

**Manuscript version: Published Version**

The version presented in WRAP is the published version (Version of Record).

**Persistent WRAP URL:**

<http://wrap.warwick.ac.uk/114602>

**How to cite:**

The repository item page linked to above, will contain details on accessing citation guidance from the publisher.

**Copyright and reuse:**

The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

Copyright © and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable the material made available in WRAP has been checked for eligibility before being made available.

Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

**Publisher's statement:**

Please refer to the repository item page, publisher's statement section, for further information.

For more information, please contact the WRAP Team at: [wrap@warwick.ac.uk](mailto:wrap@warwick.ac.uk)



# **The Digital Person**

## **the State of the Art and Science**

---

A White Paper from the 2nd Wolfson - HAT International Symposium on the Digital Person

18 Feb 2019

# Contents

<b>Executive Summary</b>	<b>1</b>
<b>Data Analytics, Data Science and Technology</b>	<b>3</b>
Personal Data and Data Analytics	3
Discrimination and Big Data Analytics	3
<b>Digital Personhood, Freedom and Democracy</b>	<b>4</b>
Identity in a Networked World	4
Self-Sovereign Identity	4
<b>Value, Economics and Markets</b>	<b>4</b>
Capability to “Speak” Data	5
Digital Innovation	5
Awareness of Problematic Personal Data Issues	6
Other Issues of Digital Identity	7
Other Issues of Personal Data in Economic and Business Domain	7
<b>Implications</b>	<b>7</b>
<b>Recommendations</b>	<b>8</b>
Paradigm shift in Personalisation	9
Digital Trust	9
Equal Opportunity	9
Digital Culture	10
Engage Both Sides of the Divide	10
Restore Clarity	10
Taxation of Data	10
<b>Conclusion</b>	<b>11</b>
<b>Speakers</b>	<b>1</b>
<b>Panellists</b>	<b>1</b>
<b>About the Symposium</b>	<b>2</b>
<b>Authors</b>	<b>2</b>
<b>For further information contact</b>	<b>2</b>
<b>To cite</b>	<b>2</b>

## Executive Summary

In the digital era, what we do is to a great extent reflected in the digital world. We are now physical persons with a digital twin; in short, a digital person with digital personas entwined with the physical aspects of our lives. The digital person has the right and freedom over how we choose to portray ourselves in the digital world, be it truth or fiction. Thus, the digital person could become very controversial. The focus of the Symposium was to elicit a conversation on the challenges and opportunities brought about by being a digital person. This paper reports the discussion of the 2nd Wolfson/HAT International Symposium on the Digital Person 31 May 2018. The symposium was chaired by Professor Irene Ng, representing the social sciences, Professor Jon Crowcroft, representing the sciences and Professor John Naughton, representing the humanities.

The symposium defined a digital person as ‘personal data<sup>1</sup>, personalised’. Companies depend on personal data generated to understand what is real about individuals, and what motivate individuals to behave in certain ways. Personal data has become the new fuel in the 21<sup>st</sup> century, feeding our digital economies even while enabling individuals to interact online. While technological advancement has seen the development of new data science tools and methods such as AI and machine learning, their increased application on personal data has an impact on identity, privacy and values. These challenges often arise from the lack of clarity and understanding of personal data and its capabilities.

Personal data has been defined and studied through different disciplines and perspectives such as technology, law, economics, sociology and humanity, but in order to address the challenges and opportunities of personal data, a trans—disciplinary approach was needed in its manifestation of a digital person<sup>2</sup>. The Symposium sought to enhance the understanding of the digital person and its impact on society. Hence, it discussed the issues, opportunities, and tensions arising from personal data from three main perspectives - humanities, science and social sciences. The Symposium consisted of three segments focused on the issues about from these three perspectives, eliciting discussions among panellists who raised further issues to be explored in future symposiums and in future research. Implications and recommendations for the digital person from social, legal, economic, business, technical, and policy perspectives were also discussed.

### From the Sciences

This segment of the symposium focusing on the sciences explored the topics of data analytics, data science and technology. Key points were:

- *Privacy issues were largely cause by centralisation of personal data*
- *Decentralised technologies now exist to emerge a better model for data sharing*
- *Centralisation of data that resulted in “big data” creates issues of privacy, fairness and transparency and usage of data will entail trade offs between them.*

---

<sup>1</sup> Personal data refers to data about a person or data generated by a person, the latter also known as Human Generated Data. Data labelled as personally identifiable data would be deemed as a subset of personal data.

