evidence for a full MSc in Law and Computer Science.

For the second consecutive year, an exclusive group of students from the Department of Computer Science and their peers from the Faculty of Law have taken part in the interdisciplinary Law and Computer Science course. The course stems from world-leading research (bit.ly/3tGtrdf) into the use of AI in the provision of legal services and related research into the mindset, skill and knowledge gaps between lawyers and computer scientists. This has enabled the Oxford academic team to create a unique course at the intersection of the two disciplines.

The course has both a practical and a theoretical stream. The former requires the students to develop a techno-legal solution to a real-world problem, benefiting from technical supervision by leading Oxford researchers. This year, the project work of all participants in Law and Computer Science was also supported by a group of industry mentors and sponsors, who shared practical insights, data, and technical tools. Five projects were undertaken by students, based on either smart contracts and blockchain technology; or natural language processing. The pedagogical aim of these practical projects is to teach lawyers and computer scientists how to work together productively—a skill that will be needed by graduates of both disciplines working in law firms and public-sector legal bodies of the future.

The theoretical stream offers the students a unique opportunity to engage in discussions (a feature not typical of Computer Science courses) based on wide reading and research-led presentations by academics from both departments. The first block of these theoretical sessions is designed to introduce the two disciplines to each other and to encourage them to think about the similarities and differences between the two fields and between the professionals working in those fields. The second block of theoretical sessions is devoted to examining how technology can automate and augment legal practice and what the ethical and other challenges of doing so might be. In the third block, the students are introduced to a different substantive area of Law each week and asked to examine how the use of technology will raise new challenges for that area of Law and how practitioners of Computer Science and of Law might be expected to work together to solve those challenges. The final block, comprising a single session, concludes the course by bringing together some of the key concepts and strands encountered throughout the course.

At the end of the course, the students also present the results of their hard work in a session modelled on a start-up company pitch for seed investment to over thirty experts from across industry, academia, and venture capital investment. The products and services – wholly conceived, designed, and created by the project teams this year – were these:

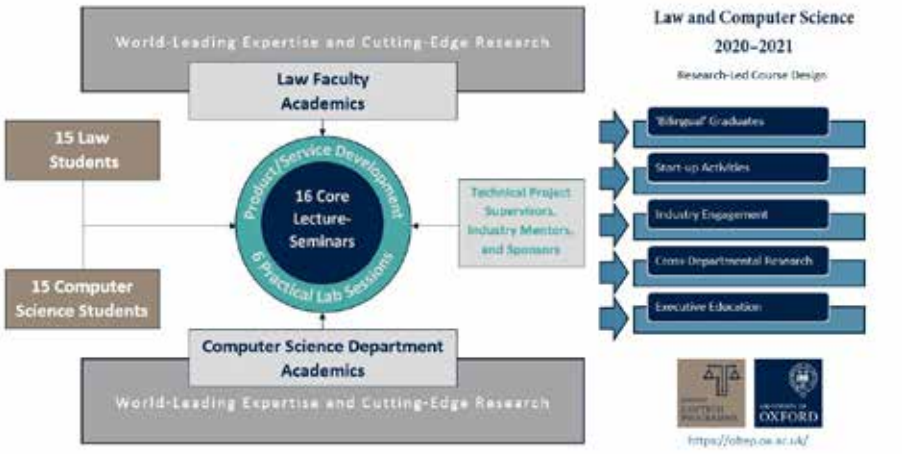
* Natural Language Processing (NLP)-powered service to summarise key clauses in Limited Partnership Agreements,

* Blockchain-based authentication tool to fight counterfeit luxury goods,

* NLP-based named-entity recognition service for court judgments,

* Privacy-preserving and NHS-verifiable Track & Trace app for venues,

* NLP-powered analytic tool to identify boilerplate clauses and determine their risk-score.



continued on next page ▶

from previous page ▶

The audience included Professors Richard Susskind OBE, John Armour and Ewart Keep, and Dr. Anna Donovan; together with representatives of Allen & Overy, Slaughter and May, Thomson Reuters, Latham & Watkins, Clifford Chance, and Oxford Sciences Innovation. The attendees were impressed by the student projects in particular how professional and sophisticated the projects were in their conception, execution, and presentation. In the words of Professor Susskind, this was 'a great session. Brimming with energy, insight, and a few ideas that I can imagine attracting investment. A triumph of inter-disciplinary teaching and collaboration.'

Indeed, the entrepreneurial nature of the course and the research behind it has also led to the establishment of the practice-oriented Oxford LawTech Education Programme (OLTEP), a joint initiative by the Oxford Law Faculty and the Oxford Department of Computer Science. OLTEP's mission is simple: to train future leaders in the legal market, confident providers of tech-enhanced legal services and successful innovators who can spot, analyse and utilise trends in digital technology.

Based on their research into the skills gaps, the Oxford team has developed a series of pilot learning units in collaboration with several organisations, including Slaughter and May, and the Government Legal Department. Over the last few months, over 700 participants from the profession have now attended the pilot programme. The participants highly praised 'the myth-busting and no-nonsense approach' of this innovative educational offering.

Over the next 12 months, OLTEP will be expanded into a full non-degree education programme for public and private sector lawyers. As announced elsewhere in this issue (page 5), OLTEP has gained funding from Oxford's EPSRC Impact Acceleration Account to support this development.

If you want to learn more about the course or are interested in sponsoring opportunities, do not hesitate to get in touch with our team: Professor Rebecca Williams (Professor of Public Law and Criminal Law), Professor Tom Melham (Professor of Computer Science), and Václav Janeček (Research and Course Development Fellow in Law and Technology).

Another successful year of undergraduate group projects in collaboration with industry affiliates

Each year members of the Department of Computer Science work collaboratively with industry affiliates and small teams of undergraduate students to produce software solutions to a variety of real-world industry supplied questions. Students in their second year of a Computer Science degree are given a choice of project briefs which vary from financial and trading right through to environmental and educational.

Students work on projects with their industry sponsor for around two months alongside their studies in Hilary term (spring term), culminating in a presentation day where teams present the final software solution to their peers, academics and invited industry affiliates. Many industry affiliates this year noted the positive interaction with the students and expressed an interest in connecting with members of their team for future projects and internships. Industry projects are one of the best ways for industry affiliates to network with undergraduate computer scientists for future initiatives.

Prizes are awarded to the teams who present the best overall solution, best presentation and best technical execution, as judged by a panel of academics and invited industry affiliates. The prizes awarded this year were;

- The prize donated by Fetch.AI was awarded to Team 13 (Project in collaboration with Earth Trust) for a fantastic presentation and a practically useful tool to assess the impact of climate on different tree growing strategies.
- The prize donated by G-Research was awarded to the Team 12 (Project B: Web-based Editors simulation of C/C++ code and Python | Project in collaboration with Micro:bit Educational Foundation) for a well-designed educational tool they created and a clear presentation and demonstration on how this tool can be used for learning purposes.
- The prize donated by the Department of Computer Science was awarded to Team 6 (Project E: AI Racing Market | Project in collaboration with G-Research) for the excellent technical execution of the project and the engaging physical environments they created.

