Stephen Deadman - Group Privacy Officer and Head of Legal – Privacy, Security & Content Standards at Vodafone Group

The Future of Privacy

The Global Challenge

The right to privacy finds its expression in all the major international human right instruments. They were all, without exception, drafted and agreed in different times to those we find ourselves in today. Even as we contemplate the years ahead, there is almost universal acknowledgement of the continuing value and relevance of these instruments and the rights enshrined. Yet, the subject of privacy has never been more in flux, facing a seemingly endless barrage of pressures. Privacy is becoming one of the most vexing public issues of our time, and will remain so in 2025.

Contemporary concerns and debates about privacy are essentially debates about technology and the role and impact of technology on our lives and societies. Practically every mega-trend in the world of technology is creating tensions for privacy, personal freedom and autonomy - ubiquitous connectivity, big data, the cloud, wearable tech, artificial intelligence, the internet of everything, connected health, drones – the list goes on.

It's no longer just a case of leaving digital footprints from our movements around a digital landscape. As the size of computing continues to shrink to nanotech levels, and the cost continues to fall, technology will become embedded in both the physical world and our physical bodies. We will be living in a world where we are 'surrounded by computational intelligence'[1].

Technology is becoming invisible. And its unobtrusiveness will aid its pervasiveness – there are already estimated to be 16 billion connected objects today and this is predicted to reach 40 billion by 2020[2]. And this pervasive connected technology will create ever more data. IDC estimates that by 2020 people and connected objects will generate 40 trillion gigabytes of data that will have an impact on daily life in one way or another[3] . This data will make known about us things that were previously unknown or unknowable (including to ourselves). And in doing that, it will enable actions and decisions to be taken about us that will have profound consequences far beyond the display of adverts on our variously sized screens, or personalised pricing based on profiles of our income and propensity to pay .

Evgeny Morozov, the author[5] and researcher, gave an example of this recently in his talk at the Observer Ideas festival 2014 in London[6]. In the Philippines, sensors have been placed in public toilets which emit an alarm if someone uses one of the stalls and then tries to leave without using the soap dispenser. You can only turn off the alarm by using the soap dispenser. The sensor thereby has a deliberately regulating effect on the behaviour of users, in this case encouraging hand washing. This is just a logical extension of the seat belt alarms fitted to most new cars built today or the use of speed cameras, the purpose in both cases being to use

Knowing The Unknown
By 2020 people and connected objects will generate 40 trillion gigabytes of data that will have an impact on daily life in one way or another. This data will make known about us things that were previously unknown or unknowable (including to ourselves).

futureagenda.org

What do you think? Join In | Add your views into the mix

Value of Data
There is undoubtedly a huge economic incentive to generate and collect data from whatever sources it becomes available. As more data from more things becomes available, we can expect to see a data "land grab" by organisations.

technology to regulate our behaviour and thereby reduce injury and the cost to health services of car accidents.

Let's stick with cars for a moment. The installation of a wide range of new sensors in vehicles is already transforming other aspects of motoring, such as insurance. Usage based insurance schemes utilise sensors that collect data on location, speed, braking and acceleration to determine the risk profile of the driver, and consequently their insurance premium. The other touted benefit is that such technology acts to discourage risky driving behaviours. In return, we subject ourselves to a degree of surveillance. It is not long before we can see the same technology being used for other ostensibly worthy purposes, e.g. perhaps identifying if you are too tired to drive and automatically disabling the engine.

Of course, it might be argued that none of this compels us to allow sensors into our cars, homes and other parts of our lives, and the collection of data about us - we are not compelled to use usage based insurance or drive "intelligent" cars, and so we have a choice. But if refusing to allow the collection of data by sensors begins to become a costly decision (e.g. increased car, home or health insurance[7] premiums), it's a choice that is easier to make for those who can afford it. And, of course, once sensors and data-generating technologies become embedded in products as standard, there will come a point when there are few realistic alternatives.

This rise of technology that not only observes, but intervenes (I'll term it "bossy tech"), is a consequence of placing sensing technology in more and more places where these 'interventions' can be automated, based upon the exponential increase in data sources that can be analysed in real time with intelligent computing. And as bossy tech gets a lot smarter it will no doubt get bossier, as public authorities acquiesce in the notion that technology can regulate our behaviour far more efficiently than traditional enforcement methods – why waste money on policing public spaces if cameras and audio sensors can detect potentially unsociable behaviours, use facial and voice recognition to identify the individuals involved, and then order them to stop or else face the consequences?