<sup>2</sup> In computer science, personal data is a bitstring; in information systems, personal data is stored information; in the study of sociology or behavioural sciences, personal data is behaviour; in economics, personal data is an asset; in humanities, personal data is a record of our personhood.

## **From the Humanities**

This segment of the symposium focusing on the humanities explored the topics of digital personhood, freedom and democracy. Key points were:

- *Identity needs to be reimagined as our digital and physical worlds become more entangled*
- *Surveillance capitalism is now the dominant form of capitalism*
- *Self sovereign identity will soon be a reality*

## **From the Social Sciences**

This segment of the symposium focusing on the Social Sciences explored the topics of value, economics and markets. Key points were:

- *Personal data “signals” face market failure and society needs better data sharing models*
- *Decentralisation create new models for data sharing*
- *Identity is an “assemblage” of digital and socio-material that creates value for person or firms*
- *Privacy is a function of value*

The symposium then continued to discuss the issues and implications and provided recommendations on personalisation and digital trust; creating equal opportunities and a better digital culture; engaging both sides of the divide, promoting clarity and addressing the taxation of data.

## Data Analytics, Data Science and Technology

This segment of the Symposium focused on problematic issues regarding data (including personal data and big data) brought on by data technology such as the ubiquity of the Internet and connected things, as well as data science tools and data analytics. Solutions – technical and otherwise – were discussed.

### Personal Data and Data Analytics

Imperial College's Dr Hamed Haddadi discussed the challenges of personal data embedded in a data ecosystem. With the ubiquity of Internet and IoT devices (such as smart metres, IoT monitors) a large amount of data is generated around us. Indeed, a lot of inferred data could be derived from the data around us. When we are 'on' the social media and use wearable devices, we generate data of us. In the digital world, we leave a data trail about us, but we are not aware of its surrounding issues. Our personal data could be harvested and traded by trackers across the world. These issues could impose a great threat to the privacy and security of personal data. Moreover, the current dominant approach to personal data is centralisation. This centralisation of personal data and the associated data analytics could bring forth further challenges such as real-time control and adaptation, scalability, accountability and liability, algorithmic bias, and the privacy and security of personal data. These issues need to be addressed to exploit opportunities with personal data, and Haddadi proposed potential technical solutions. First, we should give the control of data management back to users. Second, we could shift centralised data analytics towards user-centric and contextual analytics. And third, we could apply other new technical approaches for personal data, such as ambient sensing, actuation, and Human Data Interaction.

### Discrimination and Big Data Analytics

Dr Augustine Chaintreau from Columbia University discussed issues in commerce, information and politics brought about by the data revolution and big data analytics. He proposed that the challenge lies in reconciling big data with our values. For example, customers could face price discrimination based on information such as gender or race, along with biased information like segregated advertisements. It gets worse with personalisation, which runs the gamut of moral hazards. For example, the 'sharing' economy exacerbates discrimination; in information, ad-networks exclude recipient-based races while in politics, social media channels are used by law enforcement.

Dr Chaintreau suggested three pillars to fix big data's disparate impact. The first pillar is privacy through preventing data disclosure, which would provide individuals with strong protection from future threats. It is however not an ideal solution due to its theoretical complexity, lack of incentives for implementation and possible reduction of utility. The second pillar is fair use by focusing on restricting algorithms which can enforce values. However, there are many obstacles for implementing this solution including litigation over what's fair, multiple definitions of fairness, and limitation of observational fairness. The third pillar is transparency by focusing on revealing and reconciling how data is used, as a solution for enabling accountability. Dr Chaintreau further pointed out that these solutions are complementary and entail trade-offs.

## Digital Personhood, Freedom and Democracy

In this segment of the Symposium, the focus was on our identity in a networked world brought about by technology and how with decentralised systems, users can control their identity in a network they choose or construct.

