MANCHESTER
1824
The University of Manchester

ON DIGITAL TRUST

ON DIGITAL TRUST

Foreword

Dorothy Byrne

This is a publication of great importance and I am honoured to introduce it. Our lives are being transformed for better and for worse by the digital revolution. Within seconds, a doctor can call up scrupulously-researched information which will save a child's life. Elsewhere, a bogus medical expert is flogging homeopathic remedies on a website which may be read by millions. A young person crying out for help might come across a chat room where they will receive support from caring experts or may be urged to hurt themselves further. When I was a child, my knowledge of children in far-off lands came from text books which told me how the British Empire had made the world a better place. Now kids in classrooms in Manchester can speak directly to children in schools across Africa and learn the truth about their lives. It's been information which young people have accessed directly themselves which has made them demand action on climate change. But they are also being fed porn and may be the victims of grooming by someone living thousands of miles away. Many have no concept of the privacy we took for granted.

The public is aware that much of what they read is nonsense. A Reuters Institute report last year which surveyed people across 40 countries found that only 23% trusted news on the internet and just 10% trusted social media news, yet young people increasingly rely on those sources for all their information about the world. We may think we can judge the truth of what we see but when Channel Four Television showed six stories, three of which were true and three false, to 1,700 people, only 4% of people guessed correctly. What are the implications for our democracy if voters are being fed lies in messages targeted at them individually by unknown forces using information from their search histories acquired by unknown hands?

We need excellent publications like this to alert us to the risks, to inform us about the massive benefits to our health and lives which harvesting data can bring, and to feed into thinking about how we can regulate so that we control our futures.

Dorothy Byrne is Head of News & Current Affairs at Channel Four Television.

During her tenure, the Channel's news and current affairs programmes have won numerous BAFTA, RTS, Emmy Awards and others.

Dorothy was made a Fellow of The Royal Television Society for her "outstanding contribution to television" and received the Outstanding Contribution Award at the RTS Journalism Awards in 2018. She has received a BAFTA Scotland award for her services to television and has also won the Factual Award given by Women in Film and Television. She is a trustee of the Ethical Journalism Network which supports the development of ethical codes in journalistic organisations across the globe.

She is a former World In Action producer and editor of ITV's The Big Story. Before joining Channel 4 she also produced arts programmes and executive produced history series for the channel.

She is a Visiting Professor at De Montfort University where Channel Four supports an MA in Investigative Journalism.

Democracy at risk? Detecting and deterring the flow of disinformation in elections

Professor Rachel Gibson

The impact of online activity designed to disrupt democracy and sway elections is a matter of growing concern worldwide. From cyber-attacks and the deployment of malware, to data leaks and the spreading of 'fake news', subversive activity to influence political outcomes is becoming more sophisticated and widespread. Much of it is taking place on social media platforms. But what can be done to protect citizens, society and democracy itself?

Growing evidence, mounting pressure

Official investigations into the misuse of voters' personal data during political campaigns have increased following the Cambridge Analytica scandal, a watershed moment which uncovered the harvesting of millions of people's Facebook profiles. There is also growing evidence of concerted efforts by anonymous 'hostile' actors to use AI to automate the spread of misinformation during elections in a bid to deceive the electorate and disrupt outcomes. Meanwhile stories of the deliberate hacking of political parties' and candidates' emails and malicious attacks on commercial and public agencies' operations via ransomware are all on the rise.

Efforts by governments to address these problems are mounting, as is pressure on social media providers and other tech businesses to be more accountable and transparent in their practices. Such interventions are clearly important. However, in order to effectively deter these threats to the political process we first need to define the range and nature of the problems we face more clearly, determine which ones we can tackle now - given the resources available - and outline the range of mechanisms that exist, or are within reach, to deal with the most serious of these.

Stories of the deliberate hacking of political parties' and candidates' emails and malicious attacks on commercial and public agencies' operations via ransomware are all on the rise.

The scale of the problem

Debate about the impact of new communication technology on democracy preceded the arrival of the internet. The invention of the printing press, the telegraph, radio and television all fuelled hopes and fears about the diffusion of new ideas and the empowerment of ordinary citizens. The emergence of the World Wide Web in the early 1990s was no different. For Howard Rheingold, one of the early 'gurus' of the online community, the internet provided the opportunity to transform society and 'revitalise citizen-based democracy'. Decades on, however, the narrative has shifted quite profoundly. The talk now is of 'dark web' activity, where voters are profiled without their consent and 'deep fakes', 'bots' and 'troll factories' lurk, seeking to confuse and manipulate an unsuspecting electorate.

While there is no doubt such techniques are being deployed in elections, there is surprisingly little systematic evidence or consensus on how widespread or how effective they are. In 2017, survey research from the US reported that the average American adult saw at least one fake news story during the Presidential campaign of 2016, that most such stories favoured Donald Trump, and that over half of those exposed actually believed what they read. However, analysis of voters' Twitter feeds found that fake news accounted for only 6% of all news consumed on the platform during the campaign, and that it was heavily concentrated among certain users – with just 1% of users being exposed to up to 80% of fake news stories.

In 2017, the public release of tweets and Facebook posts from accounts linked to the Russian Internet Research Agency (IRA), by the US Senate intelligence committee, prompted a flurry of investigations into efforts to interfere with the 2016 presidential election. While there was universal agreement that the IRA had embarked on a coordinated effort to confuse and demobilise American voters, particularly those likely to support the Democrat candidate Hilary Clinton, there were mixed verdicts on its success in doing so. Some research using over-time analysis of tweet release, and subsequent changes in public opinion polls, suggests a concerning pattern of linkage. However, other research argues trolls played only a minimal role in the Twitter election debate compared with 'authentic' accounts, and that despite having an extensive reach, the content of the IRA automated messages was of limited power to persuade, given the crudity of expression and syntax.

Even where false information is shared or posted during an election, if the person(s) responsible does so in ignorance, how far should their actions be penalised?

Misinformation, disinformation and mal-information

Given the difficulties associated with measuring and tracing the impact of these new rogue actors and algorithms, where should policymakers be targeting their efforts? We might start by dissecting the problem of election misinformation according to two criteria – importance and tractability. What is of most concern, and what is most amenable to governmental intervention? For example, playing hard and loose with facts in order to promote oneself and discredit one's opponents is hardly a new campaign strategy. Tasking bodies such as the Electoral Commission with the job of deciding whether an advertisement crosses a line from truth to lie risks becoming a time-consuming exercise that ends up enmeshed in court proceedings. Even where false information is shared or posted during an election, if the person(s) responsible does so in ignorance, how far should their actions be penalised? Again, the blurred lines of accountability and proportionality threaten to stymie any attempts at an effective regulatory clamp down.

Leaving to one side concerns about the flow of 'standard' propaganda and the accidental diffusion of misinformation that digital channels encourage, there are a range of more malicious and coordinated misuses of information that social media is particularly prone to. These include attempts by foreign and domestic actors to actively misinform voters or engage in what we might label as disinformation campaigns. The goal here is to deliberately decrease the amount of accurate information in society by increasing the supply of false and extremist

POLLING STATION
POLLING STATION

information in circulation. While the result of such activity may simply be increased confusion and distrust among the public, it may also have a more specific end of encouraging support for a preferred candidate, while discouraging votes for their rivals. One step beyond this type of social 'hacking' are more targeted and illegal uses of the internet designed to spread 'true' information in order to disrupt and damage. This type of mal-information includes the leaking of confidential data and information designed to discredit opponents, or the promotion of hate speech online toward an individual, based on personal characteristics such as race or religious identity. The authors of such attacks will of course take steps to cover their tracks. However, this type of strategic and coordinated misuse of technology often leaves some type of digital breadcrumb trail that is susceptible to detection and investigation.