The value of digital identity, i.e. the sum of all digitally available information about an individual, has been estimated to be worth €1 trillion to the European economy by 2020[8]. The internet of things is predicted to generate a value-add of $1.9 trillion globally by 2020[9]. Much of that value is not likely to be from the 'things', but from data derived about those things that promise to transform every sector, bringing efficiencies and cost savings, but also entirely new service possibilities[10]. Whatever the figures, there is undoubtedly a huge economic incentive to generate and collect data from whatever sources it becomes available. As more data from more things becomes available, we can expect to see a data "land grab" by organisations.

The control of data provides organisations with valuable insights and enables influence over purchasing decisions and other behaviours. Increasingly, therefore, data is power, economic or otherwise. But there is already undoubtedly an asymmetry in power between organisations and individuals today, as organisations have an abundance of information about consumers and analytics tools to interrogate it, while consumers suffer information scarcity and possess few tools to make any sense of their own data[11]. And this appears to be getting worse, according to Sir Tim Berners-Lee[12]. In the 2014 – 15 Web Index, an annual report measuring the Web's contribution to social, economic and political progress published by the World Wide Web Foundation, it is revealed that the web is becoming less free and more unequal.

In the absence of any countervailing forces, the current technology mega-trends look set to create further asymmetries in power resulting in less privacy for individuals in 2020.

Options and Possibilities

There are plenty of predictions about technology – from the utopian visions of a bright new hyper-efficient world where robots free humanity from drudgery, to doom-laden predictions of pervasive surveillance and the demise of personal autonomy at the hands of governments and corporations. But there are a number of counter-trends emerging that present their own narrative about how the future will play out.

Privacy is a public issue: The public's perception of the threats to privacy, personal freedom and autonomy – whether from corporations or governments - is growing. Privacy has already emerged beyond a niche, specialist concern to being a mainstream public issue. It seems that almost weekly new research is released revealing increasing public concern about privacy and declining levels of trust in organisations' handling of peoples' personal data[13].

In addition, a lesson the public has learnt thanks to the revelations from Edward Snowden is that data controlled by organisations will always be susceptible to access by governments using extensive legal powers of disclosure and surveillance. This is becoming a liability for communications and technology companies, under pressure from their users, who are beginning to take measures to put some control back into the hands of their users[14].

This growing consumer and citizen awareness and distrust looks set to accelerate and will increasingly become a factor in decision making for ordinary people – decisions about the products we use or abandon, the brands we associate with, the political leaders we elect. And as data insights become increasingly actioned by bossy tech, this will exacerbate the trend - behavioural observations, and the interventions that result, will increasingly be seen as unwarranted intrusions and restrictions on personal freedom and autonomy.

Digital activism will expand the digital commons: Consumers are taking matters into their own hands. A 2013 study from the Pew Research Internet project found that "86% of internet users have taken steps online to remove or mask their digital footprints—ranging from clearing cookies to encrypting their email, from avoiding using their name to using virtual networks that mask their internet protocol (IP) address"[15].

The plummeting cost and complexity, and increased 'consumerisation', of computing, processing and storage means that activists are now able to harness technology for themselves, without the aid of corporations and governments. The 'digital commons'[16] will continue to grow, empowering more and more citizens and consumers to take matters into their own hands, such as deploying end-to-end encryption, anonymizers[17], and by "watching the watchers"[18].

Business model disruption is inevitable: The default internet business model – advertising – is showing some signs of strain, and even the biggest players such as Google are openly exploring new models[19]. Yet the value in personal data is so great, and the levels of public mistrust in organisations' handling and use of personal data is so high, that it is inconceivable to me that entrepreneurs will not make a serious effort to exploit this disparity. What we are already witnessing is the emergence of new business models that threaten to disrupt not just the default internet business model, but more broadly the assumption that the organisation is the natural and legitimate point of control and ownership of personal data. Instead, new disruptive providers are seeking to put the individual in control of their personal data[20]. In the process, they are seeking to disintermediate data-intensive businesses from their existing sources of data.

Regulation will get tougher: Policy makers will act to toughen laws, even though they move at geological speeds compared to the rate of technology development.

New laws and regulations are being promulgated around the world, many following the European model[21]. And Europe is on a journey to update and toughen its data protection laws[22]. The EU proposals will increase fines, place tougher requirements on organisations for obtaining consent, and create a new 'data protection by design' obligation. The fines alone will focus attention, forcing organisations to devote more time and resources to compliance.

Privacy is a Public Issue
The public's perception of the threats to privacy, personal freedom and autonomy – whether from corporations or governments - is growing. Privacy has already emerged beyond a niche, specialist concern to being a mainstream public issue.