We would like to thank this year's industry affiliates, Fetch.AI, G-Research, Tradeteq, Earth Trust, Micro:bit, Apex:E3 and Bloomberg for their continued support despite COVID restrictions.

For information on participating in next year's event and any other industry affiliate benefit please email industry@cs.ox.ac.uk and also visit bit.ly/34ELw0h

Re-working informed consent in research: engage, include, and respond

by Arianna Schuler Scott (Doctoral Researcher in Cyber Security, University of Oxford).

Researcher A uses an informed consent form to show that she has asked for Person B's permission to put them at risk of harm. In any other situation, Person B might refuse, but Researcher A is carrying out a vaccine trial and Person B believes that taking part will work towards a greater good. Informed consent was originally designed to protect against physical, rather than digital, harm.

As research moves online, fundamental issues with informed consent have become magnified: online consent options tend to overload readers with information (Obar and Oeldorf-Hirsch, 2018), and are designed to coerce the reader into making immediate judgements without understanding the information provided.

As researchers, we design our own informed consent processes, so we are responsible for how different options are presented. We act as 'choice architects'. Online informed-consent processes normalise information overload and consent fatigue, which violates the original purpose of informed consent: to protect. Someone giving consent makes a decision to trust whoever is asking for that consent, and this decision relies on perceptions of transparency and accountability.

Even in a sector as highly regulated as research, there are fundamental problems with informed practices, as participants can rarely recall basic information about a study. What we call 'informed consent' is unfit for purpose.

Fortunately, researchers can demonstrate transparency and accountability using inclusive and responsive practices. Figure 1 (below) provides examples of such practices, from my own work.

When sharing information, participants are happy to delegate subject-specific knowledge to domain experts, but prefer to retain overall control of how they take part. As a cyber security specialist, I focus on data protection and privacy. These ideas are central to informed consent because individuals are often asked for their consent to unspecified secondary data-uses.

Even though we do not always know how we might use data in the future, as researchers we can build notifications into research protocols. Where data is re-used, research participants want to know what is going on. Informed consent processes are not the only time information can be provided to, and sought from, participants. Inclusive and responsive practices can be woven throughout the work that we do.

My DPhil work has focused on the use of dynamic consent, which aims to inform participants over time, updating the information they have access to. I carried out a service evaluation of dynamic consent in practice and found that enhancing the available feedback, providing information about how personal data was used, enriched data-collection (see Figure 2).

The project I worked with, the Rare and Undiagnosed Diseases studY (RUDY), launched in 2014 and is a study on rare genetic conditions. Rare conditions, (sometimes called 'health orphans' because knowledge of causes and effective therapies are limited) are particularly problematic because they are under-researched. There is little data available to draw from, and the conditions are often severely disabling: they restrict physical and mental capacity, and impact life expectancy. This kind of research illustrates a shift towards inclusive and responsive practice: people with rare conditions are often experts on their own conditions,

continued on next page ▶

Inclusive practice	Responsive practice
Online focus groups (4 groups) asking participants for feedback on research direction.	A two-page report thanking participants for their time and describing project progress.
Email requests asking for individual feedback (which would validate research findings).	A 2-minute progress update and graphics distributed via social media.

Figure 1: examples of inclusive and responsive research.

Figure 2: modelling enhanced feedback.

from previous page ▶

and their research role is being reshaped from passive participant, to consultant and collaborator.

The enhanced feedback intervention I carried out with RUDY made the information researchers already had more easily available online, bringing together pieces of information that had previously only been saved in different places. Rather than create a new website, I worked with RUDY to curate the resources at their disposal. Key information, such as the number of participants, was made more prominent on the project website (see Figure 3), and technical terms were made more accessible. For example, 'different phenotypes' was changed to 'differences between individuals with the same rare disease'.

RUDY asks participants to submit questionnaires online. Once a participant has submitted questionnaires for the first time, a request is then sent every six months. The questionnaires are used to understand what it is like to live with a rare genetic condition. The enhanced feedback intervention measured completion rate – the number of questionnaires submitted, as a percentage of the number of questionnaires requested. The enhanced feedback intervention increased general participation by 5%, and I saw a 30% increase in first-time completions alone.

Engaging research should be interesting, informative and interactive. There should be opportunities for participants to take part in the research process; providing feedback on findings, co-writing research papers or consulting on an advisory panel. Engaging research should also be inclusive and responsive. Inclusive data-practices relate to seeking input and responsive practices relate to offering feedback. Participatory research relates to seeking input outside of study participation, to improve the validity and relevance of research.

In conclusion, good research seeks input from the public, and excellent research responds to public need. Two-way communication needs to be part of 'good practice' because it strengthens research and offers an excellent way to demonstrate public approval.

To read the references for this article please go to bit.ly/2Riv96B

Figure 3: RUDY website (research.ndorms.ox.ac.uk/rudy).

Alumni Profile

Ines Marušić – A Co-Founder of the Oxford Women in Computer Science Society (OxWoCS), now Engagement Manager at QuantumBlack, McKinsey & Company

What course did you study here and when?
I did an MSc in Mathematics and Foundations of Computer Science (MFoCS) in 2011-2012, and a DPhil in Computer Science in 2012-2016 where I was supervised by Professors James Worrell, Stefan Kiefer, and Michael Benedikt.

What was your background before that?
I am originally from Croatia, and had completed a Bachelor's degree in Mathematics from the University of Zagreb before coming to Oxford.

What attracted you to studying Computer Science as a subject?
When I first came to Oxford my biggest interest was actually in mathematics, especially probability theory and statistics. During my MSc in MFoCS, I took a few courses in the Department of Computer Science, including Probability and Computing; and Machine Learning which I found incredibly interesting. They looked at new applications of many of the areas of mathematics I was already interested in within algorithms and theoretical Computer Science.

What aspects of the course you studied here did you particularly enjoy?
I particularly enjoyed topics that were at the intersection of probability theory and computer science, especially randomised algorithms and learning theory. Outside of my courses, I contributed to the department by co-founding the Oxford Women in Computer Science Society (OxWoCS) with a few friends who were all DPhil students and postdocs at the time. The society, which we founded in 2013 with the aim of supporting and promoting women in Computer Science, has since gone from strength to strength, and I am proud of the impact we've had on the department especially through our distinguished speaker series and our annual Oxbridge Women in Computer Science Conference which we co-organise with the Cambridge women @CL society.

What did you do when you left Oxford?
I joined QuantumBlack, McKinsey & Company, where I am currently an engagement manager leading cross-disciplinary teams in developing advanced analytics products for some of the world's largest organisations, helping them adopt machine learning at scale to transform their businesses and enhance their performance.

How has the course you studied here helped you in your current profession?
The courses I studied at Oxford were hugely helpful in my current role as they gave the technical foundations to be able to build machine-learning driven software products, and understand the best algorithmic approaches and implementation complexity and trade-offs. Beyond the technical knowledge, studying at Oxford has helped me learn how to learn and get good at synthesising new pieces of information quickly – both of which I have found to be invaluable in my current role.