Where Next?

Given the wide range of informational 'ills' that digital technology can now release into the political ecosystem, the question arises of what can be done to stem their flow? Numerous reports such as the Digital, Culture, Media and Sport (DCMS) committee publication *Disinformation and 'fake news'* seek to map this terrain. Distilling their contents and using my proposed combined importance and tractability 'test', I have identified four proposals for positive progress in this area:

- Mandate providers of social media platforms to maintain, and make available to government agencies, accurate records of all political advertising purchased on their platforms (with no minimum threshold applied). All paid advertising should carry an imprint that identifies who funded it. In addition, 'fake news' teams should be actively deployed by the companies to identify the categories of information misuse highlighted above, ie attempts at mal-information, disinformation and also, where possible, misinformation. These teams would feed into my next recommendation.
- A fact-checking consortium should be established for elections, as a joint initiative between government, media, and platform-providing companies. This would carry out impartial checks on social media accounts suspected of spreading dis or mal-information and provide corrections. They would be promoted as a 'trusted' go-to source for citizens to report suspected stories and to fact check campaign claims.
- New government-funded Democratic Digital Defence Teams should be set up to work across key departments and agencies such as the Electoral Commission and Information Commissioner's Office. These units would recruit highly skilled data and social scientists to develop AI early warning systems that would use sophisticated techniques of machine learning and network analysis to spot bots and other malign actors, designed to spread false news during elections.
- Taking a longer view, there needs to be a more concerted and compelling effort to educate the next generation of voters about the need for vigilance when consuming news and information online. A variant of citizenship classes, these would focus on instilling the digital security skills required for voting and particularly ways to distinguish real versus fake news stories. This could be linked to the teaching of a wider set of online skills that are necessary for staying safe online in more general day-to-day activities such as finance and banking, purchasing goods, curation of social media profile content and email etiquette.

Given the wide range of informational 'ills' that digital technology can now release into the political ecosystem, the question arises of what can be done to stem their flow?

While there are no easy answers to the challenging problems we face, governments do now need to get on the 'front foot' in addressing some of the more harmful intended and unintended democratic consequences of digital technologies. A key part of that process of deterrence is detection. Investment in the interdisciplinary research that can deliver on this task is an increasingly vital next step, for governments, the tech industry and academics to take.

Rachel Gibson is a Professor of Politics at The University of Manchester and leads a new EU commission funded project on Digital Campaigning and Electoral Democracy (DiCED). She has a long-standing interest in researching the impact of the internet on political parties, voters and elections.

Citizen's data, healthcare and trust: the need for 'no surprises'

Professor John Ainsworth and Professor Niels Peek

The UK's National Health Service (NHS) has had electronic health records in GP practices for more than 20 years. These records are kept from cradle to grave and, increasingly, electronic records are also being used in hospitals, social care, dentistry, and other parts of the healthcare system. The NHS number provides a unique identifier for each citizen which can be used to link data from different databases together, providing a rich, comprehensive source of real-world evidence. However, its enormous potential for purposes beyond direct care was soon realised and some high-profile cases of data misuse have dented public trust. So, how can we maximise this resource for the benefit of all, and rebuild that trust?

Powerful, useful but highly sensitive

The data in electronic health records (EHRs) is powerful and extremely useful. It can help us improve healthcare services, understand diseases in populations, and assess the safety and effectiveness of treatments. But health is an intimate area of personal life and few people feel comfortable with the idea that strangers can see their health record.

All health professionals therefore have a duty of confidentiality, which means that they cannot disclose this information to others without the patient's consent. A legal framework exists to share EHR data for purposes beyond direct care without needing consent from every citizen. This is the Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR). In essence, it says that all person-identifying information should be removed from personal data before such data is processed for purposes beyond the reasons for which it was originally collected – in this case, healthcare provision.

> **The use of personal health data for uses other than providing care is contentious, because of the lack of public trust.**

Legal cases, headlines and damage to public trust

So, problem solved? Unfortunately, not. The use of personal health data for uses other than providing care is contentious, because of the lack of public trust.

In 2018, the Information Commissioner's Office (ICO), responsible for upholding data protection laws, ruled that the Royal Free Hospital had broken the law when it provided the personal data of 1.6 million patients to DeepMind, a subsidiary of Google. The ICO found no legal basis for the sharing of this data. Clearly, the failure of an NHS trust to follow the law on data sharing with a company that has commercial interests has damaged public trust and confidence. As has Care.data, launched in 2013 with the aim of providing a single national data repository for UK health records. The project soon ran into trouble, with much criticism reported in the national media. A communications plan, which relied heavily on a flyer distributed to every house alongside menus for takeaways, was woefully inadequate. More than 12% of the UK population chose to opt out of the database, and this was not trivial. The programme was finally scrapped in 2016.

A matter of public trust

Why did Care.data run into trouble? Unlike the Royal Free/DeepMind case, no laws had been broken. The problem with Care.data was the lack of public trust. Three objections that cumulatively led to the breakdown of trust have been identified. Firstly, it was unclear in whose interest Care.data had been established. Secondly, it was unclear that this was established for the public good. Thirdly, Care.data lacked reciprocity; data was taken with seemingly nothing offered in return. Non-exploitation, service of the public good and reciprocity are three necessary conditions for a social licence, and hence trust, to use health data for purposes other than providing care.

> **If you were told that an NHS trust was sharing data with a commercial company for a particular purpose would you be surprised?**

A useful way to think of this is through the principle of 'no surprises'. If you were told that an NHS trust was sharing data with a commercial company for a particular purpose would you be surprised? If yes, then something is wrong because it is outside your expectations. The keys to no surprises are transparency, communication and the social licence.

Citizens' juries, public opinion and policy

We have undertaken a novel form of public engagement, called citizens' juries, to try to understand what the public thinks about reusing data from NHS health records for purposes beyond direct care. Citizens' juries are a form of deliberative democracy, based on the idea that people from a variety of backgrounds with no special knowledge or experience can come together and tackle complex public policy problems. A group of citizens, selected to be broadly representative of the general public, deliberate over a clearly framed question and they reach a decision either by consensus or voting. During the course of the deliberation (normally three to five days), the jury will have access to expert witnesses.

We have run two citizens' juries. In the first, we asked the jurors, "To what extent should patients control access to patient records for secondary use?" We found that, when informed of both the risks and opportunities associated with data sharing, citizens believe an individual's right to privacy should not prevent research that can benefit the general public. The juries also concluded that patients should be notified of any such scheme and have the right to opt out if they so choose. Many jurors changed their minds about this complex policy question when they became more informed. Many, but not all, jurors became less sceptical about health-data sharing, as they became better informed of its benefits and risks.

In the second citizens' jury we asked the jurors to evaluate eight scenarios of reusing health data, from improving health service to reuse for private commercial gain. Jury members tended to be more accepting of data sharing to both private and public sectors after the jury process. Many jurors accepted commercial gain if public benefit is achieved. Some were suspicious of data sharing for efficiency gains. Juries elicited more informed and nuanced judgement from citizens than surveys.