Growing Distrust
Growing consumer and citizen awareness and distrust looks set to accelerate and will increasingly become a factor in decision making for ordinary people – decisions about the products we use or abandon, the brands we associate with, the political leaders we elect.

Digital Commons
The 'digital commons' will continue to grow, empowering more and more citizens and consumers to take matters into their own hands, such as deploying end-to-end encryption, anonymizers, and by "watching the watchers".

Individual Control
New disruptive providers are seeking to put the individual in control of their personal data. In the process, they are seeking to disintermediate data-intensive businesses from their existing sources of data.

Stronger Regulation
Policy makers will act to toughen laws, even though they move at geological speeds compared to the rate of technology development.

What do you think? Join In | Add your views into the mix

Proposed Way Forward

That the technology mega-trends predicted for 2020 and beyond will continue on their march seems to me to be inevitable; we're just left debating the timeframe. But it's the counter-trends that I believe will determine whether privacy is a winner or a loser.

Business models that put the individual in control: Today, data about people is almost exclusively controlled by organisations, whether public or private sector. People have very little control over their own personal data. If data is power, then the scales are tipped heavily in favour of corporations and governments against the individual.

But the cost and complexity of processing, storing, transferring, computing and analysing data are such that it is perfectly feasible for individuals to control their own data – in fact, billions of people now do this daily in a rudimentary form, as they manage profiles on social media, and use smartphones to capture, manipulate and share data. There is no longer any reason why the organisation should be the default point of control of personal data.

What's more, where organisations function as the default data controllers, the economic potential for personal data is limited, because data remains locked up in corporate silos (even silos as big as those controlled by Google are still silos). The utility of much of this data cannot be unleashed because it cannot easily, legitimately or lawfully be connected with other data from other sources. This data only becomes really valuable when it can be combined with relevant data across all services that relate to a person's life - online, retail, financial, governmental and the myriad other sources coming available.

New entrepreneurs recognise this and are developing solutions that put the individual back in control. By making the individual "the single point of control and integration of data about their lives"[23], they are able to aggregate data about an individual from all sources and services. In doing so, they are creating an entirely new, and enormously valuable, asset class[24] that is currently diminished by being spread across the myriad data silos owned by the many hundreds of corporations and government agencies we interact with. And there is good evidence that this will enable entirely new services, and significant new economic growth and value[25].

Aside from enabling economic growth, these new models also happen to offer a market-driven solution to many of the privacy problems we are facing with the onward march of data-generating technology where the organisation is the default controller of that data. Shifting the balance of power back towards the individual must produce a positive outcome for privacy. And because it also offers the possibility of enabling innovation and economic growth, privacy is no longer trapped in one–sided conflict with forces it cannot hope to defeat. It does not require a balance, or a trade-off, between privacy and growth – it enables both.

A typical example of the sort of new service provider that is beginning to emerge is the personal data vault or bank[26]. A personal data bank provides the single point of integration for personal data under the control of the individual, and provides related services (much like a normal bank does with your money) that enables the individual to get value from their data - from eliminating repetitive form filling (providing address, delivery and payment data to online merchants), to monetising one's own data through purchase preference and 'intent-casting', to enabling new, complex 'decision support' services[27]. In this model, the individual becomes the curator of their own personal data, able to volunteer more, or more relevant, data and manage that data to ensure it is relevant, accurate and as comprehensive as they want it to be.

Once consumers have realistic alternatives, we can expect to see an end to the 'privacy paradox', i.e. individuals' actual behaviours defying their expressed attitudes, as it becomes possible, without disproportionate consequences, to act upon those attitudes by making meaningful choices.

While the emergence of personal data banks and similar business models do not in and of themselves prevent organizations

from collecting and exercising control over personal data regardless, they have the potential to disrupt this simply by being inherently more valuable. Because the value of personal data is closely connected to its relevance and currency – think of personal data as having a 'half-life' [28]- 'personally curated' sources of data will have higher value simply due to the fact that they will represent the actual wishes and desires of an individual, rather than the presumed wishes and desires based on derived data. Plus, our personal data changes all the time (think of musical tastes, favourite bars or hangouts, travel interests, and, for many people, even where they live, or the job they are doing). Maintaining personal data at the level of accuracy and currency needed for many applications to be optimally effective is an impossible task for an organization without the individual's direct involvement. Conversely, for the individual it is practically impossible to manage and keep up-to-date and accurate their own personal data when it is spread across hundreds of organisations, each with their own interfaces and approaches[29].

Technology development that supports social norms and values; It's a cliché that technology is disruptive. And too often we hear that we should accept disruption to our sense of privacy because technology has made it an outdated and redundant concept, and we can't turn back the clock. Not infrequently the people who express these views are the very people who helped to create the technology that has brought these things to pass in the first place. This is simply a form of technological determinism.

