Abstract

International experts, including, policy makers, clinicians, scientists, researchers and representatives of private sector, professional and other associations, convened in New York on 4-5 October 2018 to discuss the opportunities of Internet of Things for smarter models of wellness and care. The consultation was organised jointly by the Organisation for Economic Cooperation and Development (OECD) and the Global Coalition on Aging (GCOA) and co-hosted by Cornell-Tech.

The OECD refers to the Internet of Things (IoT)\(^1\) as “an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world”. A growing important part of this ecosystem is remote care, which can be deployed in smart home settings to monitor health, enhance wellness and support independent living of elderly and disabled populations. Remote care is becoming a 21\(^{st}\)-century standard of care, as it is increasingly recognized for its value in improving quality of life and enabling cost-effective delivery of new models of care.

The Expert Consultation reviewed the emerging health and wellness IoT ecosystems providing examples of applications for greater access to treatment, treatment adherence, remote care monitoring and related use of Artificial Intelligence (AI); and for personalised care solutions including for prevention and promotion of healthy behaviours. Experts discussed what actions are needed to create the conditions for effective adoption of IoT-based innovative care solutions.

The following questions informed discussions:

---

What is the potential of IoT to support the promotion of healthy behaviours and a healthier and more active ageing population?

What user welfare and better health outcomes may be derived from the goods and services enabled by the IoT?

What are the main IoT-related data privacy, security and safety concerns?

What actions are needed to unlock the value of IoT for wellness and healthcare?

What is the effect of the IoT—and the innovation it spurs—on our economy as a whole?

From the two-day conversation, the expert group outlined four key insights:

1- Along with the opportunities, IoT raises new challenges. First, the largest source of value from health applications would seem to arise from improving the quality of life and extending healthy life spans of older people and patients with chronic illnesses. Evaluation has however not kept pace with technological developments and robust evidence on whether (and under what conditions) IoT can support the delivery of appropriate care that is of higher quality and cost-effective is still lacking. That said, specific examples of remote monitoring in heart failure, diabetes and even in the conditions of aging such as vision health, were identified as promising use cases. Studies on healthcare solutions based on mobile technology have had so far a strong focus on the technological components, but non-technical aspects such as value proposition, organisational, and reimbursement models have not received the attention required. Experts agreed that while the technology itself continues to improve, it is also the responsiveness of payment systems that is essential for maximum value of remote care tools to be realized. With an answer to these questions, it will, in turn, be possible, to inform policy and start addressing the trade-offs involved for the users/consumers in adopting IoT and what actions and economic incentives are needed to steer developments towards desirable outcomes.

2- Second, a greater reliance on IoT potentially increases digital security risks; and ubiquitous personal data collection raises new data governance challenges and creates additional privacy risks (OECD, 2015). The “greater value and service” brought by the IoT is only possible through the enhanced access and sharing of personal data. On the other hand, it was recognized that some consumers are ready to give up a degree of privacy against promises of greater safety, convenience and functional independence. Many of the examples of health and wellness IoT devices are accompanied by an interactive smartphone application (app), through which the user can configure and control the device, store and interrogate the data it collects. Data collection using apps may also introduce various data quality and associated privacy, security and safety challenges. Many of the health and wellness apps on the market are not considered medical devices and are therefore not subject to specific evaluation. Poor data quality could result in suboptimal outcomes, including missed opportunities for effective intervention or even wrong information to improperly guide health decisions. As with the use of other information and communication technologies (ICTs) in healthcare,
there is a role for governments in combination with industry in making sure that security and privacy are considered from the outset, as part of a device’s design.

3- Skills development is another area in which government policy and investment may be required to make full use of the benefits of IoT. Skills are required for the development of products but also for their deployment and effective use. IoT deployments involve potentially 10s to 10s of thousands of devices making the design and physical installation complicated. Even at the level of setting up a “smart home”, the installation of sensors in order to monitor activities of daily living is a specialist process. Operationally, elder carers and health professionals need to be able to understand and make use of the data provided and integrate this in to the workflow of their usual care. This will require further education and skills and support and commitment from healthcare organisations and governments. In other words, developing IoT-based care services will require a combination of resources and competences from different fields.