Policy principles for the future

We recommend the following policy principles be adopted for the reuse of healthcare data:

- Transparency: Publish every use of data, who data is shared with, and for what purposes. Publish the results of any research on a publicly accessible platform.

- Communication: Actively engage with the citizens whose data you are reusing. Be clear on benefits and risks.
- Maintain the social licence: Only reuse health record data for public benefit and in a non-exploitative manner, with clear reciprocity for the people whose data is being reused.

By following these policy recommendations, we can achieve the aim of 'no surprises' and so maintain public trust when health data is used for purposes beyond direct care.

With such powerful benefits to gain or lose, an ageing population and a national health service under severe pressure, we should make every effort to get this right.

John Ainsworth is Professor of Health Informatics at The University of Manchester and Director of the Health eResearch Centre. He runs a programme of research on enabling the use of sensitive data for research.

Niels Peek is Professor of Health Informatics and Strategic Research Domain Director for Digital Health at The University of Manchester. His research focuses on data-driven methods for health research, clinical decision-making, and healthcare quality improvement.

Risk in a digital age: why solutions lie in people, not just technology

Professor Gerard P Hodgkinson

We live in a digital age. Along with vast and varied benefits, this revolution has brought equally vast and growing risks. From data mining and fraud, to activity that could close a company or even put national security and lives in danger, mitigating these risks is an extremely high priority. But while billions are spent on technological fixes, are we failing to see – and more importantly act – on the psychological, social and cultural factors at play?

A growing problem

An alarming increase in the number of high-profile cyber security breaches shows not just the growth of the problem of cyber crime and hacking, but also the vulnerability of systems that ought to be highly secure. Take the well-documented case of Gary McKinnon, the Scottish UFO enthusiast who hacked into US Military and NASA computers and ended up in a high-profile extradition case, indicted by a federal grand jury on seven counts of computer-related crime. Or the Windows-based computer worm known as 'Stuxnet', which was implicated in the temporary shutdown of Iran's uranium enrichment program observed by UN inspectors in November 2010. It is all too apparent that much of the world's infrastructure and associated data systems are highly vulnerable and inadequately protected. Governments, hospitals, financial institutions, educational establishments, transportation systems, professional services providers, and manufacturing installations alike, indeed, all sectors are susceptible. So what is being done?

In an attempt to safeguard their hardware, software, and data many organisations have sought technical solutions, investing increasingly large sums of money in enhanced antivirus software, elaborate authentication procedures, and associated encryption systems. However, cases such as the ones highlighted above illustrate the ease with which people intent on this kind of activity are often able to overcome such technical 'fixes', no matter how elaborate and seemingly impenetrable.

Learning from history

As ever, we can learn from the mistakes of the past. Many new technologies have been introduced and failed to perform as expected because of a failure to consider human behaviour. A well-known concept, known as 'sociotechnical systems', was pioneered as long ago as the 1950s when researchers looked at why new mechanised ways for extracting coal more quickly, and safely, had not reaped the expected increase in productivity. The reason? This new technology had been introduced without anyone considering that it would dramatically reduce and alter social interaction between the coal miners. The designers of this new technology had unintentionally eroded some of the social psychological benefits of the traditional mining techniques that their innovative machinery replaced.

Many new technologies have been introduced and failed to perform as expected because of a failure to consider human behaviour.

A complex blend of human and machine

It is clear then that digital technologies, like all technologies, are only one half of a more complex system, the technological elements being inextricably intertwined with the human beings who make use of them. Safeguarding the digital infrastructure at the heart of the world's economy, therefore, demands a sociotechnical approach, which seeks symbiotic solutions that blend both technological and human insights. The absence of such cross-disciplinary thinking in organisations risks the development of solutions that place unrealistic demands on employees, leading in turn to 'work arounds' (I'll just 'work around' this) to bypass the burdens of compliance.

If people find a potentially secure system difficult, inevitably, they will be motivated to find such workarounds; all too often, for example, they 'work around' the need to set passwords, thus posing a massive threat to computer security. Gary McKinnon was able to hack into 97 US Military and NASA computers, using nothing more sophisticated than a simple script that could search 65,000 computers for blank passwords in less than eight minutes. Having accessed highly sensitive information through this surprisingly straightforward approach, he then deleted critical files from an assortment of operating systems. The US authorities claimed that his actions rendered the Army's Military District of Washington network of 2,000 computers inoperable for 24 hours. The clean-up operations are estimated to have cost around $800,000, and this figure doesn't include the costs, paid by US and UK taxpayers, of nine years of legal procedures.

It is clear then that digital technologies, like all technologies, are only one half of a more complex system.

Redressing the imbalance

The research my colleagues and I are undertaking here at The University of Manchester is seeking to redress the fundamental imbalance of understanding between the human elements and the technological elements underpinning cyber crime, to find more effective ways of addressing it. Drawing on the insights of anthropology, behavioural science, criminology, and sociology, among other specialist fields, we are working closely with computer scientists, in a wide-ranging programme of multidisciplinary work to augment, and in some cases challenge, some of the more conventional technical approaches designed to enhance digital security and thwart the efforts of cyber criminals.

There are many ideas and areas for further research and exploration. For example, nudge theory in behavioural economics – making it easy for people to embark on desired courses of action – has helped shape all kinds of behavioural change, so why aren't we applying it more often to enhance digital security, one of the most pressing challenges of our times? By designing simple behavioural routines that fit in easily with people's everyday task environments, and avoiding anything too onerous, we will get results that are much more effective.

We also need to learn more about how culture variously gets in the way of or helps to promote digital security and trust. To illustrate, one organisation I have been working with was blissfully unaware that its team of cyber security experts were perceived by many of its managers and front-line employees as an outsider group, 'geeks' who lacked sufficient understanding of the day-to-day realities of people's jobs. The everyday practices and artefacts displayed around the organisation's premises reinforced an overwhelming sense that cyber security was a lower priority than the many other issues it was attending to, resulting in cynicism towards the cyber security team and the policies it enacted. Not surprisingly, cyber security work arounds were commonplace.

Effective communication and education are key. Some of my own research, published more than a decade ago, found that most people could identify risk scenarios of varying seriousness in terms of their consequences or likelihood of taking place. However, serious 'meltdown' scenarios were typically considered very unlikely, whereas scenarios expected to be trivial in their effects were considered very likely. A decade on, it's sobering to reflect on the numerous examples of real-life cyber security breaches that closely match the more serious and consequential ones that our study participants identified as low-frequency, low-likelihood events. Of course, the actual frequency of such events is difficult to measure objectively, not least because organisations don't like to share how close they have come to a major catastrophe or how they have managed to get out of one, so the true scale of this issue is not public knowledge.

There is much work to do to. But in the meantime, there are some simple, practical ways for using behavioural and social science insights to enhance digital security and mitigate the risks associated with cyber crime in the workplace and beyond:

- Consider not just the technology but also how people will interact with it. These are inseparable components of one, sociotechnical system. If either of these essential components fails, then the whole system fails.
- Consult with and incorporate the views of users. This not only has a direct impact on whether people fail to comply (leaving organisations vulnerable); it also has a material bearing on job satisfaction and productivity.
- Make it easy for people to do the right thing – consider how nudge theory and other behavioural science insights and techniques could support your plans.
- Consider how you will communicate why particular cyber security solutions are being implemented and do not assume employees have the requisite prior knowledge. Most people do not have a clear sense of where the risks lie, what those risks really are, and how their behaviour fits into the bigger picture.