But technology should and can develop in a way that reflects and supports social norms and values. Since technology is created by people, we are perfectly capable of creating it in ways that take account of privacy and other values. Urban architects have learnt to do this with our physical environment – concerning themselves not just about function and aesthetics, but also with broader environmental impacts, the need for building communal living spaces and creating a sense of community[30].

More significantly, technology is largely the product of private enterprise. To understand why technology has developed the way it has, or how it will develop in future, we need to understand the economic motivations and drivers of those who create it, and the business models that justify investment.

Early applications for data processing technology were focused on efficiency – replacing manual processes with automated processes. Automated data processing requires data as input, but once used, remained surplus to requirements. Personal data was relatively scarce, and even though it was recognised that data needed to flow across borders, it was not seen as a valuable asset in and of itself. But it was recognised that automated data processing had the potential to cause harm to people's privacy, and so new codes and regulations[31] were created that essentially treated personal data like 'toxic waste', to be contained and made safe. Now, today, rather than being a mere by-product of digitisation, data is a resource defined by superabundance, and has become perhaps the most important driver of economic growth in the digital economy. This will become even more so as we move towards 2020. Organisations are therefore incentivised to create and capture personal data and exercise control over it.

In short, technology continuously causes friction with privacy because commercial organisations haven't really tried to address the problem. While "Privacy Enhancing Technologies" have a reasonably long history, particularly within academia, they have failed to be adopted commercially or at sufficient scale[32]. For instance, cryptographic tools have not been adopted by the general user due to a lack of commercial investment in embedding them seamlessly into products that consumers want[33]. This is because, beyond mere legal compliance, privacy hasn't featured as a strategic priority, and correspondingly there has been insufficient investment by organisations in developing the broader range of skills and expertise needed to create and deploy privacy-enhancing products or services, such as in product marketing, engineering or user

Personally Curated Data
'Personally curated' sources of data will have higher value simply due to the fact that they will represent the actual wishes and desires of an individual, rather than the presumed wishes and desires based on derived data.

Privacy Visibility
The security industry has been estimated to be worth $350 Billion in the US alone; security is a sophisticated and maturing market. The 'privacy industry' by contrast is hardly recognizable at all.

experience. There simply hasn't been a sufficient incentive to do so. And now there is precisely the opposite incentive – to generate and use data as a revenue driver in and of itself.

However, if the individual begins to become the point of control, businesses that want to leverage the vast pool of personal data assets available will need to compete with each other to provide the most attractive destination for people's data. And if businesses are competing to provide individuals with the best 'personal data banks' and other tools that enable them to gain control of their own data, and 'invest' it on their own terms, then it will become a business imperative to find innovative and attractive approaches to issues such as individual control and permission, transparency and usability, data portability and ownership, as well as data protection, anonymisation and other counter-surveillance measures. There will be an economic incentive to encourage technology development where personal data control and privacy are functional necessities, not regulatory pipe dreams.

This in turn will create a demand by organisations for new skills from technologists and service designers that enable them to create products that embed respect for privacy- related values from the outset. Universities and colleges will seek to meet this demand by providing courses and modules on the fundamentals of what privacy is and why it's important, but also qualifications in new fields like privacy engineering and privacy design.

The contrast in this respect between privacy and security couldn't be greater. On the one hand, the security industry has been estimated to be worth $350 Billion in the US alone[34]; security is a sophisticated and maturing market. The 'privacy industry' by contrast is hardly recognizable at all. The reason is simple - in an organisation-centric world, where data is valuable and where corporations control data, it is in their self-interest to secure that data. Hence, supply meets demand. But in the privacy arena, there has simply been insufficient demand to stimulate a supply.

But this is changing. Something approximating a privacy marketplace is now becoming a reality[35], consisting of tools that prevent tracking[36] and other counter-surveillance services on the one hand[37], and personal data vaults and banks that enable the curation and management of one's own data on the other[38]. Major players in the internet and communications space have also already begun to lay down their markers[39]. As this market develops, consumers will benefit from the greater control over their personal data that results.

Second generation regulation: Nevertheless, we must be wary of substituting technological utopianism with economic utopianism. These competitive forces can be harnessed, but are unlikely to create change for the good all by themselves. Regulation has an important role to play. But we need a different type of regulation to the existing data protection and privacy regulation we have today.