What advice would you give to current students on applying their knowledge in the workplace, when they leave university?
The knowledge you receive at Oxford is a gift that will continue paying off throughout your entire career. Some of it may be the technical knowledge directly applicable in your job, eg, the knowledge of programming, algorithms and data structures. Some of it will be the soft skills, eg, the ability to form a well-structured logical argument on the fly or time management skills you gained during the busy Oxford terms. Leverage all of these in your first job, but also be aware that the industry is changing quickly and that your ability to absorb new knowledge over time will be a great asset.

What would the student you have thought about what you are currently doing – would you have been surprised, proud, amazed?
I think she would be pretty surprised with how things turned out given that at the start of my MSc I had a plan of becoming a university professor 🙂. Still, I hope she would be proud of the career I have built and pleased with how I have been able to find a job that I truly enjoy and where I can leverage my broad set of skills both technical and non-technical.

Oxygen delivery in tumours

by Joe Pitt-Francis (Department of Computer Science) and Philip Maini (Mathematical Institute)

The precise nature of red blood cell distribution and oxygen delivery in cancerous tumours can make a big difference to treatment outcomes. A predictive model recently developed by an international, interdisciplinary team hopes to pin down more precisely the routes which are favoured by red blood cells as they pass through the tumour vasculature. This knowledge will then inform us as to which parts of tumours are receiving oxygen and which are not. Tumour cells which are habitually exposed to low concentrations of oxygen are known to develop into more aggressive variants, which may be harder to treat.

A tumour typically begins as a ball of cancerous cells which don't have a normal life-cycle: they grow and divide too quickly and they have the usual mechanism of programmed cell death switched off, so they don't die. A ball of cells which grows in an out-of-control manner like this soon begins to run out of resources, so cancerous cells send out angiogenesis signals to ask for more nutrients. In this way the tumour hijacks the body's network of blood vessels, forcing the vasculature to grow and support the cancer. New blood vessels grow in an erratic manner. Blood vessel networks that support growing tumours are typically immature, irregular, leaky and tortuous.

You might suppose that the best way to treat a tumour with an inefficient blood supply is to make the vessel network worse and thereby to starve the cancer of nutrients. Counter-intuitively treatment can often be made better by increasing the efficiency of the blood supply, typically by treating with anti-angiogenesis drugs. Chemotherapy treatments rely on the blood network to deliver drugs to the tumour mass, while radiotherapy will only kill rapidly dividing cells – ones which are healthy and well-oxygenated. But in many tumours there are patches of cells which don't get very much oxygen because red blood cells fail to make their way through that part of the vasculature.

This problem has been the focus of a multi-disciplinary investigation, led by Miguel Bernabeu from the Centre for Medical Informatics, University of Edinburgh (and Oxford Computer Science DPhil alumnus), Tomas Alarcon, CRM, Barcelona (an Oxford Maths alumnus) and Oxford Mathematician Helen Byrne; and also involving Oxford colleagues Joe Pitt-Francis (Computer Science), Philip Maini (Mathematics) and Ruth Muschel (Oncology), together with researchers from University of Ljubljana, University of Glasgow, the Alan Turing Institute and University College, London.

Recent work in this field has focused on the fact that red blood cells normally travel in the main flow at the centre of a vessel, so that near to the vessel wall there is a cell-free layer. When there is a non-symmetric bifurcation in the network then one daughter vessel may receive a greater proportion of the red blood cells. (Imagine a wide vessel which splits into two daughters: one wide and one narrow. The narrow vessel might receive only blood plasma from the cell-free layer.) The insight in the new work is that the cell-free layer is disrupted by every bifurcation and will take time to re-establish. If the next bifurcation happens immediately downstream then the blood flow still has a 'memory' of the disruption and the cell-free layer will be different.

The team built a new phenomenological mathematical model of this 'memory' effect from experimental data and from painstaking computational fluid dynamics simulations of red blood cells travelling in a simple network of two bifurcations. Once the model was built, it was embedded in MicrovesselChaste, which is a bolt-on project to the Chaste computational biology library originally built in Oxford University's Department of Computer Science. MicrovesselChaste simulations track how the concentrations of red blood cells vary as blood flows through a network and then track how oxygen from those cells diffuses into the surrounding tissue.

The key finding is that a cancerous tumour vasculature, which has shorter sections of vessels between bifurcations, is affected by this 'memory effect' and delivery of oxygen to the tissue is patchy. Meanwhile, on normal vasculature and on vasculature that has been treated with anti-angiogenesis drugs, the model predicts that there is very little memory effect so oxygen delivery is normal. This means that, if blood supply to tumours is improved by anti-angiogenesis treatment, then future chemotherapy or radiotherapy treatment may be more viable, leading to better prognosis for cancer patients.

Citation for this work: bit.ly/3ggzmjq

Reimagining the human body

An outlook on technological enhancement

By Research Associate Pericle Salvini

Recently, a Silicon Valley company announced that a macaque was able to play a videogame thanks to a chip implanted in its brain. As observed by a journalist commenting on the news, the novelty was not so much in the technological achievement, but in the fact that a private company, and not an academic laboratory, had performed that research. Indeed, neural implants are nothing new. They are currently used to treat Parkinson's disease, and in research to restore the lost sensory-motor functionalities to people affected by spinal cord injuries.

For scientists dealing with responsible research and innovation, neural technologies represent a special case of innovation responding to a relevant social need and at the same time raising potential harms and important ethical, legal and social implications, both in the research process and in application. A few examples of these cases include animal testing, human enhancement and mind-control. In this article, I wish to focus on the impact of technological enhancement – namely neuro-mechatronic devices (also known as robotic prosthesis) – on the human body by addressing the following question: to what extent would healthy people be willing to sacrifice their own body to benefit from technological enhancement? However extreme such a question may appear, it is not the result of a cyberpunk nightmare, but it was brought to my attention by the current users of this enabling technology. Michael Bailey, a 35-year-old, lost three fingers in a road accident. Now he uses a robotic prosthesis. In a 2010 interview in the *Fast Company* magazine he said: 'When I'm wearing it [robotic prostheses], I do feel different: I feel stronger […] As weird as that sounds, having a piece of machinery incorporated into your body, as a part of you, well, […] It's a very powerful thing'.

Kiera Roche is the chairperson of a company customizing robotic prostheses. The following statement is taken from her website: 'In the first few years my focus was on trying to be normal, wearing clothes that hid the fact that I was an amputee, but over the years I have become more comfortable with who I am and I now embrace having different legs for different activities and different occasions. I think losing a limb has a massive impact on one's self esteem and body image. Having a beautifully crafted limb designed for you makes you feel special'. Exploring the idea of what it might be like to be interfaced with a piece of advanced technology and the aesthetic possibilities offered by it (eg changing shape, colour, height, etc), along with the potential improvements in functionality with respect to conventional (non-robotic) prostheses, is transforming the perception of disability. From something to hide, to something not to be ashamed of and, in the few cases I mentioned, something even to show off. However, the downside is that technological mediation could be perceived as better than the natural, original limb.