In the final analysis no amount of investment can ever eradicate the growing security threats confronting the digital economy. Organisations need to develop routines that assure they maintain situational awareness and adapt their mitigation strategies as threats evolve.

Investment needs to shift towards more social and behavioural science-informed approaches. Governments, businesses and other sorts of organisations need to be better educated on how attitudes and behaviour can enhance, or undermine, efforts to promote digital security and prevent the growing threat of cyber crime.

Professor Gerard P Hodgkinson is Vice-Dean for Research in the Faculty of Humanities and Professor of Strategic Management and Behavioural Science at Alliance Manchester Business School, The University of Manchester. He is leading the Digital Trust and Security Research Cluster addressing workplace security, as part of The University of Manchester's Digital Futures programme.

Social media and mental health: can we trust what we're being told?

Dr Margarita Panayiotou

The relationship between social media and mental health is a hot topic for users, researchers, the media, and government. People are worried. In the light of recent events, it is difficult not to be. Anyone that attended (or followed on social media) the 2019 International Congress of the Royal College of Psychiatrists would have heard that social media is harmful not only for our mental health but also for our 'neurotransmitter deposits'. A South Korean intervention in which young people are sent to boot camp to rid them of their addictions was one speaker's suggestion. We are constantly bombarded with news and information about how social media, screen time, and technology in general are detrimental to our mental health. Some go as far as to suggest these are as dangerously addictive as a gram of cocaine. But can we trust what we're being told?

'Chicken or egg?'

The relationship between social media use and mental health is a complex one and far too understudied to allow us to draw such strong conclusions. So far, there has been some evidence to suggest that frequent use of social media platforms in adolescents is linked to increased symptoms of depression, suicide rates and overall psychological distress. These findings are often portrayed by the media using attention-grabbing headlines such as in the Guardian in 2018: "Are smartphones causing more teen suicides?" But when you look closely at the evidence you realise that such strong correlations are flimsy. Why? Well, first, much of the evidence is based on cross-sectional data, meaning all data was collected at a single point in time. In short, there is no way of knowing if increased social media use causes increased symptoms, or the other way around – the classic 'chicken or egg' situation.

Even when longitudinal data is used, the link between social media use and mental health is found to be trivial and possibly random (for instance due to large sample sizes). Indeed, robust evidence is starting to paint a different picture: the role of social media use in young people's mental health, wellbeing and life satisfaction is very small to non-existent.

> **Even when longitudinal data is used, the link between social media use and mental health is found to be trivial and possibly random.**

Addictive behaviour

Another flaw of the current evidence is the way social media (use) is measured. Researchers primarily ask questions about the time spent online during a typical day or week. However, we know that these questions are sub-optimal, as they are based on arbitrary criteria and do not adequately capture individuals' usage patterns and behaviours. In other cases, researchers use questionnaires that measure 'addictive social media use'. This is highly problematic for two reasons: first, the classification of social media use as an addictive disorder is based on anecdotal evidence; second, many of these measures, on which some of the current conclusions are based, were developed based on gambling addiction and nicotine dependence diagnostic criteria, which possibly include

entirely different behaviours. It's not surprising then, that addictive social media use is linked to psychological distress, given that they share substantial measurement and conceptual overlap. Indeed, where more robust measures have been used (eg smartphone data), the evidence – although new and in need of replication – points to the opposite direction: young people report better wellbeing and mental health on days when they were more active on social media.

Moral panic and misinformation

So, can we trust what we're being told? The answer is: not always. Blaming social media for young people's increased rates of poor mental health is very compelling, especially given the increase in technology and social media use. However, social media use may not be the culprit, much in the same way the body of research suggests that violent video games do not seem to cause increased aggression. The evidence is simply not sufficient.

There are no studies examining social media use and depletion of 'neurotransmitter deposits.' What is more, sending young people to boot camp to rid them of their addictions or calling for laws to ban social media for young people under 13, at a time when we are no way near classifying social media as an addiction, would be like speeding up, when we don't even know if it's a dead-end road.

What we can do

The good news is more robust research is starting to shed some light into this complex relationship, so instead of giving in to unjustified moral panic, there are a few things we can do instead.

First, we need to be more critical of existing claims. While it is often difficult to untangle misinformation or poor research from robust evidence, one thing is sure: research on social media use is new, underdeveloped, and inconclusive. It is therefore wise to take things with a pinch of salt.

Which brings me to my second point: improved research is urgently needed. This is in fact one of the key issues raised by the UK House of Commons in a 2019 Green Paper on the impact of social media and screen use on young people. We need better measurement and more accurate data. The latter cannot be achieved without the former, which is why the role of big tech companies might be more crucial than we think. Social media companies such as Facebook hold very rich data regarding their users' behaviour, which they use for their own research purposes. Requiring these companies to share their data with independent researches will not only enable us to tackle some of the methodological challenges we are faced with, it will start untangling the complex relationship between social media use and mental health and bring overdue accountability.

> **Research on social media use is new, underdeveloped, and inconclusive. It is therefore wise to take things with a pinch of salt.**

Until that happens it is unwise and dangerous to rush into strong conclusions or radical policy changes. After all, we still do not know what it is we are trying to change. Instead, we should focus on educating people. This is not a pioneer suggestion. The Children's Commissioner has repeatedly called for a compulsory digital citizenship curriculum in schools. Instead of censoring, banning and sending kids to addiction boot camps, all of which assumes that social media addiction is a fact, why not focus on increasing evidence-based social media awareness and giving young people tools and tips for self-regulation?

In a report by The Royal Society for Public Health and the Young Health Movement, eight in ten young people agreed with this. We should listen to them, not alienate them from life-impacting, decision-making processes. We have the tools and responsibility to do better than that.

Dr Margarita Panayiotou is a Research Associate at the Manchester Institute of Education. Her research interests include social media, mental health and psychometrics.

How the digital space oils the wheels of unlawful and unethical business

Professor Nicholas Lord

Imagine you are involved in criminal, unlawful or unethical activity that makes serious money for you or your employer. You might, for instance, be a public official awarding procurement contracts, who extorts or accepts substantial bribes and hides them in overseas bank accounts. Or perhaps you work for a multinational corporation that systematically and aggressively avoids tax liabilities in its home country, using schemes that exploit transnational legal mismatches to shift profits to lower tax jurisdictions. From individual and corporate elites, to those implicated in organised crime, the vast global flow of illicit and unscrupulous financial activity is now a priority policy issue for governments and societies worldwide. And, as indicated in the United Nations Sustainable Development Goal 16.4, there is particular concern with the illicit movement of money out of low-income economies and the role those working within wealthier ones are playing in this. So how is it done and what can we do about it?

Keeping secrets

In this murky world of dodgy dealings, those individuals and corporations implicated will seek to keep, if necessary, their illicit finance secret from regulators or enforcement authorities. So how do they hide their identity in order to protect their assets? How is this finance converted into what looks like legitimate money for use in legal markets? And how has the digital space influenced how these objectives are accomplished?