Existing data protection regulation emerged in the 1970s and 1980s in response to computing and data processing developments beginning in the 1960s. The underlying assumption was that data processing would always be a complex and resource intensive activity, and hence would always be the preserve of large, well-resourced organizations. Individuals needed the protection of regulation against the impacts of automated data processing and the decisions it enabled. The regulatory frameworks were generally "command and control" style frameworks that provided rules that regulated the behaviour of large, static organization (the 'data controller'), and were designed to protect the individual who lacked any means to exercise control themselves (the 'data subject').

This assumption that the organization is the natural point of control for personal data no longer holds. Yet our current data protection frameworks are built upon this assumption. Even the latest EU proposals are still essentially based on this model[40]. But with the real possibility for personal control over personal data, and business models

What do you think? Join In | Add your views into the mix

emerging to support this, policy makers need to focus on helping this nascent market develop, rather than trying to stem the tide of technology with rules and guidelines.

What's more, policy makers have struggled to find ways to effectively regulate technology in a way that produces commercially deployed technologies that reflect or support privacy norms and values, rather than disturbing them. While there are regulatory restrictions surrounding the use of personal data, this has predominantly resulted in legalistic methods of compliance. I would contend that these haven't had any significant impact on the design of technologies themselves, how they generate data, or how they make that data available.

Issuing decisions and guidelines after technology has already been commercially adopted and has started to negatively impact privacy is like closing the stable door after the horse has bolted[41]. And yet while concepts like data protection or privacy 'by design' are constructive ideas, they are unlikely to translate into better technology design on a large scale simply because they happen to appear in a regulatory instrument[42]. What is so often needed on many aspects of privacy is creativity and innovation, and you cannot command an organization to innovate.

But you can incentivize it to innovate. If a market is encouraged to develop where individuals are placed in a controlling position at the centre of a personal data market and ecosystem, there will be economic incentives to look for better solutions to issues people care about. The role of regulation should then become less about issuing detailed rules and requirements (e.g. telling companies what to include in their privacy statements, or specifically how they should capture consent, or whether they need to seek regulatory approval to use data for certain purposes), and more about ensuring that fair and open competition develops and operates to produce beneficial privacy outcomes for individuals, while also allowing innovation and growth with data. This type of regulation has been called "second generation" regulation, a term coined by Professor Dennis Hirsch in the context of evolving environmental regulation[43]. Hirsh describes the evolution from the not-so-effective early post-war environmental "command and control" regulation to the more sophisticated and effective frameworks we see today that embrace a broad understanding of how economic incentives can stimulate innovation. Hirsch sees a parallel between regulating information privacy and environmental degradation – both require innovation if they are to achieve satisfactory and effective outcomes without stifling economic growth.

However, one very important principle that has emerged within Europe's attempt to modernize its data protection regime is "data portability"[44]. This principle will require organisations to allow personal data to be exported to another entity at an individual's request. While the mechanisms for achieving this are by no means trivial (look at how long it took the mobile industry to implement mobile number portability, which is a far simpler undertaking), this is the sort of measure that will facilitate a personal data market to develop and grow. It is both a typical "second generation" form of regulation, and an essential component of an individual taking control of their personal data.

Impact and implications

Shifting Power To The Individual
This potential for economic disruption to come to the aid of privacy if not its complete rescue) by shifting power over data from the organisation to the individual is one of the most significant trends emerging.

Threats to privacy from new trends and developments in technology look set to continue in 2020 and beyond. But the impact of the counter-trends and the effect they may have in constraining or shaping technology has received less attention – perhaps with the exception of law and regulation. As someone who has spent most of their professional life helping large organisations comply with law and regulation, I am often surprised at the level of faith in the law or regulation alone in delivering acceptable outcomes to complex problems like the impact of technology on our privacy.

Law and regulation is very effective at creating momentum and movement. By creating fear in board rooms, it can galvanise organisations to focus on compliance. But this does not guarantee that the things organisations do as a result will be pleasing to all concerned, even if they appear to meet the requirements of the law, and organisations can claim to be fully compliant. This is the problem we have faced to date with technology and privacy – there is no lack of law, legal opinion and guidance; yet there is continuing dissatisfaction with how things are, i.e. the outcomes we are left with.

This is because very often policy makers do not know what those outcomes should be and it would be a mistake for the law to try to determine them. While we are capable of identifying what we don't like, it's much harder to say what we do like - or more to the point, how we would like the future to actually look.

It's therefore a case of sticks and carrots. Hit the donkey with a stick and the donkey will move. But it's unlikely to go in the direction we want it to. Dangle a carrot under its nose in the direction we do want it to go, and it will generally follow the carrot. Law and regulation is good at creating impetus and momentum, but it won't guarantee that we get to a desirable destination. To do that, we need incentives. Fortunately, the green shoots of these incentives can be found among the other counter-trends.