### Identity in a Networked World

Professor John Naughton from University of Cambridge emphasised that we need to reimagine identity in a networked world, as its nature<sup>3</sup> is changing. Identities are an enabler for controlling, accessing or personalising services, and social identities in particular have become most important. However, they are not created by us but by organisations like Google, Facebook and Microsoft whom we don't trust. And over the last decade we have lost control of our cyberspace social identities, to the point that we no longer know what they look like. Research by data scientists has found that based on enough Facebook likes, computers can judge our personality traits better than our friends, families or even partners. Analysing anonymous Google search results, US data scientist Seth Stephen-Davidowitz has uncovered disturbing truths about our desires, beliefs and prejudices, intimate information we wouldn't entrust with anyone. Surveillance capitalism is now the dominant form of capitalism.

### Self-Sovereign Identity

Nicky Hickmann, founder & CEO of Inglisjane.ltd, addressed the issue of identity in the networked world more positively, stressing that with decentralised systems, users can control their data and sell it to generate wealth. If wealth creation in the digital economy is based on ownership of the means of insight production, data can be created by individuals who can also be equipped with the technical and business capabilities (such as the HAT) to sell it. Thus, the means of insight production from data is not always controlled by the firms. Data becomes currency, leading to the emergence of new data currencies related to different spheres of life, e.g. if you are ill, your data has value in the health market. According to Hickmann the current power structure in the Internet economy, where our identity is defined by our service provider or government in a hierarchy, will be replaced by a self-sovereign identity in a network by the end of the 21<sup>st</sup> century. This is where as individuals we could create our social identity and, in a decentralised model, own our data. That way, our identity is governed by self-organising groups chosen by us. Our digital identity is determined by context, and we control which data are shared in each transaction. However, there are no absolutes, only different data states.

## Value, Economics and Markets

This segment of the Symposium focused on the value of personal data from the perspectives of economics and innovation.

---

<sup>3</sup> There are three components of our identity: psychological (intensely personal, evolving), social (multiple and evolving), legal (fixed). Legal identity is fixed over a life time. Psychological identity is intensely personal and evolving over a life time. Psychological identity is who you are that changes as you grow. Psychological identity: such as private traits and attributes are predictable from digital records of human behaviour (Kosinski, et al, 2013)

## Capability to “Speak” Data

To shift the focus from abstract personal data to the use of the data, we could look at the economic properties of data and understand what can be done with it. According to Professor Irene Ng of the University of Warwick, personal data contains signals and one of the key properties of personal data is perishability of a signal. For example, you are in London and have half an hour free for lunch. These are perishable signals that are valuable for businesses to co-create value and co-produce services with their customers; if companies picked up this signal, they could offer you lunch deals for that half an hour. There is big demand for perishable signals that are real time, on demand and dynamic, although there are many challenges to getting such personal data at scale. Ng argued that such perishable signals face market failure as the externalities are too great for one company to be given that much data, and yet data sharing is much needed for data to be useful to society.

In order to solve these issues, she argued that there is a need to develop our capability to “speak data” ie. share data in real time and on demand and to do so, to have the technology that understand the economics of data sharing and a platform that can increase personal data “liquidity”. She argues that this can only be achieved when individuals have the ability to share data as an asset that they have first party, legal ownership rights over. She argued for the need to have a better economic, legal, and technical model For data sharing and she presented the open sourced HAT microserver as a the solution to the challenges of data sharing facing society today. According to Ng, due to the value of data for innovation and personalisation, quality data is needed but its availability is challenging under current models. As we move into a decentralised world, new mechanisms may be available.

## Digital Innovation

Professor Youngjin Yoo of Case Western University discussed innovation driven by new technology. Digital technology brings about the unique characteristics of digital objects<sup>4</sup> and changes the nature of human experience<sup>5</sup> as well as that of value co-creation with the digital value co-creation loop<sup>6</sup>. In terms of innovation, data and algorithm are the drivers of value creation. Physical resources are combined only when and where they add value. Firms are algorithmically orchestrating distributed digital and physical

---

<sup>4</sup> Digital objects “take shape on a screen or hide in the back end of a computer program, composed of data and meta data regulated by structures or schemas” (Hui 2016, p. 1). The two essential properties of digital objects are: (i) Non-materiality whereby digital objects demand to be “printed” on physical bearers so that users can interact with them; (ii) Computed, requiring an execution of a set of instructions to come into being as they are either re-programmable or they are the result of pre-formatted, automated, contingent, “live actions” performed by software (for example, when you do cut & paste) each instance being an emergent and temporary reproduction of non-material objects created instantaneously by a set of instructions.