Individual and corporate actors need mechanisms for concealing, converting and/or controlling the illicit finance generated from their activities if they wish to use this wealth for purchasing assets, such as houses and cars, or services such as private school tuition fees, to reinvest into business activities or protect their reputations (eg unauthorised tax avoidance, which is lawful but unethical).

‘Corporate vehicles’ and the global financial system

The University of Manchester’s Corporate Vehicles and Illicit Finance project, run in partnership with Police Scotland and the Centre for Information and Research into Organised Crime (Netherlands) is the first such study in the UK to be looking into this. Our research has demonstrated that one way to accomplish the concealment and control of illicit finance is by using so-called ‘corporate vehicles’ – a term used to refer to an array of legal structures such as companies, trusts, partnerships, and foundations. Such vehicles enable a range of commercial activities including the control and movement of wealth and assets within the financial system. For instance, they permit businesses to incorporate companies in low or no tax regimes, provide flexibility in global markets, and reduce the level of regulation, particularly when set up in jurisdictions that offer great confidentiality.

Individual and corporate actors need mechanisms for concealing, converting and/or controlling the illicit finance generated from their activities if they wish to use this wealth for purchasing assets.

Large flows of monies move through the global financial system via such vehicles and this has become a central feature of business in market-based economies.

However, the Panama Papers leak in 2015, the Paradise Papers leak in 2017, the Mauritius leaks in 2019, and subsequent investigative journalism have illustrated how such legal structures are being misused and abused for illicit purposes, such as the evasion and avoidance of tax by wealthy individuals, the concealment of corrupt funds by public officials, and money laundering, amongst others. These issues have come to the fore globally, but also in the UK specifically. For instance, in 2017 Transparency International found that UK companies have been implicated in facilitating the hiding of illicit wealth and assets and corruption around the world, whilst the National Crime Agency estimates money laundering costs the UK more than £100 billion a year. The movement of illicit finances into the UK property market is also of concern: according to international NGO Global Witness, over £100 billion worth of properties in England and Wales are owned by anonymous companies in overseas tax havens, whilst in 2018 Transparency International identified £4.4 billion worth of UK properties bought with suspicious wealth.

Research evidence

Our research found strong evidence for three key propositions: firstly, that corporate vehicles create an illusion of legitimacy through the abuse of otherwise lawful business arrangements including fabricated financial arrangements and contrived ownership structures; secondly, they provide anonymity for the beneficiaries of illicit assets and insulation from enforcement, making illicit finance virtually untraceable, particularly when organised across jurisdictions that provide great secrecy, or confidentiality; thirdly, these schemes are most often accomplished with the witting collusion or sometimes unknowing (or wilfully blind) assistance of third party legal, financial and other professionals, including company formation agents or trust and company service providers. These professionals help manage other people’s ‘dirty money’, whether generated by commercial enterprises or organised crime groups. In all the cases we have come across, corporate vehicles provide opportunities for managing illicit finances that individuals alone cannot access.

Easing corruption through digital technology

The core matter here is that the digital space has significantly eased how corporate vehicles can be misused by enabling quick, online company formation via transactions that are conducive to anonymity and has opened access to such misuse to a much wider array of individuals. As evidenced by our own research and the World Bank, amongst others, it is now straightforward for anyone to obtain anonymous corporate vehicles at reasonable cost and quickly, online.

As evidenced by our own research and the World Bank, amongst others, it is now straightforward for anyone to obtain anonymous corporate vehicles at reasonable cost and quickly, online.

An internet search will find numerous providers of company formation and registration services, plus more. Bank accounts for these companies can then be opened in foreign jurisdictions without having to go there physically. For those implicated in serious financial crimes including those who facilitate it, the ease of the process opens up new opportunities for creating and controlling illicit finance and hiding the identity of the beneficial owner. Furthermore, the boom in online-only companies that offer company formation services has created a lucrative market that caters for varied clientele.

Whilst the transition from paper-based to digital-based company formation systems and services should also make it possible for enforcement authorities and regulators to obtain information on who owns, controls and benefits from these companies, there are currently major gaps in terms of the data available and how they are scrutinised. The sheer number of vehicles being created in this way makes it difficult for the identity of beneficial owners to be established. Regulatory non-compliance often goes unchecked due to an under-resourced and poorly mandated Companies House in the UK, as acknowledged in the UK Government's Corporate Transparency and Register Reform consultation of 2019. We also have a fragmented regulatory system that involves over 20 responsible regulators, such as HMRC, the Financial Conduct Authority and varied professional supervisory authorities.

> **Currently the digital landscape enables any person anywhere in the world to form UK companies that can be used as vehicles in laundering illicit finance.**

Regulations and policy measures

UK Government rhetoric recognises the need for corporate vehicle misuse to be addressed (as can be seen in the 2017 HM Treasury/Home Office Risk Assessment into Money Laundering and Terrorist Financing), and this issue was also highlighted in the Financial Action Task Force's (FATF) 2018 evaluation of the UK's anti-money laundering measures.

In policy terms, a plausible route to minimising misuse is to focus on a) professional intermediaries by improving the regulation and supervision of them to reduce opportunities for misuse by their clients, and b) tightening laws and regulations on how and where corporate vehicles can be created.

Currently the digital landscape enables any person anywhere in the world to form UK companies that can be used as vehicles in laundering illicit finance. In the short-term, making it a requirement for only licensed and regulated company formation agents to have the capacity to form corporate vehicles could improve the validity of registration data, ensuring enhanced due diligence of client wealth, and minimising misuse by foreign agents. Such reform initiatives are underway in the UK, eg in relation to the misuse of (mainly Scottish) limited partnerships, but there must be enough resources and mechanisms for enforcing this and they must apply to all forms of corporate vehicle.

In the medium to long-term, I would like to see the creation of a new UK Screening Authority to act as a centralised authority with the budget and scope to regulate company registration data (including foreign ownership) and undertake due diligence on the creation of all vehicles. This would remove the burden on Companies House and reinforce political commitment to addressing 'dirty money' flowing into, from and through the UK and its overseas territories. We see a similar authority in the Netherlands with the Judicial Agency for Testing, Integrity and Screening under the Ministry of Justice and Security, which is responsible for assessing the reliability of people and organisations.

> **We must do more to prevent the movement of illicit finances, and this implies the need for substantial financial investment in enforcement.**

A serious challenge

Awareness as to the nature (eg the role of 'legitimate' actors) and seriousness and harms of corporate vehicle misuse needs to be raised, particularly within political spheres, as governments seek to protect economic interests whilst also appeasing pressure to respond. For instance, finances stolen from public funds in low-income countries that flow overseas significantly impact on investment opportunities in local infrastructure, diverting money that could be spent on health, education, transport, etc, not to mention in some cases jeopardising financial stability in these places.

Similarly, the flows of illicit finance elsewhere can distort legitimate markets, such as creating booms in house prices and in turn forcing low-income individuals out of their local areas. Yet state responses remain frustratingly piecemeal and lack sufficient vigour, but then as the leaks mentioned have demonstrated, individual and global elites, such as politicians and business leaders, have also benefited from these secretive financial arrangements.

Due to these tensions, there is a lack of urgency to create regulations that reduce the scope for these structures and vehicles to be misused. We must do more to prevent the movement of illicit finances, and this implies the need for substantial financial investment in enforcement, to support the punitive rhetoric, and recognition that both private and civil society organisations have a role to play in this.

Lastly, governments need to be challenged to take a much stronger position on this issue within conversations about creating an attractive economic and fiscal climate for businesses.