The possibility that individuals can now begin to take control of their own personal data is upending long established norms about the control of personal data - the assumption that the organisation is the default point of control. This is heralding the emergence of new entrepreneurs that see an opportunity to strike a new deal with consumers, offering them control. But not control simply for its own sake (worthy though that may be); rather control as a way to exercise greater autonomy over many aspects of their lives that today are made too complex and too difficult by data being controlled elsewhere. And in doing so, there is the potential to unlock enormous economic value from personal data.

This potential for economic disruption to come to the aid of privacy (if not its complete rescue) by shifting power over data from the organisation to the individual is one of the most significant trends emerging as we look to 2020. It needs to be harnessed if we want to shape the development of technology to preserve the rights enshrined in all the major human rights instruments.

The 19th August 2014 was the 25th anniversary of the Web. This year, 2015, is the 800th anniversary of one of the most important legal developments in history – the Magna Carta. The Magna Carta was all about a shift in power – from the English King to the nobles, but in defining the principles for how power is distributed and constrained, it laid down the foundations of England's legal system, and has influenced legal systems across the world. In celebration of the 25th anniversary of the web and the 800th anniversary of the Magna Carta, Sir Tim Berners-Lee has called for the creation of a 'Magna Carta for the Web' in 2015[46], and has declared that we need to "hardwire the rights to privacy, freedom of expression, affordable access and net neutrality into the rules of the game"[47].

This is a fitting aspiration. But just as the Magna Carta was a response to the shift of power from King to nobles, hardwiring the web in order to protect privacy will require a shift of power over personal data from the organisation to the individual.

[1] Brian David Johnson, Intel, Wired UK retail talk, available at: http://www.wired.co.uk/news/archive/2014-11/24/brian-david-johnson-intel (accessed 10/12/2014)

[2] ABI Research, "The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020", available at: https://www.abiresearch.com/press/the-internet-of-things-will-drive-wireless-connect (accessed 10/12/2014)

[3] ICD white paper, "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things", April 2014, available at: http://idcdocserv.com/1678 (accessed 10/12/2014)

[4] Blogger Alistair Croll declares that "Personalization" is another word for discrimination" in his post titled "Big data is our generations civil righjts issue", available at: http://solveforinteresting.com/big-data-is-our-generations-civil-rights-issue-and-we-dont-know-it/ (accessed 23/11/2014)

[5] Evgeny Morozov homepage, available at: http://www.evgenymorozov.com/ (accessed 01/12/2014)

[6] Observer Ideas - A Festival for the Mind, 12 October 2014. For an introduction: http://www.theguardian.com/reader-events/2014/jul/18/observer-ideas-2014-an-intoduction (accessed 17/12/2014)

[7] Barclay Ballad, "Now you can get financial reward for your personal fitness data", 9 December 2014, available at: http://www.itproportal.com/2014/12/09/health-insurance-firm-offering-240-year-personal-data/ (accessed 17/12/2014)

[8] Liberty Global, "The Value of Our Digital Identity", available at: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf (accessed 10/12/2014)

[9] Gartner, Inc. newsroom, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020", available at: http://www.gartner.com/newsroom/id/2636073 (accessed 09/12/2014)

[10] Harbour Research, "Where Will Value Be Created In The Internet Of Things & People?", available at: http://harborresearch.com/where-will-value-be-created-in-the-internet-of-things-people/ (09/12/2014)

[11] Mark Little, Ovum, "Personal Data and the Big Trust Opportunity", available at: http://www.ovum.com/big-trust-is-big-datas-missing-dna/ (accessed 10/11/2014)

[12] World Wide Web Foundation, "Recognise the Internet as a human right, says Sir Tim Berners-Lee as he launches annual Web Index", available at: http://webfoundation.org/2014/12/recognise-the-internet-as-a-human-right-says-sir-tim-berners-lee-as-he-launches-annual-web-index/ (accessed 17/12/2014)

[13] The Royal Statistical Society, "New research finds data trust deficit with lessons for policymakers", available at: https://www.ipsos-mori.com/researchpublications/researcharchive/3422/New-research-finds-data-trust-deficit-with-lessons-for-policymakers.aspx (accessed 10/12/2014)

[14] Apple, Inc, "A message from Tim Cook about Apple's commitment to you privacy", available at: https://www.apple.com/uk/privacy/ (accessed 10/12/2014)

[15] Pew Internet Research, "Anonymity, Privacy and Security Online", 5th September 2013, available at: http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/ (accessed 12/12/2014)

[16] In her 2012 book, "Consent of the Networked", Rebecca Mackinnon describes how activist individuals play a key role in influencing the shape of technologies and the balance of power in her chapter on the Rise of the Digital Commons. Summary available at: http://consentofthenetworked.com/about/