4- Finally, it has been shown that much of the economic benefits from IoT will not be realised if systems are not interoperable and data is not used beyond the purposes of the system that generated it. One of the major challenges to implementing the IoT has to do with the ability of the various devices to “communicate” seamlessly with each other. Manufacturers each have their own proprietary protocols, which means sensors by different makers cannot necessarily speak with each other. In addition, as networks evolve to keep up with the IoT and coming 5G New Radio standard, the sheer level of complexity will require automation. Interoperability goes beyond simply being able to share data and agree on what it represents. There are calls for greater transparency of algorithms that are developed to interpret the data. This will require standards and again, policy to incentivise researchers and industry to collaborate and openly publish this information.

Session 1: Internet of Things Wellness/Health Care Ecosystem: State of Play

Moderator: Jenni Nordberg (Director and Head of health division at Vinnova; Sweden)

“With technology and medicine, we have choices and people are making choices. It is not just the longevity itself, but the structure of society which has the huge impact on our institutions and public policy” Michael W. Hodin, GCOA

Falling fertility and increases in longevity have resulted in a shift in the demographics of OECD countries with more people over 60 than under 14. The fiscal pressure from ageing populations is large. In the absence of policy action, pension, health and long-term care (LTC) spending is forecasted to grow faster than national income in most of the OECD economies. Innovation in health and social services, whether supplied by the public, private or third sector, will be important to meeting the challenges of an ageing society. The rapidly growing silver market is evaluated at US $15 trillion by 2020 and companies like Philips are changing their business models to focus on health care with specific reference to this market.
Nick Padula of Philips detailed the challenge of increasing the quality of life along with increasing longevity. He viewed this as a challenge that technology can address with new models of healthcare and changing personal behaviours. IoT will generate data that through advanced analytics promises to lead to earlier detection and diagnosis, itself leading to improved treatment and care, ultimately resulting in better outcomes, shifting care out of the hospital and into the home and community. The main challenge of implementing this model of care is lack of awareness, skills and the concomitant lag in new payment and reimbursement models.

“Adding longevity without quality (of life) is simply cruel”
Nick Padula, Philips
Evan Patton of MIT’s Internet Policy Research Initiative talked about the role of AI in handling the data deluge from IoT in healthcare. There is both breadth and depth in the data that must be aggregated and processed to provide a holistic overview of one’s health. MIT is developing techniques and frameworks to allow developers to create apps leveraging AI and Big Data. Edge computing, especially on the mobile phone, provides one way of handling large amounts of data and increasing security and privacy. Development of distributed AI techniques to bring together different medical technologies, to track the provenance of the data they collect, and to build models of health to benefit each individual is critical to supporting an aging population at scale. In the near future it will also be possible to aggregate at the population level to look for trends and to train models for the benefit of all. However, while new technologies such as 5G cellular will make bandwidth more plentiful and access to cloud-based solutions more plentiful than ever before, there are still a number of privacy issues that will need to be addressed with the management of large amounts of patient data. Increasingly centralized services will become valuable targets for attackers, so security implications must also be considered. A distributed, mobile-focused approach is a key component to overcoming these challenges. Data aggregation should also be designed to be opt-in whereas most IoT solutions today are configured to share data with third parties by default.

Jose Valverde DG CONNECT of the European Commission described initiatives to utilise IoT and wearables for remote care in Europe. One such initiative is the third Data Package (2018) that provides more effective use of public and private sector data and the establishment of databases, AI and digital health care. The Data Package includes a Communication “Towards a common European data space” which addresses the issue of access to private sector data for public interest purposes. Mr Valverde also presented the ACTIVAGE project which aims to be the first European IoT ecosystem across 9 deployment sites and 7 European countries. A
multi-stakeholder project that aims to build a set of techniques, tools and methodologies for IoT platform interoperability. Mr Valverde reported on a number of key challenges to the adoption of digitally enabled solutions for health and care as:

- Identifying and getting reliable information on solutions available on the market
- Solutions have limited scope and difficult to integrate into existing systems
- Lack of interoperability
- Lack of openness

He further noted that for the period 2014-2021 under Horizon 2020, the European research and innovation programme, the EU is investing almost EUR 500 million in Internet of Things-related research, innovation and deployment. In particular, the European Commission is currently co-funding five large-scale pilots for the deployment of trusted and personalised digital solutions in the following areas: Smart living environments for ageing well; Smart Farming and Food Security; Wearables for smart ecosystems; Reference zones in EU cities; Autonomous vehicles in a connected environment. The European Commission has also launched a specific cluster of R&D projects to investigate new solutions for security and privacy by design and by default in the Internet of Things.