Nicholas Lord is Professor of Criminology in the Centre for Criminology and Criminal Justice (CCCJ) at The University of Manchester with research expertise in white-collar, financial and organised crimes, such as corruption and fraud, and their regulation and control.

Why victims of cyber crime deserve ‘Cyber CPR’

Professor Emma Barrett, Professor Danny Dresner and David Buil-Gil

Recovery support for victims of cyber crime is unevenly distributed. Large organisations can call on the resources of the state, whereas support for the thousands of ordinary victims is scarce. The impact on citizens’ security and trust can be profound. It’s time for an urgent focus on everyday cyber crime victims.

Financial cyber crimes are rising rapidly in scale, complexity and social impact. The 2017 Annual Fraud Indicator estimated that frauds represent a cost to the private sector of £140 billion a year, the public sector £40 billion, and individual citizens £6.8 billion. Over half of all frauds are committed online. How are these crimes perpetrated, and what impact do they have on ordinary victims?

Insecurity, opportunity and exploitation

Criminals profit from information insecurity and poor cyber hygiene. Use of insecure passwords puts you at risk. But even a strong password won’t help if the website you’ve entrusted your data to doesn’t adequately protect it – if it’s hacked, your details can be leaked. Cyber criminals can then use an automated technique called ‘credential stuffing’: trying your leaked email/password combination on multiple websites, in the hope that you reuse the same credentials (as many of us do). And there’s phishing emails containing links to sites which can trick you into revealing your login details for banking or other potentially lucrative sites.

> **Use of insecure passwords puts you at risk. But even a strong password won’t help if the website you’ve entrusted your data to doesn’t adequately protect it.**

As well as exploiting our mistakes, cyber criminals have an array of psychological tricks up their sleeves. For instance, they take advantage of periods of consumer uncertainty when organisations are disrupted. The massive IT failure that prevented British bank TSB’s customers from accessing their accounts, the 2018 breach of British Airways’ customer data, and the collapse of Thomas Cook in 2019, were all opportunities for cyber criminals to exploit customer fears. Consumers received phishing emails, warning them to update their credentials immediately, with a link to an authentic-looking but bogus website. Even access to a victim’s IT is not essential. Posing as trustworthy representatives from the affected organisation, criminals phone potential victims, arguing convincingly that the only way to avoid loss in a follow-on attack is to transfer money to a ‘safe’ account, which, of course, belongs to the criminals.

And then there are internet-age blackmail schemes and hustles. ‘Sextortion’ criminals and dating fraudsters deliberately engage in the construction of trust with their victim, sometimes over weeks or months, with the express intention of betraying it. In the case of dating fraud, where a criminal feigns a romantic attachment, the realisation of what has happened can leave victims not just financially but psychologically devastated.

In every case, cyber criminals get at your cash by exploiting your trust: trust that people won’t try to steal your password, trust that a company will keep your data safe, and trust that the person you’re

interacting with online is who they say they are and is being honest about their motives.

The emotional impact of cyber crime

Interpersonal cyber crimes are a betrayal of trust, and the emotional impact of 'cyber betrayal' can be as profound as betrayal in the physical world. Victims have reported feeling distressed, anxious, powerless and angry. They can become depressed, even suicidal, and lose trust in others. One victim of a dating scam told researchers she found the experience so traumatic she likened it to being "mentally raped".

A common and corrosive reaction is embarrassment. Victims may ask themselves if they might have been partly to blame. If you trust a stranger and they let you down, does it say more about you and your gullibility than about the cruelty of your betrayer? Were you guilty of 'blind faith'? An employee of a company already in financial difficulty was devastated at the thought that she had let colleagues down when she realised she'd entered company credit card details into a bogus site.

In dating scams it's particularly hurtful to realise that a relationship apparently built on openness, intimacy, and trust is instead founded in deception. And the potential that the situation might become public, opening the victim up to ridicule or pity, can also evoke deep feelings of humiliation.

Shame has consequences. Victims may be reluctant to confide in people around them, who might otherwise offer practical and psychological support in the aftermath of a crime. And they may also fail to report crimes to the authorities for fear of ridicule or belief that police would do nothing. No wonder cyber crimes are vastly underreported.

Interpersonal cyber crimes are a betrayal of trust, and the emotional impact of 'cyber betrayal' can be as profound as betrayal in the physical world.

Unsurprisingly, cyber crimes can leave people fearful. Those with prior experience of being a victim tend to be most fearful of such crimes, according to a recent European study. Fear can corrode trust, even in people who might be trying to help. Some victims might be afraid of ever logging on again.

How can people become resilient to the effects of an attack? We need the ability to recover quickly: technically (cleansing devices, software and data to erase any malware), financially (regaining control of bank accounts and plugging the holes), and psychologically.

Asymmetry of support

The National Cyber Security Centre (NCSC) has responsibility for supporting cyber security in the UK, and when large organisations fall victim to cyber-attacks, it steps in to help. The scale of resources devoted to mitigation, investigation, and recovery depends on which of six categories the incident falls into, from a 'Category 1 National Cyber Emergency' to a 'Category 6 Localised Incident'. The most serious, nationally important incidents (such as the 2017 NHS ransomware attack) prompt a specialist incident response, drawing on a vast array of government resources, working with investigators in NCSC's parent organisation GCHQ to identify the attackers, coordinating with overseas partners, and helping the victim organisation get back up and running. Even a 'Category 4 Substantial Incident' affecting a medium-sized organisation may qualify for NCSC support.

But what about everyday victims – small businesses and ordinary citizens, for example? They're in categories 5 and 6. They will be told to report the crime to Action Fraud, the national reporting centre run by City of London Police alongside the National Fraud Intelligence Bureau, who will then allocate the case for investigation.

The scale and complexity of cyber crime is such that a report may be logged and even passed to local police, but they may not have the resources to investigate.

Or so you would like to think. In practice, the scale and complexity of cyber crime is such that a report may be logged and even passed to local police, but they may not have the resources to investigate. Fewer than one in fifty reports results in a suspect being caught, and a 2019 undercover enquiry by The Times newspaper revealed that contractors used by Action Fraud to collect reports treated victims, often defrauded of huge sums, with disdain. Once they put the phone down, call handlers reportedly mocked victims as "morons", "screwballs" and "psychos". No wonder victims told The Times they felt ignored and disrespected. If this is how victims perceive they will be treated, trust will further be eroded. Anger, humiliation and anxiety will be associated with the authorities, as well as the cyber criminals.

Cyber CPR

The Government's Victims' Strategy, published in September 2018, includes welcome support for victims of crimes, and a raft of proposals to improve victims' experiences throughout the investigation and court process. However, cyber crimes are notoriously difficult to investigate due to the global and largely anonymous nature of cyber space, and even the best-resourced criminal justice system will struggle to prosecute all successfully. When it comes to how to support victims of cyber crime, the Strategy has very little to say.

As well as doing more to support the effective investigation of cyber crime, we also need to invest in helping victims recover – practically and psychologically – in circumstances where prosecution is not possible. We need to recognise that most citizens who fall victim will have little by way of protective or contingency methods. Whilst resources to recover will be at hand for critical infrastructure, food, and finance, ordinary people who have suffered an attack may find themselves excluded and unable to engage with public services, shopping and entertainment, banking and other financial services. A proliferating quagmire of prevention advice is often difficult to navigate, conflicting, and ironically assumes that the person needing it will have internet access, when in practice they may have lost all safe access or may be too nervous to log back online. Many will not have alternative resources to turn to; cyber-attacks, therefore, create a new kind of digital exclusion.