[17] For example, The Onion Router (TOR). See the Wikipedia entry available at: http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29

[18] An example is the TrackMap project, whose aim is to show where data travels when people visit their favourite news websites through visualization, available at: https://github.com/vecna/trackmap (accessed 15/12/2014)

[19] CITEworld, "Google for business: Now 100 percent ad-free", 16th May 2014, available at: http://www.citeworld.com/article/2156043/cloud-computing/gmail-ad-free.html (accessed 10/12/2014)

[20] Ctrl-Shift, "New market for 'empowering' personal data services will transform relationships between customers and brands", 20th March 2014, available at: https://www.ctrl-shift.co.uk/news/2014/03/20/new-market-for-empowering-personal-data-services-will-transform-relationships-between-customers-and-brands/ (accessed 10/12/2014)

[21] For example, in South Africa the Protection of Personal Information Act 4 of 2013 (http://www.saflii.org/za/journals/DEREBUS/2014/84.html), in Ghana the Data Protection Act 2012 (http://mobile.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=229717) and in India proposals in the form of a Privacy Bill (http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2233)

[22] European Commission Data Protection newsroom, available at: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[23] Alan Mitchell, Strategy Director, Ctrl-Shift, speaking on "The Business and Economic Case" at Personal Information Economy 2014, available at: https://www.youtube.com/watch?v=xbQh0DNzAlA&feature=youtu.be&t=5m2s (accessed 17/11/2014)

[24] World Economic Forum, "Personal Data: The emergence of a new asset class", available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (accessed 10/12/2014)

[25] Ctrl Shift, "Personal Information Management Services: An analysis of an emerging market", available at: https://www.ctrl-shift.co.uk/research/product/90 (accessed 12/12/2014)

[26] Some examples are You Technology (http://you.tc/), Personal.com (https://www.personal.com/) and QIY (https://www.qiy.nl/)

[27] An example of a complex decision support service would, for instance, enable a household to recalibrate its domestic energy consumption needs. For more information, see "Personal Information Management Services: An analysis of an emerging market", supra note 27.

[28] Martin Doyle, "The Half Life of Data", available at: http://www.business2community.com/infographics/half-life-data-infographic-0971429 (accessed 10/12/2014)

[29] Online contact books, like Plaxo (http://www.plaxo.com/), and social networking services like Facebook (https://www.facebook.com/) and LinkedIn (https://www.linkedin.com/home) are good examples of how there has already been a shift of control to the individual. In these cases, the process of giving out contact information (e.g. via business cards) and allowing others to manage one's contact data is replaced with the individual managing their own contact information and creating stable connections online with people they want to stay in touch with.

[30] Somewhat ironically, urban architecture is also concerned with other social issues, such as how to reduce crime in urban planning and design through 'natural surveillance'.

[31] The 1980 OCED Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (http://www.oecd.org/internet/ieconomy/

[32] As this recent academic paper illustrates, solutions are available to many of the privacy problems highlighted with pervasive technologies - "A Roadmap for IoT/Cloud/Distributed Sensor Net Privacy Mechanisms", available at: http://internet-science.eu/publication/1141 (accessed 15/12/2014)

[33] Justin Troutman, "People Want Safe Communications, Not Usable Cryptography", MIT Technology Review, available at: http://www.technologyreview.com/view/533456/people-want-safe-communications-not-usable-cryptography/ (accessed 12/12/2014)

[34] ASIS International, "Groundbreaking Study Finds US Security Industry to be Worth $350 Billion Market", available at: https://www.asisonline.org/News/Press-Room/Press-Releases/2013/Pages/Groundbreaking-Study-Finds-U.S.-Security-Industry-to-be-$350-Billion-Market.aspx (accessed 17/12/2014)

[35] Mark Little, Ovum, "Personal Data and the Big Trust Opportunity", available at: http://www.ovum.com/big-trust-is-big-datas-missing-dna/ (accessed 10/12/2014)

[36] For example, Ghostery, Inc. Website available at: https://www.ghostery.com/en-GB/

[37] For example, devices like the Blackphone are designed to ensure highly secure and encrypted mobile communications. Website available at: https://www.blackphone.ch/

[38] Supra note 27

[39] CNET, "Google to encrypt data on new version of Android by default", available at: http://www.cnet.com/uk/news/google-to-encrypt-data-by-default-on-new-version-of-android/ (accessed 17/12/2014); and see supra note 14.