Indeed, Michael goes on to say: 'I don't think I would have said this if it had never happened […], but I'd cut the rest of my hand off if I could make all five of my fingers robotic'. Michael is not alone in thinking this. According to Hugh Herr, a well-known roboticist and amputee himself, new technological prostheses 'are becoming so lustrous and so efficient that some people are already willing to chop off a perfectly good limb to get one'. This is the case of the bionic pop artist Viktoria Modesta, who had voluntary undergone the amputation of her leg, which was affected by malformation since her birth. But what about healthy people? Would

continued on next page ▶

from previous page ▶

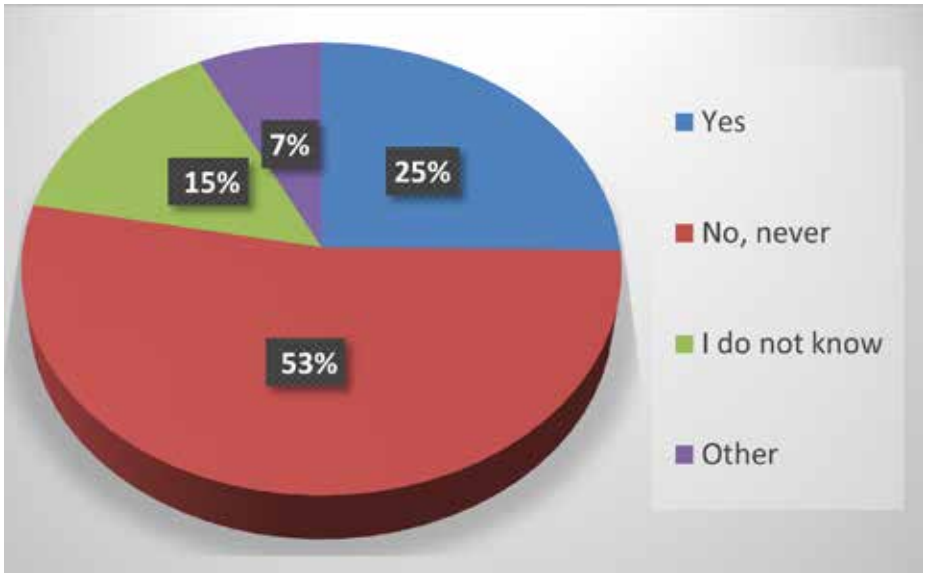
they be willing to chop off a healthy limb to take advantage of a powerful technology?

In order to give an answer to this question, I carried out a survey during a popular science exhibition on the topic of the nexus between the human and the artificial. Among the questions I asked: 'If the surgical operation were 100% safe, (ie without risks or consequences for your health), technically feasible, and economically accessible, would you be willing to replace a healthy part of your own body (eg a limb) with a robotic prosthesis?'

120 visitors took part in the survey by answering the above question: 53% of the respondents answered 'no', 25% accepted to renounce a body part, 15% did not know and 7% chose 'other'. It is interesting to consider the explanations provided:

1. 'it depends on the body part and the trade-off enhancement vs loss of functionality';
2. 'only if necessary due to physical problems';
3. 'no, but not 'never'";
4. 'only if necessary';
5. 'the prosthesis must be maintenance-free and lifetime should be greater than human expected life';
6. 'only if I'm the only one to have it';
7. 'yes, if the prostheses could perfectly replicate and enhance the replaced part';
8. 'only if the limb being replaced was at risk of future degeneration'

Apart from number 3, all the answers can be grouped into 2 main categories: a) 'yes, but only for therapeutic purposes' (answers number 2, 4 and 8), and b) 'yes, but only if enhancement is safe, highly performing, maintenance-free and exclusive (answers number 1, 5, 6, and 7), namely for non-therapeutic purposes. With respect to gender, male respondents seemed more in favour than women of replacing a healthy part of their body (29% and 22%, respectively). Likewise, among those who answered 'no', women were the majority (60% female vs 47% male). As to age, there were no substantial differences between adults and young adults (ie the most representative categories). However, adults were more willing to accept the replacement of a healthy body part with a technological device than young adults (35% and 17%, respectively). Finally, as far as education is concerned, I did not find any significant difference among the most representative categories considered (university and college students).



In conclusion, the results of this survey, with all its limitations, show that there exists a certain level of acceptability towards 'extreme' forms of technological enhancements, characterised by the replacement of the human body with an artificial limb or organ better than its natural counterpart. The goal of the survey was to anticipate a possible future scenario. Indeed, in a not-so-distant future, neuro-mechatronic devices directly linked to the nervous system could exacerbate the trend towards the gradual escape from the limitations of the body. Companies could start to exploit the availability of augmenting technologies by creating new needs and desires concerning the construction of one's own identity. How would we regulate this phenomenon (ie the desire to become a cyborg) if we had to face it? It is now time to reflect on the consequences of augmenting technologies when not used for therapeutic purposes.

For further reading on this subject please read: *If new metal legs let you run 20 miles/hour, would you amputate your own?* bit.ly/3fEUNvD

Marquard Smith and Joanne Morra (Eds). *The prosthetic impulse. From a posthuman present to a biocultural future*. The MIT Press: Cambridge (Mass): 2006.

The results presented here are the outcome of a pilot study and designed to be a preliminary test with a small sample. The longer term goal is to replicate the survey in a wider context.

How Government COVID-19 policy announcements have inspired a cyber-crimewave

Billions of people's lives changed across the world when the pandemic began, as we experienced a 'new normal' with more people, spending more time online than ever before.

With this there came a surge of unique cybercrime-related circumstances affecting society and businesses. There has been a remarkable surge in cyber-security crime experienced during the global COVID-19 pandemic, with a noticable link between governmental policy announcements and cybercrime campaigns. A consortium of researchers report that some days as many as three to four new cyber-crimes were being recorded.

Xavier Bellekens from the University of Strathclyde, said 'Over the last year we have seen a surge in cyber-attacks targeting critical infrastructures, governments, organisations and end-users, influenced by governmental announcements. These have ranged from targeted attacks to selling counterfeited respirators to hospitals, denying of essential services through ransomware, selling fake online COVID-19 testing equipment as well as more recently, generating fake Covid travel tests. These techniques, while common, had never been observed in relation to an event of this magnitude, making this study unique.'

The COVID-19 pandemic created a new normal, for billions of people around the world, with people working from home, ordering shopping and socialising online, as shops and businesses were closed. However, with an increased amount of people being online, an increase in cyber-attacks has also been found.

Researchers from University of Oxford, WMG (part of University of Warwick), Abertay University, University of Kent and University of Strathclyde worked in collaboration in the study, 'Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic,' published in the journal *Computers & Security*.