David Ryan General Manager Health and Life Sciences Sector at Intel talked about Intel’s initiatives for remote care of ageing customers. Remote monitoring is resulting in cost savings and reductions of re-admission to hospitals. He detailed different use cases including:

- Post-acute care: congestive heart failure and frail and chronic disease
- Medication adherence
- Pharmaceutical trials
- Workplace direct primary care
- Chronic condition management of diabetes and hypertension
- Assisted living

Better care monitoring and delivery, as well as cost savings, as demonstrated by these use cases have led to value-added progress. In the US, the Medicare physician fee schedule now includes 3 new remote patient monitoring codes and reimbursement for “virtual check-ins” and for inter-professional consults via telehealth, with more codes to be deployed in 2019. Remote patient monitoring is now considered to be a basic benefit in the Medicare Advantage program. Medicare Home Health Prospective Payment System allows home health providers to include remote patient monitoring tools as an allowable Medicare cost.

**Key points**

1. There is a need to achieve interoperability between systems and to make data accessible from systems through open APIs.
2. There is also a need to define what is meant by evidence in the context of IoT ecosystems applied to health care and wellness.
3. Whilst industry participants emphasised the many small and some larger, pilots, randomised controlled trials (RCTs) were seen as being the gold standard for gauging
effectiveness and were less frequently cited in support of the benefits of IoT wellness and health care ecosystems.

Session 2: Enablers of progress: Security, Privacy and Trust in the IoT

Moderator: Jennifer Stoddart, Former Privacy Commissioner of Canada (Canada)

Gilad Rosner of the Internet of Things Privacy Forum talked about privacy risks and accountability in the IoT Ecosystem. Rosner outlined the privacy risks of IoT:

- IoT will expand data collection practices of the online world to the offline world
- IoT portends a diminishment of private spaces
- IoT will encroach upon emotional and bodily privacy
- The notion of privacy invasion will decompose especially as people’s expectation of being monitored increases
- IoT will fade into the background, so people will be less aware of it and potentially reveal more intimate, personal data to devices
- As the market for ‘smart’ devices matures, people may have less choice – less ability to buy products that do not monitor them. It will become harder to opt-out of data collection Meaningful consent very difficult
- IoT’s impact on children gives parents additional privacy management responsibilities

In response to these risks, there are emerging frameworks and strategies:

Pre-collection

- Data collection minimisation
- Do Not Collect Switches
- Wake words
- Privacy Impact Assessments

Post-collection

- Allow data deletion, withdrawal of consent
- Data encryption at rest and in transport
- The default for sharing IoT device data on social media should be OFF. People must opt-in to it Raw data should exist for minimum amount of time

Identity Management

- Breaking links of users between devices and online
- Make sure systems are “blind” to user activity
- Use selective sharing
- Create dashboards for users to see, understand and control data
- Separate different people’s use of device from one another
Just-in-time, periodic, context-dependent and layered notices.

Automation of privacy notification and consent (www.privacyassistant.org)

Governance Strategies

- Greater use of the precautionary principle in IoT policy
- Creation of omnibus privacy laws for US
- Use-regulations: Regulations restricting IoT data from certain uses
- Expansion of PII to include sensor data in US
- Reasonable expectation of privacy standard needs bolstering
- Regulation of privacy notices for comprehension
- Trusted IoT labels and certification

Robin Wilton of the Internet Society discussed consumer trust and health care IoT.

“Trust is a belief that someone will act in your interests, even if they have the opportunity and the motivation to do otherwise”
Robin Wilton, Internet Society

Mr Wilton discussed the problems of the business models centred on the monetization of personal data. There is a need to provide users with the right amount of information and the right amount of control. In order to achieve this, there is a need for transparency, presenting the user with relevant information in order to increase their agency. What is common however are “design anti-patterns”. Changing a privacy setting, for preventing access by a 3rd party website for example, can only be achieved through a complicated and large number of settings.