<sup>5</sup> Experimental computing – we are going to “feel” computing. Representational computing relates the computer to a representation of the customer. Human experiences would be ‘embodied experience of computing in mundane activities through everyday artifacts that have embedded computing capabilities in all or partial digitally mediated environments’.

<sup>6</sup> The value creation process refers to “the steps and activities (within and across firms or industries) that lead to the production of marketable goods”. Traditionally, the binding of resource takes place early and permanent through irreversible process of value creation to produce goods with irrevocable status. Information was deemed as a representational by-product of physical activities. With digital technology, the binding of resources could be deferred and temporarily at or near the point of use through reversible value co-creation process on demand, deferred and temporary. The binding of resources entails the recombinant assemblage of distributed material and non-material resources through the ‘live actions’ by software-enabled instructions. Binding (assemblage) of resources are done at or near the point or near of use through “printing”.



assets to deliver value. Thus, user experiences could be computed through a network of algorithmic activities at the point of use, Yoo explained. True understanding of value requires a comprehension of the multiplicity of self as socio-material assemblage in the multiplicity of reality as socio-material assemblage. Privacy is a function of value.

## **Panel Discussion: Issues raised**

Based on the presentations delivered by the keynote speakers in the Symposium, the panel and wider Symposium also discussed many other issues, which are summarised as follows.

### **Awareness of Problematic Personal Data Issues**

There needs to be greater awareness of the problematic issues associated with personal data. For instance, the gap between legal provisions such as the General Data Protection Regulation (GDPR) as a rights-based approach to privacy law and the data subjects' awareness about their rights needs to be addressed, along with their knowledge of technology and how it can enhance the protection of their rights.

Education is important to enhance individuals' data literacy and their understanding of privacy. Some panel experts suggested during the Symposium that Privacy should be a curriculum subject in primary schools for the next generation. This however imposes a huge burden on the individual and therefore care needs to be taken that this is not used to push back against the individual. It was suggested that all one needs is to know that their data and its use on the Internet is safe. It was also pointed out that there needs to be safety standards for industry, as a safe use framework does not yet exist.

With the Internet of Things (IoT), trust negotiation is key for the development of a trustworthy system. This negotiation, involving the exchange of credentials that allow a requesting party and servicing party to deliver a service or resource, requires identity management and access control. Any trust negotiation mechanisms developed in IoT must have appropriate access control and ensure that the mechanism is fine-grained but not burdensome, especially since there is no adequate object identity management system. Technically, trustworthiness is contextual and therefore needs to be addressed accordingly, with different variables considered for different contexts. From the user's perspective, trust comes from a sense of trustworthiness rather than actual security of the system. Therefore, we need to gain more insights in terms of where assurance or trustworthiness comes from and what are the new meanings of trustworthiness in a dynamic way.

The panel also discussed the conduct of big corporations, and how we cannot take a rose-tinted view of them. It was agreed that at best, corporations obey the law, and that some, like Facebook, have become an enforced monopoly and hence they do little about data protection. Dr. Chaintreau suggested that future big data technology may not be too different. Younger generations are being let down by the asymmetry of power but technology is not the only solution. There is some change, for example, one big corporation – Apple – is putting privacy at the centre of everything they do. Indeed, it is suggested by some members on the panel that major enterprises may want to listen and do better than they currently are do.

## Other Issues of Digital Identity

The focus has been on the identity of people. However, with the development of IoT, the focus could shift to, or include things. Indeed, things play a significant security role in IoT. However, complexity issues (such as Robustness, Redundancy, and Authentication) cause big hurdles for the digital identity of things. In the management of personal data, in addition to the identity of the data subject, the data collector and data requester also need to prove who they are. This can be achieved with artefacts like HAT. But some markets will still need a centralised regulator with whom to check the legitimacy of requests.

## Other Issues of Personal Data in Economic and Business Domain

In the digital era, services could be more personalised with the aid of personal data. For example, the HAT has the ability to deliver personalised learning and create a paradigm shift in education. According to the panel members, the main focus should be on the business models of personal data, as they will drive acceleration of harnessing economic value of the personal data, shared correctly. However, real value comes from action; actionable insights. Indeed, many players are trying to make sense of personal data and understand how to use this for the customer's benefit. The challenge is to be able to address and access what other information might be available to provide even better services. The support and the understanding of the marketplace was recognised as a big barrier to progress for leveraging the economic value of personal data.