By using the UK as a case study, the paper reveals the explicit connection between governmental policy announcements and cyber-crime campaigns. Although this is a pattern that's been suspected for a while, this is the first analysis from hundreds of cases around the world which makes this connection clear. Harjinder Lallie, from WMG, University of Warwick comments, 'The analysis presented in this paper has highlighted a common modus-operandi of many cyber-attacks during the coronavirus period. Many of the cyber-attacks begin with a phishing campaign which directs victims to download a file or access a URL. The file or the URL act as the carrier of malware which, when installed, acts as the vehicle for financial fraud. The analysis has also shown that, to increase the likelihood of success, the phishing campaign leverages media and governmental announcements. In fact some days we recorded as many as three to four new scams.'

Since the outbreak of the pandemic in 2019 there have been reports of scams impersonating public authorities such as the World Health Organisation, and organisations such as supermarkets and airlines targeting support platforms such as suppliers of Personal Protective Equipment and offering COVID-19 cures. They often target the public, who are now socialising and spending more time online in general, as well as the increased population of people who are working from home.

continued on next page ▶

from previous page ▶

Such scams can be sent by text or email, and in most cases a URL pointed to a fake institutional website which requests debit/credit card details.

In order to support ongoing research, the researchers have proposed a novel timeline of 43 cyber-attacks related to the COVID-19 pandemic. This timeline and the subsequent analysis can assist in understanding those attacks and how they are crafted, and as a result, to better prepare to confront them if ever seen again.

They found that from the point that the first case was announced in China the first reported cyber-attack was 14 days later. From this point onwards the timeframe between events and cyber-attacks reduced dramatically.

The cyber-attacks were categorised, and it was found:

* 86% involved phishing and/or smishing (fraudulent text messaging)

* 65% involved malware

* 34% involved financial fraud

* 15% involved extortion

* 13% involved pharming

* 5% involved hacking

* 5% involved denial of service

Jason Nurse from the Institute of Cyber Security for Society (iCSS) at the University of Kent (and visiting academic at the Department of Computer Science at the University of Oxford) said, 'COVID-19 has had a substantial negative impact on society, and this impact, as we show in our new research, has also meant a notable increase in cybercrime globally.

'There are several significant novel findings emerging from our analysis, but the one I found most salient was the targeted use of threats, scare tactics and fake incentives within attacks. Cybercriminals clearly understood that many people would be anxious, worried, distracted and away from their support networks (personal or work-related), and sought to exploit this as much as possible. I hope our research can provide a pathway for future work into faster reaction to these cyber-attacks, and also increase society's awareness of their prevalence.'

In conclusion, Arnau Erola, from the Department of Computer Science at the University of Oxford comments, 'Cybercriminals take any opportunity to their advantage. By getting insights on their modus operandi, policies to tackle cybercrime can become more effective. This is not only deterring cybercriminals from their unlawful activities but also educating the society about improper and unethical actions.'

Read more here: bit.ly/2RWCzMN

'I hope our research can provide a pathway for future work into faster reaction to these cyber-attacks, and also increase society's awareness of their prevalence.'

Jason Nurse, University of Kent

Rebuilding and enhancing trust in algorithmic systems

by Senior Researcher Jun Zhao

Algorithm-driven online systems are increasingly encountered in everyday life. They make recommendations for us on things such as items we might like or make automated decisions about our job applications; case evaluations in the justice system; or students' exam results. A survey by the British Computer Society in 2020 indicated that the majority of British adults do not trust algorithms.

The sense of distrust associated with these systems contributes not only to negative effects on people's online wellbeing but also impedes the success of future innovations that may provide critical solutions to digital services of national importance. As put by the UK Information Commissioner, they stated that 'a lack of trust in the [NHSX contact tracing] app would have meant a lack of engagement with the app. And the benefits the service offered society would have been lost.'[1]

Trust is a key component of the digital economy. It is important for the smooth running of the economy, underpinning the success of new technological innovations and enhancing collaboration between organisations and individuals. However, trust breakdown is commonly observed from users of algorithmic systems, regarding their fairness, accuracy and reliability. People often feel unable to trust algorithmic outcomes, feeling anxious, disempowered, or losing faith in both the platforms and the authorities. This state of perception can lead to disengagement with new innovations as well as distrust toward platforms and their providers. The ReEnTrust project (reentrust.org) is funded by the EPSRC Digital Economy Programme, between 2018 and 2021. It is led by Professor Marina Jirotka at the Department of Computer Science in Oxford and involves partners from University of Edinburgh and University of Nottingham. The project recognises the imperative of repairing the current trust breakdowns of users today and explore ways to rebuild trust in online algorithmic systems.

Drawing on 12 workshops, 300 responses to online surveys and 30 interviews, involving stakeholders across different sectors and user groups of different age groups (16-25 and 65+), the ReEnTrust project has produced three experimental online applications to explore deeply what is needed by our users for trust rebuilding. We believe that the findings from these experiments and workshops will be critical not only for the research community, to further pursue novel design and innovation opportunities, but also for policy-makers to identify gaps in existing regulations and policies, and make changes that are needed for repairing one of the most imminent challenges we are facing in the digital economy and for rebuilding our society post a prolonged global pandemic.

Our findings provide three key messages:

1. Design for increased systemic transparency
Algorithmic explanations describe how outcomes from an algorithmic system are generated. They are largely well-received by the general public for making sense of algorithmic outcomes. However, while explanations may be necessary, our research showed that they do not always provide sufficient transparency for users to trust the results they see. Users demand systemic transparency about how an algorithmic system came to its conclusions, the purpose of the system in an organisation and how the data will be used, and in the underlying business model, with a balance between increased transparency and the protection of intellectual property rights and trade secrets.

2. Engage diverse user groups and consider a range of application contexts
The second key finding from the ReEnTrust project is that there is no one-size-fits-all way in terms of enhancing trust. Trust in online systems is contextual and depends on many factors, including the task to be completed and the relevance of the algorithmic decision to the user. Different age groups approach trust in different ways, with older people more likely to place their trust in established institutions that they are familiar with, while both young and old tend to expect that websites should behave in a trustworthy way.

3. Increase citizens' awareness of algorithms
Our final key finding has shown that users largely have limited awareness about how algorithms are deeply embedded in our everyday life, especially for the older citizens. People need to be able to recognise the involvement of algorithms in digital services as a necessary first step to allow them to critically engage with these systems. Although sites are required to provide information about security and their use of cookies, for example, this does not provide

continued on next page ▶

[1] ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/from-facial-recognition-technology-to-children-online-regulating-data-protection-in-2021/

from previous page ▶

support for users to judge whether an algorithm is fair or accurate.

The findings have identified critical gaps with regard to supporting the rebuilding of users' trust in algorithmic systems. They provide critical contributions to the current research roadmap in HCI and AI as well as related policy development in the UK. We have recently witnessed how lack of trust can deter the uptake of technologies in critical public sectors, such as policing, education or healthcare. As the public pushback towards the deployment of these technologies such facial recognition. Without any doubt, the development and adoption of these algorithmic systems in these critical application areas must undergo careful thinking and planning. It is increasingly recognised that transparent, responsible and fair technology innovations should be the future of an AI-driven society. However, trust of technologies must be rebuilt so that new innovations following in a positive direction can be appreciated and recognised. We do hope that findings from the ReEnTrust project will inform new design developments, increase public awareness, and stimulate associated policy developments. In this way we will facilitate the development of a truly trustworthy digital society for people and for the future.