It's time to consider giving unprepared citizens the capacity for self-help. We propose development of a 'Cyber CPR kit' with advice and tools to help victims recover. Local police cyber crime units may be the ideal owners and distributors of this in the first instance, and it could become an offering from local cyber resilience centres of the type already established in Scotland, London, and Manchester.

A recovery kit needs to be practical, recognising that victims' work and domestic lives are dependent on multiple digital accounts, including banking, social media, and e-mail. And they might rely on multiple devices to access these: laptops, tablets, smartphones, as well as 'Internet of Things' devices such as cameras and Fitbit-type devices. An increasing number will depend on internet-enabled critical medical equipment such as pacemakers and insulin pumps. Some or all of this will be unavailable after an attack. Cyber CPR should recognise that a victim may be cut off from internet-based services, including those that can help recovery when a problem occurs. The kit may contain a variety of technical fixes and advice for quick action (think 'sticking plasters') and powerful recovery tools (think 'defibrillator' or 'EpiPen').

Cyber CPR should recognise that a victim may be cut off from internet-based services, including those that can help recovery when a problem occurs.

Most of all, the design of the kit needs to be humane. It should demonstrate empathy with the psychological and emotional suffering experienced by victims and provide practical steps to help them rebuild trust. This means explaining that the maelstrom of emotions they may be feeling is normal, encouraging them to use social support and, where victims are socially-isolated, providing such support. It means being honest about what the police can and cannot do, but reassurance that they are doing the best they can.

The crime may be virtual. The harm is real.

Emma Barrett is Professor of Psychology, Security and Trust and The University of Manchester Strategic Lead for Digital Trust and Security. She is also Director of SPRITE+, the EPSRC NetworkPlus for Security, Privacy, Identity and Trust.

Danny Dresner is Professor of Cyber Security at The University of Manchester. Danny is also a founder and director of the IASME Consortium which champions cyber security for small businesses and runs a cyber security programme for neurodiverse individuals, employing them in a community security operations centre offering security oversight for charities, SMEs, and vulnerable people.

David Buil-Gil is a Research Fellow in cyber crime at the Department of Criminology of The University of Manchester. His research interests cover environmental criminology, crime mapping, emotions about crime, new methods for data collection and open data.

Beyond privacy and security: opening-up 'trust' in digital healthcare

Dr Barbara Ribeiro

Digitisation is a phenomenon that has been transforming the way we live and work. Today, ubiquitous devices that generate, interpret and share digital data are increasingly mediating our social relationships and our interactions with organisations. While innovation often promises a brighter future, the use of digital technologies is permeated with challenging questions around its effects on everyday life, public benefit and, ultimately, public trust in these systems. The digital healthcare sector is no exception.

New technologies and trends

The term digital healthcare refers to those forms of health or social care delivery that are mediated by digital technologies, such as telecommunications and sensing technology that allow patient assistance, for example by triggering a control centre to try to make contact and to get help if there's no answer. It is supported by devices like electronic medical records, wearables and data analytics software.

Digital technologies support three approaches to healthcare: preventative, predictive and personalised. Preventative healthcare consists of taking measures that avoid the development of health conditions through monitoring of things such as blood glucose, medication adherence and physical activity; predictive approaches make use of data analytics to assess the likelihood of developing conditions such as dementia; while personalised healthcare seeks to combine our genetic and clinical information to deliver tailored treatment on an individual basis.

In the context of digitisation, our understandings of health and healthcare are at risk of becoming reduced to what is simply health data.

The informatisation of medicine and the rise of data

Digitisation in healthcare is part of a broader process of informatisation of medicine; one where digital data plays not only a fundamental but a lead role. This process is underpinned by trends in genomics, physical and behavioural sciences and the assumption that our bodies – and their 'illnesses' – are best assessed via our DNA and various forms of metrics.

In the context of digitisation, our understandings of health and healthcare are at risk of becoming reduced to what is simply health data. Policymakers tend to reinforce the focus on health data by prioritising issues such as confidentiality, anonymity, privacy and security which become dominant in public debate. As a consequence, the ethics of digital healthcare – that is, what we deem as matters of interest and concern to society – are mainly framed in data-centric terms. For instance, a policy paper produced by the UK Government in 2018 on the future of digital healthcare puts forward an ambitious vision for the implementation of digital technologies. This vision is accompanied by principles of social inclusion and a focus on user needs, which are definitely matters of social interest. However, aligned to the idea that health means data, potential public concerns are seen reduced to privacy and security issues in the Government's parlance, at the expense of much wider issues around how technology is affecting healthcare and what impact this is having on patients.

Are we confusing trust with agreement to share?

How is this happening? Despite the undeniable importance of privacy and security, public trust has also become primarily defined in these data-centric terms. The short-lived Care.data programme launched by the NHS a few years ago, which was the subject of a public backlash over the use of patients' data by the NHS and its partner organisations, helped frame the debate on trust and the future of healthcare around privacy and security.

Despite the undeniable importance of privacy and security, public trust has also become primarily defined in these data-centric terms.

Care.data follows a trend of supply-driven, top-down approaches to the implementation of health innovation in the NHS. Here, we might end up confusing a complex concept such as trust with acceptability: we assume that people will either reject or embrace a programme that was imposed in a top-down manner like Care.data, based on how much they agree to share their data with public and private organisations.

A 2018 survey found, for example, that older people are generally more reluctant than younger groups to use an app or fitness tracker to self-collect lifestyle data and to have their data shared with private organisations for research purposes. This does not tell us anything about the reasons why these people might be reluctant, but because most of us know very little about, or are unaware of, how organisations use our health data (something that the same survey shows), we too quickly jump to claim that a lack of this knowledge is the main reason behind a lack of public acceptance and, therefore, of public trust (something that the same survey does).

When thinking about trust in digital healthcare we therefore tend to take two shortcuts that support and justify the focus on privacy and security issues, like the one adopted by the UK Government in their vision for the future of healthcare. The first is the assumption that trust means acceptability or people's agreement in sharing their data; the second, which follows from the first, is the simplified explanation that the main reason why people might be wary of sharing their data is only because they lack knowledge on how their data will be used.

Trust, assumptions and what's missing

So, what's missing here? I'd argue that what we rarely do is ask how the very nature of healthcare is being transformed by delivery through digital technologies and how people make sense of and value these new forms of healthcare. We need more nuanced and rich understandings of trust across different publics, practices and spaces.

Take, for instance, the case of insulin pumps, a technology to support self-care practice that is used by people living with Type 1 diabetes. Research into use of insulin pumps found that some insulin pump users have experienced a change in their relationship with healthcare practitioners and family caregivers after they adopted the technology; others felt frustrated by not seeing their high expectations materialise; some perceived a lack of control over the technology; and some even struggled with an increased awareness of their own body. Insulin pumps are not digital technologies, but these are the kinds of issues that shape people's acceptance of new healthcare technologies and, ultimately, their levels of trust in these and, importantly, in those involved in their care.