A related issue discussed during the panel session was the taxation of the data economy. For example, the treasury in some countries are beginning to think about how data can be taxed. As the digital revolution proceeds, GDP becomes an increasingly inaccurate measure of wealth and there may be a need to include data as an asset on the balance sheet.

## Implications

The Symposium proceeded as an event platform to highlight and discuss thought-provoking issues on the digital person. Therefore, it served as a catalyst in addressing the profound issues shaping the future of the digital economies. It is clear that the fundamental right to privacy and the protection of personal data is currently pragmatically approached by all the stakeholders within the ecosystem. The symposium calls for greater transparency in data sharing that fosters innovation and technological advances but at the same time supports and empowers users by increasing trustworthiness and accountability with the aim of achieving societal well-being. The compelling issues and their implications are discussed in this section.

The pace of technological change is moving at an unprecedented speed and the world around us is becoming ever more connected as everyday activities such as obtaining information, entertainment, shopping, communications are facilitated by the use of digital devices. The proliferation of such devices and the technological advancement has resulted in significant improvements to our lives, but it has also led to a vast amount of personal data being generated, analysed and monetised.

Customer experiences have become increasingly personalised. Companies rely on personal data to build buyer personas that are tailor-made to the digital footprints of the customers. The ability to build profiles based on individual attributes and preferences for accurate marketing and product recommendations are fundamental to leverage transactions and stay ahead of the competition. Conversely, it is this very need

for personalisation that has given value to personal data and turned it into a valuable commodity that fuels data harvesting and trading. This has resulted in a multitude of issues including privacy infringement, data breaches, manipulation, misleading and corrupted data as well as false information which has tarnished the novel use of data to create transformations that improve products and services for the betterment of the individual and society.

Personal data has many implications apart from leveraging favourable transactions and commercialisation as mentioned above. To the individual, our identity, be it legal, psychological or a projection of our social persona, is curated as part of the construct of a digital person. It encompasses characteristics and traits related to our personal, psychological and emotional state that affects and empowers the choices we make. The very fact that organisations and data brokers are able to manipulate and use our digital twins as a tool of commerce creates a power imbalance that cultivates and exacerbates the feeling that we lack control. This also erodes trust and puts us in an era of surveillance capitalism. As individuals, we may choose not to reveal certain private pieces of information about our lives, yet this sensitive information can be accurately inferred by deploying the simplest algorithmic and analytical tools to examine other aspects of our lives based on cues that we do reveal. Our digital persons are becoming more like our digital twin. Often, the perpetrator goes further with the intention to manipulate, using subliminal cues embedded in the targeted message based on the predictive analysis. Such intrusion to privacy is unwelcomed and we propose that it is illegal.

The implementation of the GDPR on May 25th, 2018 provides the legislative structure for the way organisations handle personal data in terms of managing portability, erasure as well as consent management to ensure unambiguous and verifiable consent from customers for processing their personal data. This is far from a means to an end, as there will always be attempts to push the boundaries of the law. A critical risk is the development of automated decision-making based on digital evolutions such as data-mining algorithms and artificial intelligence using comprehensive digital profiles of individuals. In today's world, technologies are shaping and dictating decision-making. The question remains on how this affects the human aspect and quality of life as well as the quality and reliability of the digital profile curated by the technology.

In decentralised systems, digital trust and goodwill could be restored by ensuring transparency and control. There should be principles and techniques to mitigate risk that uphold fairness in algorithms, equal opportunities, fairness of use, privacy and data protection. The issue is not to hinder digital transformations but to liberate them beyond the basic notion of compliance. Infrastructure technologies such as HAT, SOLID and Blockchains are examples of pioneering technologies that give individual ownership rights to data in a conducive environment of transparent data exchange that is not only compliant with the GDPR, but re-balance the inequilibrium by inculcating constant innovation, technological transformations and advancement in product and services that creates value.

## Recommendations

The Symposium discussions highlight the important issue of digital transformations and concerns about personal data. It cannot be denied that digital technologies such as HAT, blockchain, IoT, and AI will pave the way for more automated decision-making processes, and personal data is at the centre of these digital evolutions. However, the correlation between algorithmic automation and personal data generated by individuals in current models invoke fear. Recent revelations on data breaches by Facebook and

Cambridge Analytica are only the tip of the iceberg. However, this should not and must not hinder innovation. Accordingly, this section explores several recommendations to provide creative solutions to the conundrum facing the digital person.