This article is based on research outcomes from the Engineering and Physical Sciences Research Council (EPSRC) project "ReEnTrust: Rebuilding and Enhancing Trust in Algorithms" (EP/R033633/1; 2018-2021) and "From Human Data to Personal Experience" (EP/M02315X/1; 2015-2021).

CalTrack

a new way to understand calcium flow in the heart

By Doctoral Student Francesca Margara

Calcium is an important signalling molecule in the human heart. Calcium transients within cardiac cells control how the heart contracts and relaxes and can trigger life-threatening abnormal cardiac rhythms. Furthermore, calcium signalling is often altered in cardiac diseases. Thus, being able to track the dynamic changes of calcium can advance our understanding of cardiac physiology, pathology, and response to pharmacological therapies.

Nowadays, researchers can use advanced imaging techniques to acquire large amount of calcium data from many different cell types. However, the possibility of performing an accurate and automated analysis of this large quantity of data is limited.

In collaboration with Cardiovascular Medicine at Oxford, we developed CalTrack to address this need and we have made the software freely available to other researchers. CalTrack is an easy to use, adaptable, and automated analysis pipeline. It can provide several key measurements that characterise calcium transients' morphology and how it changes in different scenarios. Importantly, CalTrack enables computational investigations into the mechanisms through which calcium affects the heart function in heath, disease, and under drug action, by generating large amount of high-quality data.

In my DPhil thesis I have additionally integrated and augmented calcium data analysed by CalTrack with modelling and simulation of human cardiac cells, to better understand how genetic mutations cause a disease called hypertrophic cardiomyopathy. This is a common inherited cardiac disorder that affects 1 in 500 people and can lead to sudden death.

I constructed models of human cardiac cells under different genetic mutations and conducted simulation studies to identify and explain the mechanisms through which specific mutations underlie the changes in calcium transient as quantified by CalTrack, and how these would affect other cellular properties such as the cell's ability to contract. Based on this, I also assessed whether specific pharmacological interventions would be beneficial to restore cellular function altered by the mutation.

Such combined approach of experimental and computational research can advance our understanding on the response to drug action in specific scenarios. When CalTrack analysis is applied to cardiac cells derived from patients, analysed data and computer models can then predict and explain drug action in the individual subject. Thus, these findings can improve the development and administration of novel effective pharmacological interventions that are patient specific.

Satellite hacking: researching cyber space

By James Pavur, Rhodes Scholar and DPhil student in cyber security

The number of satellites in orbit is expected to increase by an order of magnitude over the next decade. From weather and geolocation to communications and research, these distant information systems provide critical services that impact billions of lives. Here, at the beginning of a new era in space technology, it is more important than ever to ensure that these platforms are secure.

At Oxford University's Systems Security Lab, led by Professor Ivan Martinovic, we are working to study the unique cyber security threats and requirements relevant to space technologies. The intention is to identify security gaps that have evolved in modern space missions, determine the underlying causes of these shortcomings, and invent solutions that satellite operators can incorporate to better secure their missions.

Studying SATCOMs

One particularly exciting topic has been our research into the security of modern satellite broadband communications. Satellite-based internet services are a key growth area in the space industry, with companies like SpaceX, Inmarsat, Amazon, and OneWeb betting on satellite constellations as the best way to bring the next billion internet users online.

Even today, satellite internet services support millions of customers and businesses. Understanding the security properties and requirements of status quo services can help guide our efforts to design and defend the next generation of satellite broadband.

We began with a series of passive surveys, listening to the radio emissions of 18 satellites in geostationary orbit (GEO). These GEO satellites are located about 30,000 km above the equator. The specific platforms involved in these studies serve customers on five continents, with a combined footprint area exceeding 80 million square kilometers.

Eavesdropping signals intelligence on a hobbyist budget

In exploring these signals, we found that a cyber-attacker could reliably eavesdrop on broadband traffic from dozens of different providers. To make matters worse, they could do so using about £250 worth of widely available home television equipment.

As many satellite internet service providers were not employing over-the-air encryption, this meant attackers could directly observe the internet traffic of satellite broadband customers. Additionally, due to the nature of satellite communications, this attack was virtually untraceable and could be executed over distances of thousands of kilometers.

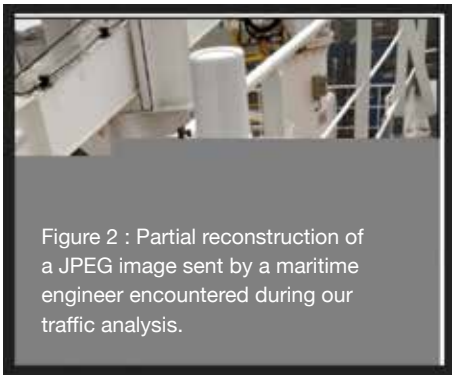


Figure 2 : Partial reconstruction of a JPEG image sent by a maritime engineer encountered during our traffic analysis.

Looking closer at the contents of these signals confirmed the severity of these findings. We encountered a wide range of data which was inadequately protected. This included consumer traffic, such as SMS text messages from passengers using in-flight Wi-Fi services over the Atlantic. It also included data from governments and some of the world's largest businesses, such as navigational charts destined for cargo vessels in the Mediterranean or login credentials for wind turbines in continental Europe.

When we encounter issues like this in our research, we follow a standard practice known as 'responsible

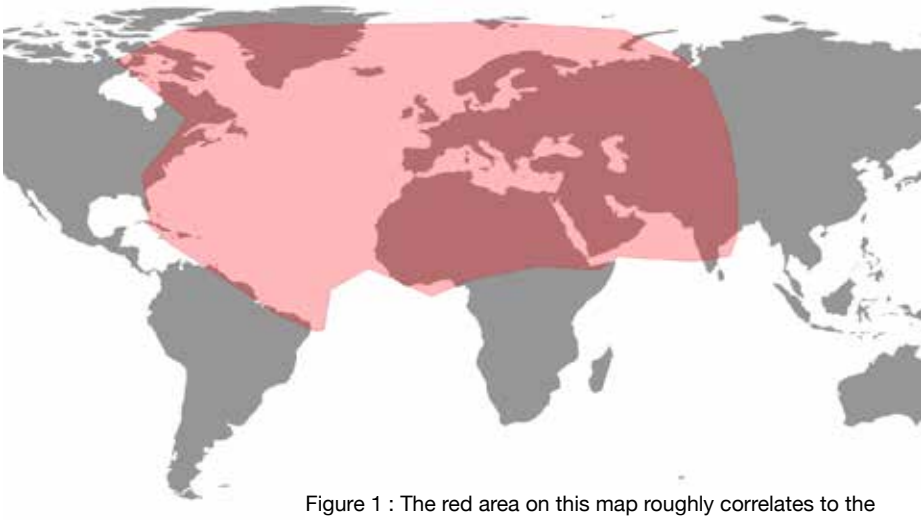


Figure 1 : The red area on this map roughly correlates to the combined coverage of the signals received in our study.

continued on next page ▶

from previous page ▶

disclosure' prior to publication. In our case, this involved reaching out directly to both satellite internet service providers and larger industrial customers to inform them of our findings and make them aware of previously overlooked risks impacting their businesses.