Digital technologies not only influence the relationship between caregivers and patients, they can also transform the way practitioners work and, fundamentally, change the nature of healthcare. Research has shown that these technologies change where care takes place and contact between people, producing new forms of monitoring, communicating, controlling, advising and attributing responsibilities in care practices.

We should challenge the assumption that digital healthcare technologies are simply new means of delivering the same form of care and learn more about what new forms of care are being created.

Because trust is embedded in our social relationships and our relationships with technological systems, these are the areas health policymakers must pay more attention to, in addition to data privacy and security issues.

Dr Barbara Ribeiro is Presidential Fellow in Innovation Management and Policy at the Manchester Institute of Innovation Research at Alliance Manchester Business School, The University of Manchester. Her research focuses on the societal and ethical aspects of emerging technologies.

The age of data: the death of privacy or its solution?

Professor Mark Elliot

The burgeoning digital economy is evolving at a fantastic pace. Plummeting data processing and storage costs have provided online companies with unprecedented opportunities. At the same time, these parallel developments continue to heighten public concern about online privacy. As more aspects of people's lives become digital, the protection of privacy continues to vex policymakers of most countries. Whilst companies and governments are becoming increasingly sophisticated in the ways they collect and claim ownership of personal data, the commercial and political value of personal data is increasingly recognised.

In this context, ensuring privacy can seem like using a finger to plug a hole in a dam. Available evidence clearly shows how privacy remains important to citizens of the information society. Internet users, however, also want access to the services and products of the digital economy in a convenient and personalised way. Liberal democracies, such as the UK, are caught between inherently valuing privacy and its fundamental connection with democracy, and perceiving privacy as a barrier to their becoming fully functioning digital economies.

The data transformation

The phenomenon often misnamed 'big data' is central to this. Misnamed because the term big data fails to capture the all-encompassing nature of the sociotechnical transformation that is upon us. Many who use the term, qualify it by stating that big data is not just about volume but also other features: that data can be captured, updated and analysed in real-time and that it can be linked through multiple data capture points and processes.

The term big data fails to capture the all-encompassing nature of the sociotechnical transformation that is upon us.

However, such characterisations are not sufficient; they still express the notion of data as *something we have* whereas the reality and scale of the data transformation is that data is now something that we are *becoming immersed* and *embedded in*. Our behaviour is increasingly documented and collated. Hence, we are now living in the *age of data* (a new historical phase that large parts of the global economy has now entered), where each individual is embedded in the *data environment*.

The problem with existing solutions

Existing solutions for obtaining analytical value from data whilst protecting people's privacy, are increasingly challenged by this new data environment. Some believe that they simply no longer work. Even the more recent data-centric technical solutions (such as differential privacy) still struggle with the intrinsic tension between the apparently opposing constraints, which can be summarised as: exactly the feature that makes data valuable to analysts and policymakers also makes it risky.

Beyond this technical issue lies an even more fundamental problem. Data-focused solutions do not in fact directly tackle the privacy problem. Even the so-called differential privacy is not actually a privacy solution.

The cause of this is a critical misunderstanding about the difference between confidentiality and privacy. Privacy concerns people and the control that we each have over ourselves, lives, space and possessions. Privacy is not primarily about data. Confidentiality, on the other hand, is all about the data.

Confidentiality can be viewed as a boundary maintained through various combinations of law, security infrastructure and governance, social norms and practices. When I say, "I am telling you X in confidence", I am asking you to agree to a confidentiality boundary that surrounds the two of us. When an organisation places information on a secure server, it is doing so in order to prevent unwanted dissemination beyond its boundaries.

Confidentiality can be viewed as a boundary maintained through various combinations of law, security infrastructure and governance, social norms and practices.

Now, breaches of confidentiality may indeed have significant privacy implications and increasingly who has control over digital information about individuals is a matter of privacy. But this privacy concern is simply not addressed by putting in place another confidentiality fix. We need to tackle it directly. Fortunately, the technology to do this is now available. Implementing it, as a society-level solution, requires significant policy commitment.

The political will for a new way forward?

To describe it simply, the proposition is this: there should be one source of data for each individual and that is the individual themselves. The concept of personal data stores has been around for a while, and there has been some tinkering around the edges, but the primary problem is the lack of political will for a full implementation.

The system would work like this: each individual would have an internet-based privacy avatar which would act as gatekeeper for their personal data store. The individual would set their own digital privacy policy and every digital interaction would be mediated by the avatar checking the privacy policy of the individual against that of the credentials, intentions and trustworthiness of the other party. Where there was clash between the privacy policy of an organisation requesting temporary access to (certain parts of) the personal data store, the transaction would be refused. Where the individual's privacy policy did not cover a particular request, the individual would be consulted directly.

The implications of such a system are manifold and it is outside the scope of this brief piece to go into all the details, but a few headlines are:

- **The law.** The current range of data protection law becomes irrelevant. Instead, criminal law around data abuse and fraud would need to be strengthened. Abuse of data (including one's own) should be a crime with the same legal weight as physical abuse.
- **Education.** The system implies a step change in the level of digital literacy. This is sorely needed in any case; if we are to truly have an information society then that implies digital citizens.
- **Existing databases.** Current estimates suggest that the average citizen in the UK is on hundreds, if not thousands, of databases. The simplest way to deal with most of these is to let them wither on the vine. As the data in them ages it will rapidly become unusable. There may remain residual societal functions that, at least initially, require some data to be held elsewhere (eg policing and national security). This could be dealt with in the same way that statutory rights to enter a home is handled in current law (and should be a clearly stated and legally regulated exception rather than the norm).
- **Security and system resilience.** A single unique copy of each individual's data implies a single point of failure and early versions of the system are likely to require multiple back-ups (just as every organisation does with its existing data).

The critical point here is that all of these issues can be dealt with in a way that makes the net effect a positive development over the existing arrangement, which you might regard as a mixture of the Wild West and increasing control, by robber barons. Another model that is being explored, developed and honed by China, is the effective control of information flows by a centralised state.

If we do nothing, then one of these two scenarios – digital anarchy or heavy-handed state control – looks increasingly likely to dominate our political economy. The work needed to deliver our proposed alternative is significant, but the prize is a fully functioning information democracy. What is needed is the political will to explore the ramifications, carry out the required research and development, and invest in the necessary infrastructure. Alongside this, governments need the courage to embrace the opportunity of the democratic data transformation.

Mark Elliot is Professor of Data Science within the School of Social Sciences at The University of Manchester. His research focuses on confidentiality and privacy and the use of data science and AI.

Analysis and ideas on trust and security in a digital age, curated by Policy@Manchester

Digital Futures connects University of Manchester researchers into transdisciplinary communities focussing on society's most important problems and drawing on our cross-cutting research strengths.

The online version of this publication contains links to the sources of evidence cited in the publication. To view this version and see the links, visit https://www.policy.manchester.ac.uk/publications/

Read more and join the debate at
http://blog.policy.manchester.ac.uk
https://www.policy.manchester.ac.uk/

@UoMPolicy
#OnDigitalTrust

The opinions and views expressed in this publication are those of the respective authors and do not necessarily reflect the views of The University of Manchester.

November 2019

The University of Manchester
Oxford Road, Manchester
M13 9PL

www.manchester.ac.uk

policy@manchester

Design and layout coppermedia.co.uk
Additional editing by Katie Brewin Consulting

The University of Manchester
Oxford Road
Manchester
M13 9PL

www.manchester.ac.uk

Royal Charter RC000797