## Paradigm shift in Personalisation

It is lack of understanding of digital personhood with the focus on bundling individuals based solely on attributes and preferences (mass-personalisation or categorisation) based on personal data that has created a void. The key is to move beyond the reliance on past-data and move towards post-data to achieve personalisation through creative methods by tapping into the perishable signal of a customer that occurs in real-time and is dynamically attuned to the moment of the individual (for example, rainy day, delay in train schedule, almost lunch time). Relying on browsing history will not reveal at that moment in time these dynamic and real-time issues that are occurring to an individual. The ability to make accurate assumptions, collate and capitalise on the current moments across several platforms (e.g. location, weather, train schedules, health trends) paves the way to how organisation stay relevant in the future. This shift also requires a technical shift from centralised systems of data and centralised data analytics to decentralised systems of data and distributed data analytics. In doing so, personalisation can evolve from the creepy predictive models to becoming real time signal sharing with a tap of a button by individuals themselves giving real time, dynamic “permission to personalise”.

## Digital Trust

Organisations should strive beyond compliance to regulations to succeed with digital transformation via a more efficient and effective infrastructure for the exchange of data. While digital transformations have immense benefits such as in distance learning in education, distance patient monitoring in healthcare, smart meters, autonomous vehicles, monitoring and forecasting air quality, smart cities and a multitude of other new opportunities, it should not be thwarted or tarnished by ambiguous and short-sighted actions. The appropriate balance between digital growth and data protection is fundamental. The aim should be to build a digital trust through infrastructures employing decentralised systems that return control of personal data back to individuals. Moreover, in order to build digital trust, from the users’ perspective, a sense of trustworthiness is crucial. Therefore, with decentralised systems (such as Data Box and HAT) we could gain more insights on how we derive assurance or trustworthiness and identify new meanings of trustworthiness in a dynamic way.

## Equal Opportunity

The issue should not be to hinder digital transformations such as HAT, blockchains, IoT, or AI but to ensure that technology serves its purpose to better the human experience. Check and balance is vital as there should be constant effort to monitor the reciprocity and interactions between individuals and algorithms, so that there is a clear understanding of the basis of the algorithms’ recommendations prior to decision-making. There are numerous examples of algorithms exhibiting unintentional discrimination and prejudice such as facial recognition, language processing as well as the association of stereotypical roles to a particular race or gender. Algorithms should be trained to be rational, objective, free of bias and reflect high ethical standards towards the rights, interests, sensitivities, privacy and security of individuals while also ensuring inclusivity as well as diversity of all representative groups within society.

## Digital Culture

The evolutionary track of digital transformations has been rapid, especially with the introduction of artificial intelligence. One of the key challenges identified during the Symposium was the need to raise awareness as well as digital intelligence amongst our youth on the aspects of digital innovation, privacy, data protection, digital flows, commercial use of data and digital rights. Education should be at the forefront to achieve a society informed of the implications of technology engagement, but it is a double-edged sword that needs to be handled with care. At its core, digital culture education for youth should not be about fear but about the need to embrace technology and being proactive in shaping the value chain to produce personalised, on demand and dynamic products, services whilst demanding accountability from all stakeholders.

## Engage Both Sides of the Divide

Individuals are increasingly concerned about their privacy and control over personal data. This in turn has contributed to modifying their online behaviour by taking measures to limit the data they provide, increasing security such as strengthening passwords and paying more attention to sharing personal information and perhaps disengaging from social networks and adopting incognito or private browsing as well as implementing ad blockers. Although such initiatives might seem to provide security to the individual, they actually hinder innovation and limit personalised customer relationships. Hence, it is vital that organisations and legislatures work together to face these challenges. Regulations and jurisdiction are important to data management. There is no question that the right to privacy is fundamental and the protection of personal data should be an absolute priority regardless of borders. Organisations should be willing to explicitly integrate customer data-handling policies with self-regulatory codes or ethical charters and standard opt-in procedures that give individuals the right to access, control and withdraw contents of their data. However, it is essential that organisations move beyond compliance by establishing ethical frameworks with the representation of all stakeholders to oversee, address and more importantly, communicate issues arising from their handling and use of personal data.