How does this happen?
During our responsible disclosure conversations, we learned that many in the industry were notionally aware of the risk of unencrypted wireless communications but had decided to accept it. In part, this was because they assumed equipment to execute these attacks was far more expensive than we found in our own research. However, there were also substantial performance costs to standard encryption approaches – such as the use of end-to-end virtual private networks (VPNs).

After reviewing some related research, we learned that the physical properties of satellites were causing VPN encryption tools to perform poorly in modern networks. Specifically, because satellites are thousands of kilometers away from the customers who are using them to communicate, the speed of light acts as a cap on how quickly messages can be sent in these networks. Because of this, certain protocols such as the TCP protocol used by most websites, require special performance optimisations from satellite internet service providers using applications called Performance Enhancing Proxies (PEPs).

These optimisation tools required the internet service provider to have full visibility into the traffic of their customers so they could determine which packets to optimise. Customers who decided to use a VPN would end up blocking this visibility and would find their connections slow to a crawl.

Building an open and actionable solution
Rather than attempt to convince internet service providers to update their systems to support encryption

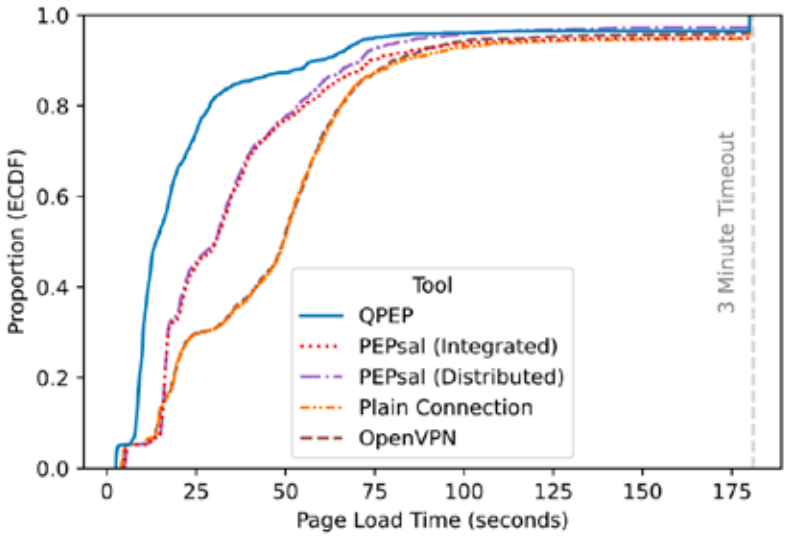


Figure 3 : Distribution of Page Load Times Across Alexa Top 20. PEPsal is an unencrypted PEP and OpenVPN is a typical VPN product.

– a liability which they seemed reluctant to adopt – we worked to invent an approach which would allow customers to encrypt their traffic independently according to their specific needs. Critically, the system had to be comparably performant to unencrypted traffic sent via a traditional PEP.

The ultimate result of this effort was the creation of a hybrid VPN-PEP called QPEP which combines the performance properties of satellite PEPs with a VPN-like encrypted tunneling mechanism. QPEP leverages a modern encrypted transport protocol, known as QUIC, which ensures reliability and reasonable bandwidth exploitation – even in high latency satellite environments.

In testbed simulations, we found that QPEP not only outperforms traditional VPNs, but its design achieves faster page load times than even unencrypted PEPs. Across the Amazon's Alexa Top 20 list of popular websites, QPEP roughly halves page load times compared to an unencrypted PEP and loads pages over 70% faster than VPN-encrypted connections in the same network.

Today, QPEP is freely available as an open-source tool which anyone can download and modify. One advantage to doing this sort of research at Oxford is that we can share information about our solutions freely, without pressure to commercialise or maintain proprietary secrets. This means other researchers can verify and improve on our ideas, paving the way to more secure satellite broadband for everyone. In an industry where encryption solutions are typically closed source and unverifiable 'black boxes', we hope that our open approach can rejuvenate innovation around a vital security topic.

Going forward
Our own work on QPEP is continuing as we move towards testing the tool in real-world satellite networks and optimising its design for use in large networks. We are also considering related topics in securing other satellite communications applications, such as inter-satellite links in Low Earth Orbit (LEO) constellations.

Beyond satellite broadband, there are many other security topics of relevance to the space community. For example, we are conducting research into the security properties of space situational awareness (SSA) data which is used to help satellites avoid on-orbit collisions with each other and with pieces of space debris. We've also exploring a variety of other topics, ranging from small satellite platform security, to the interaction between cyber security and range safety for rocket launches.

How hard is it to separate P and NP?

By Marie Curie Research Fellow Jan Pich

Can we automate creative and challenging tasks such as proving mathematical theorems or designing learning algorithms? Such questions can be formalised in the language of computational complexity theory and constitute some of the most fundamental scientific problems of our time. A famous obstacle in the centre of these pursuits known as the P versus NP problem asks, intuitively, whether it is possible to solve efficiently (in P-time) all problems whose solutions can be efficiently verified (NP-problems). The P versus NP problem is one of the central questions in the theory of computing. It was formally introduced 50 years ago. However, despite enormous efforts invested into the problem during the decades, we appear to be nowhere near a solution. What is behind its notorious difficulty? Unfortunately, since the early days of complexity theory, it has been clear that some of its main problems are not going to be easy to resolve. In the 1970s, a discovery of the relativisation barrier clarified why proof methods based purely on diagonalising arguments, otherwise successfully applied in addressing several related questions, cannot succeed in separating P and NP. Researchers then turned their attention to more concrete proof methods with a hope of developing non-diagonalising arguments.

An elegant model of boolean circuits, and proving lower bounds on the complexity of boolean circuits, looked particularly promising for that purpose. This program was met with initial success in the 1980s, with the invention of many complexity lower bounds for restricted classes of circuits. By the end of the 1980s it became, however, increasingly more and more evident that the story is not going to end so fast. These fears were fully materialised in the early 1990s when Alexander Razborov and Steven Rudich discovered the natural proofs barrier for proving circuit lower bounds, which symbolically closed another era in our attempts to attack the P versus NP problem.

Razborov, who also stood behind some of the most popular lower bounds of the 1980s had, however, a much more ambitious goal. He wanted to show that circuit lower bounds present a limit to what is achievable by strong fragments of logical reasoning and postulated several conjectures to this effect in early 2000s. One of these conjectures, in its strongest form, implies that strong circuit lower bounds cannot be proved in a theory PV. The theory PV, introduced by Stephen Cook, can be interpreted as a fragment of Peano Arithmetic, and formalises the notion of efficient

(P-time) reasoning. Ironically, the progress on proving such unprovability results turned out to suffer from similar obstacles as those preventing us from solving the P versus NP problem itself – just like we do not understand the power of P-time algorithms, we do not understand the power of P-time reasoning.