[40] The current draft of the EU Data Protection Regulation is available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 17/12/2014)

[41] The controversy over the European Court of Justice decision in the so-called 'right-to-be-forgotten' case against Google is illustrative of this, where traditional data protection rules are applied to a technology, i.e. search engines, that was never designed to 'forget', to 'age' search results, or otherwise address the privacy issues with indexing against individuals' names. The European Commission's Factsheet on the case is available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (accessed 12/12/2014)

[42] Article 23 (Data Protection by Design and Default) in the Draft Data Protection Regulation, available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 17/12/2014)

[43] Dennis D. Hirsch, "Protecting the Inner Environment: what Privacy Regulation can Learn from Environmental Law", available at: http://users.law.capital.edu/dhirsch/articles/hirschprivacyarticle.pdf (accessed 01/12/2104)

[44] Article 18 (Right to Data Portability), available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (accessed 17/12/2014)

[45] For a general description of mobile number portability - http://en.wikipedia.org/wiki/Mobile_number_portability (accessed 15/12/2014)

[46] "Tim Berners-Lee calls for internet bill of rights to ensure greater privacy", The Guardian, available at: http://www.theguardian.com/technology/2014/sep/28/tim-berners-lee-internet-bill-of-rights-greater-privacy (accessed 17/12/2014)

[47] Supra note 12

Lead Expert – Stephen Deadman

Group Privacy Officer and Head of Legal – Privacy, Security & Content Standards at Vodafone Group

Lead expert on the Future of Privacy.

Stephen Deadman is a lawyer and privacy expert. Until recently, he was the Group Privacy Officer and Head of Legal – Privacy, Security & Content Standards at Vodafone Group where he worked on many of the emerging issues for the mobile and telecoms industry including geo-location services, the mobile app economy, Big Data and analytics, identity management, law enforcement and human rights.

Stephen has also played an active role in the protection of human rights in the ICT sector since 2005, working closely with civil society organisations, academics and ethical investors. Stephen was the European Chair of the Public Policy Expert Group of the Liberty Alliance from 2005-6. He played an active role in the formation of the Global Network Initiative in 2008 and in 2009 he helped found and co-lead the Mobile Privacy Initiative, a global industry collaboration managed by the GSMA, designed to create a framework to advance privacy in the evolving mobile internet eco-system. More recently Stephen helped found the Telecoms Industry Dialogue on Freedom of Expression and Privacy, which was launched February 2013.

What do you think? Join In | Add your views into the mix

About Future Agenda

Context – Why Foresight?

In an increasingly interconnected, complex and uncertain world, many organisations are looking for a better understanding of how the future may unfold. To do this successfully, many companies, institutions and governments are working to improve their use of strategic foresight in order to anticipate emerging issues and prepare for new opportunities.

Experience shows that change often occurs at the intersection of different disciplines, industries or challenges. This means that views of the future that focus on one sector alone have limited relevance in today's world. In order to have real value, foresight needs to bring together multiple informed and credible views of emerging change to form a coherent picture of the world ahead. The Future Agenda programme aims to do this by providing a global platform for collective thought and innovation discussions.

Get Involved

To discuss the future agenda programme and potential participation please contact:

Dr. Tim Jones
Programme Director
Future Agenda
84 Brook Street, London. W1K 5EH
+44 203 0088 141 +44 780 1755 054
tim.jones@futureagenda.org
@futureagenda

Future Agenda 1.0

The Future Agenda is the world's largest open foresight initiative. It was created in 2009 to bring together views on the future from many leading organizations. Building on expert perspectives that addressed everything from the future of health to the future of money, over 1500 organizations debated the big issues and emerging challenges for the next decade. Sponsored globally by Vodafone Group, this groundbreaking programme looked out ten years to the world in 2020 and connected CEOs and mayors with academics and students across 25 countries. Additional online interaction connected over 50,000 people from more than 145 countries who added their views to the mix. All output from these discussions was shared via the futureagenda.org website.

Future Agenda 2.0

The success of the first Future Agenda Programme stimulated several organizations to ask that it should be repeated. Therefore this second programme is running throughout 2015 looking at key changes in the world by 2025. Following a similar approach to the first project, Future Agenda 2.0 builds on the initial success and adds extra features, such as providing more workshops in more countries to gain an even wider input and enable regional differences to be explored. There is also a specific focus on the next generation including collaborating with educational organizations to engage future leaders. There is a more refined use of social networks to share insights and earlier link-ups with global media organizations to ensure wider engagement on the pivotal topics. In addition, rather than having a single global sponsor, this time multiple hosts are owning specific topics wither globally or in their regions of interest. Run as a not for profit project, Future Agenda 2.0 is a major collaboration involving many leading, forward-thinking organisations around the world.