## Restore Clarity

Much of the confusion arising from the issues surrounding personal data stems from a lack of clarity in the very definition of the term ‘personal data’ as well as little understanding about the underlying technology, the law of economics and how digital society works in our modern lives. It is often the discrepancy between the new technology and the perceived risks or disruption they could potentially cause that leads to the lack of trust in firms, government or people. We tend to project our biases and prejudice accordingly, creating an obstacle to digital transformations. What further fuels confusion is the dearth of discourse about privacy and security, personal data protection, commercial use and exploitation of data, user rights and the digital flow and its implications to policies, economies and society. But clarity can be restored through proactive actions such as this Symposium, which brings together academics, researchers, industry players and businesses, policy makers as well as the media to engage in dialogue to educate and reassure the public.

## Taxation of Data

The digital labour of users in providing their personal data has long been a form of strategic revenue for digital businesses. This makes data an asset and as such, it could be taxable. It is time for the creation of appropriate legislation that governs the taxation of businesses that collect and use personal data. Digital

companies should pay taxes not only in their home country where they operate but also in countries where their users are located. The task may seem daunting due to the complexity of data as well as the need to isolate and determine a monetary value to the data obtained and processed by digital businesses, but governments, academics and businesses can collaborate to establish a model for data usage valuation.

## Conclusion

Despite the challenges faced by new digital technologies, the tides are turning and we believe the issues discussed during the Symposium will have significant implications for personal data in the digital ecosystem.

Centralised systems as well as centralised analytics for personal data and big data are still the dominant digital technologies. In such systems, our personal data is harvested, used and traded for the benefit of corporations who construct, control and influence our digital persons. Privacy regulations such as GDPR cannot regulate enforced monopolies who do little about data protection. Indeed, the centralisation of personal data and associated data analytics has posed challenges for the real-time control and adaptation, scalability, accountability and liability, algorithmic bias, and privacy and security of personal data.

A potential technical solution to such challenges is to decentralise personal data systems and distribute data analytics. This could give the data and insights back to individuals and has significant economic implications. These artefacts could improve the quality of data with perishable signals that are real-time, on-demand, dynamic, and at scale, crucial for creating value for both people and firms. Such data is key to enhancing digital innovation.

## Speakers

Dr Hamed Haddadi, Imperial College, University of London

Dr Augustine Chaintreau, Columbia University

Professor John Naughton, University of Cambridge

Nicky Hickmann, founder & CEO Inglisjane.ltd,

Professor Irene Ng, University of Warwick

Professor Youngjin Yoo, Case Western University

## Panellists

Professor Irene Ng, University of Warwick

Professor Youngjin Yoo, Case Western Reserve University

Mr. Alan Greenberg, Wide Academy

Dr. Tolga Uzuner, former Apollo Global Management

Mr. Ian Hayward, Appcoast

Ms. Nicola Klein, Direct Line

Professor John Naughton, FRSA, University of Cambridge

Ms. Nicky Hickman, Consult Hyperion

Professor Jon Crowcroft, FRS, University of Cambridge

Dr. Hamed Haddadi, Imperial College London

Dr. Augustine Chaintreau, Columbia University

## About the Symposium

The 2nd Wolfson-HAT International Symposium on the Digital Person 31 May 2018 organised by the HAT Community Foundation and supported by Wolfson College Cambridge and the University of Warwick.

**HAT Community Foundation** (HCF) pioneers thinking about the digital person and personal data and manages the “Hub-of-All-Things” (HAT) Ecosystem for personal data sharing and regulates the HATDeX platform. HCF’s mission is to enable first party data rights and ownership of data for better sharing of data, thus empowering everyone, everywhere to get the full value of their personal data and to have a voice on the Internet. HCF regulates the introduction of commercial and non-commercial participation in the network for the benefit of HAT owners and partners globally.

[www.hubofallthings.com](http://www.hubofallthings.com)

[www.hatcommunity.org](http://www.hatcommunity.org)

## Authors

Susan Wakenshaw and Lalitha Dhamotharan at the University of Warwick

## For further information contact

Jonathan Holtby at HAT Community Foundation, [jonathan.holtby@hatcommunity.org](mailto:jonathan.holtby@hatcommunity.org)

## To cite

Wakenshaw, Susan and Lalitha Dhamotharan (2019), “The Digital Person- the State of the Art and Science,” the 2nd Wolfson-HAT International Symposium on the Digital Person, a HATLAB white paper published on 18 Feb 2019