In a recent paper co-authored with Professor Rahul Santhanam, (which will be presented at the Symposium on Theory of Computing (STOC) 2021), we contributed to this research direction by showing that very strong complexity lower bounds such as NP being hard on average for co-nondeterministic circuits of sub-exponential size, which would in particular separate P and NP, cannot be proved in theories such as PV. The power of these theories can be demonstrated by the fact that many classical theorems from computational complexity are provable in them, including, for example, the PCP theorem and the circuit lower bounds discovered in the 1980s.

We hope that our result will clarify which methods are needed to derive strong complexity separations and eventually help to bring us closer to the actual solution of problems such as the P versus NP.

Acknowledgement: This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodovska-Curie grant agreement No 890220.

Will the government's online safety laws for social media come at the cost of free speech?

By Doctoral Student Claudine Tinsman, originally published in *The Conversation*

The UK government is planning to change the law so that social media companies like Facebook and Twitter will have no choice but to take responsibility for the safety of their users. Plans to impose a duty of care on online services mean companies will have to determine if content poses 'a reasonably foreseeable risk of a significant adverse physical or psychological impact' to their users.

Failure to comply with the new duty of care standard could lead to penalties up to £18 million or 10% of global annual turnover and access to their services being blocked in the UK. The UK government has released its final response to the public's input on the online harms white paper it published in April 2019 in anticipation of an 'online safety bill' scheduled to be introduced in 2021.

While well intentioned, the government's proposals lack clear instructions to guide regulators and social media companies. In failing to do so, the government has created a threat to freedom of expression in the process. Under the proposals, companies will be required to take action to limit the spread of harmful content, proportionate to their severity and scale.

Currently, social media companies are only required to remove user-generated content hosted on their services under very specific circumstances (if the content is illegal, for example). Usually, they are free to decide which content should be limited or prohibited. They only need to adhere to their own community standards, with sometimes mixed results. As Facebook reported in its community standards enforcement report, for the first quarter of 2020 it only found and flagged 15.6% of 'bullying and harassment' content before users reported it. Conversely, the company pre-emptively detected 99% of all 'violent and graphic' content before it was reported by users. This disparity in detection rates indicates that the processes used to identify 'harmful' content work when criteria are clear and well-defined but – as the 15.6% figure shows – fails where interpretation and context come into play.

Social media companies have been criticised for inconsistently enforcing prohibitions on hate speech and sexist content. Because they only need to justify decisions to leave or remove legal but potentially harmful content based on their own community standards, they are not at risk of legal repercussions. If it's unclear whether a piece of content violates rules, it is the company's choice whether to remove it or leave it up. However, risk appraisals under the regulatory framework set out in the government's proposals could be very different.

Lack of evidence

In both the white paper and the full response, the government provides insufficient information on the impact of the harms it seeks to limit. For instance, the white paper states that one in five children aged 11-19 reported experiencing cyberbullying in 2017, but does not demonstrate how (and how much) those children were affected. The assumption is simply made that the types of content in scope are harmful with little justification as to why, or to what extent, their regulation warrants limiting free speech.

As Facebook's record shows, it can be difficult to interpret the meaning and potential impact of content in instances where subjectivity is involved. When assessing the harmful effects of online content, ambiguity is the rule, not the exception. Despite the growing base of academic research on online harms, few straightforward claims can be made about the associations between different types of content and the experience of harm.

For example, there is evidence that pro-eating disorder content can be harmful to certain vulnerable people but doesn't impact most of the general population. On the other hand, such content may also act as a means of support for individuals struggling with eating disorders. Understanding that such content is both risky for some and helpful to others, should it be limited? If so, how much, and for whom? The lack of available and rigorous evidence leaves social media companies and regulators without points of reference to evaluate the potential dangers of user-generated content. Left to their own devices, social media companies may set the standards that will best serve their own interests.

Consequences for free speech

Social media companies already fail to consistently enforce their own community standards. Under the UK government's proposals, they would have to uphold a vaguely defined duty of care without adequate explanation of how to do so. In the absence of practical guidance for upholding that duty, they may simply continue to choose the path of least resistance by over zealously blocking questionable content. The government's proposals do not adequately demonstrate that the harms presented warrant severe potential limitations of free speech. In order to ensure that the online safety bill does not result in those unjustified restrictions, clearer guidance on the evaluation of online harms must be provided to regulators and the social media services concerned.

Original article: bit.ly/3cNWCV4

WatchDog: Protecting users against telephone fraud

By Doctoral Student Jack Jackson

Each year, over four million individuals in the UK fall victim to scams, incurring an estimated £7bn of personal financial losses, often with significant consequences including trauma. The largest proportion (38%) of this fraud occurs via telephone and, as such, disproportionately affects older, vulnerable adults and those less technologically literate*. Recent research suggests that victims of fraud are three times more likely to experience emotional trauma as a result of fraud, than financial loss.

I have been working with researcher Anirudh Ekambaranathan, and Professor Max Van Kleek, from the Human Centered Artificial Intelligence (HCAI) group within the Department of Computer Science. Together we are in the process of launching a spin-out company, WatchDog, which leverages the power of AI and Internet of Things (IoT) to protect vulnerable users against telephone fraud.

WatchDog first and foremost aims to prioritise the needs of senior citizens, who may be suffering from age-associated cognitive or memory decline, which makes them particularly vulnerable to scams. To make the system work well for this population – who still routinely use landlines – WatchDog will create a hardware device that can be adapted for both landline and mobile use. It is explicitly designed with simplicity and robustness in mind.

The WatchDog team is working to provide a layer of security beyond that of existing solutions, by using natural language processing and machine learning techniques to analyse the content – and conversation – level features of scam calls, to proactively detect and deter fraud in real time. From a user perspective, this would allow for the identification of fraudulent activity at any point of a telephone call, even where existing systems were initially bypassed.

Existing solutions within the space are strictly limited in their fraud detection capabilities, and are heavily reliant on blacklists of fraudulent caller identities. A small number of state-of-the-art solutions are attempting to identify callers in new and unique ways, including: creating biometric voice fingerprints for known fraudsters, attributing emotional states to callers, and detecting falsified background audio within incoming calls. Whilst these methods work to varying extents, they all share the common objective of preventing fraud by attributing identity to the caller. Therefore, in order for an adversary to circumvent the system, they need only mask their identity. This is something which existing technology is already able to facilitate, leading to the regular bypassing of these systems.

The WatchDog team was recently offered a position within the UK government academic start-up accelerator (CyberASAP), led by the Department for Digital, Culture, Media & Sport (DCMS), InnovateUK, and KTN. As part of their work, the team is developing a small number of hardware prototypes of their solution, which will allow them to conduct an initial batch of user testing.

* The figures were referenced in an NCA (National Crime Agency) report, which cited the Annual Fraud Indicator produced by Crowe UK, Experian, and the University of Portsmouth.