There are a number of forces keeping users from having the right balance of information and control. These include:

1. an information imbalance between consumer and the companies
2. a market failure that does not give consumers power to force providers to behave in a certain manner
3. perverse incentives through which providers “gamify consumers” into giving away information (especially health information)

There are existing ethical approaches to help build trust. For example, the 2012 Menlo report provided a basis for ethical framework for research involving ICT. The principles in the Belmont report can be usefully applied in fields related to research about or involving information and communication technology. Mr Wilton for example suggested that privacy specialists should be added to institutional review boards to bring a multi-disciplinary approach to research and product development.
Companies ultimately have to behave ethically, but information asymmetry will be an ongoing problem. A solution may be to have a trusted third party act on a person’s behalf. Another approach would be to ensure that all permissions are opt-in rather than opt-out.

**Session Discussion**

The presentations were followed by considerations on the need to “push” companies to protect privacy and that innovation need not be sacrificed in order to protect privacy. Ms Amie Stepanovich commented on the weaknesses of a harms-based approach to privacy and noted that it is a mistake to view young people as not caring about privacy. Robin Wilton added that from an ethical perspective, if the young were indeed misinformed, then society was failing them in its duty to making sure they were.

*Bodil Josefsson, Head of IoT security Ericsson* talked about the role of security, data protection and privacy in fostering trust in the IoT ecosystem. She noted that the main challenge for IoT is that it requires end-to-end digital security and privacy and at the same time strong authentication and identity management. However, as the diversity of IoT services and the number of connected devices continue to increase, the threats to IoT systems are also changing and growing rapidly.

There is a legitimate expectation in society that IoT solutions will be designed with privacy in mind. Patients expect to be able to control their health and behavioural data and to decide with whom this data is shared with. Data integrity, data confidentiality, accountability and privacy by design are all fundamental to the protection of sensitive personal data. Additional privacy protective measures include data encryption and data anonymization.

In a distributed IoT ecosystem, however, privacy and security issues may be common and yet hard to identify. Data aggregation from multiple sources is also an issue. Although one-time passwords and two-step authentication is the most common approach to securing databases, these are not bulletproof solutions. To cope with potentially new and greater digital security and privacy risks, technologies like “zero-knowledge databases” are increasingly promising. Zero knowledge means that the owner of the database does not know what data is stored in a specific part of the database if it does not have a username and password for that part. Novel and more robust authentication methods are today based on a combination of permission-based data access with zero knowledge encryption and blockchain technology. At the same time, decentralization of the data on user devices, increases user control over his/her data.

*Bodil Josefsson, Head of IoT security Ericsson* talked about the role of security, data protection and privacy in fostering trust in the IoT ecosystem. She noted that the main challenge for IoT is that it requires end-to-end digital security and privacy and at the same time strong authentication and identity management. However, as the diversity of IoT services and the number of connected devices continue to increase, the threats to IoT systems are also changing and growing rapidly.

There is a legitimate expectation in society that IoT solutions will be designed with privacy in mind. Patients expect to be able to control their health and behavioural data and to decide with whom this data is shared with. Data integrity, data confidentiality, accountability and privacy by design are all fundamental to the protection of sensitive personal data. Additional privacy protective measures include data encryption and data anonymization.

In a distributed IoT ecosystem, however, privacy and security issues may be common and yet hard to identify. Data aggregation from multiple sources is also an issue. Although one-time passwords and two-step authentication is the most common approach to securing databases, these are not bulletproof solutions. To cope with potentially new and greater digital security and privacy risks, technologies like “zero-knowledge databases” are increasingly promising. Zero knowledge means that the owner of the database does not know what data is stored in a specific part of the database if it does not have a username and password for that part. Novel and more robust authentication methods are today based on a combination of permission-based data access with zero knowledge encryption and blockchain technology. At the same time, decentralization of the data on user devices, increases user control over his/her data.

*Brigitte Acoca, Senior Policy Analyst, OECD* described work conducted by the OECD on product safety in the IoT and consumer policy and the smart home. Product safety risks can result from:

- A product defect
- A software update
- A software defect

---

2 *Consumer Product Safety in the Internet of Things* (2018), at: [https://doi.org/10.1787/7c45fa66-en](https://doi.org/10.1787/7c45fa66-en); *Consumer Policy and the Smart Home* (2018), at: [https://doi.org/10.1787/e124c34a-en](https://doi.org/10.1787/e124c34a-en)
- An unsafe decision taken by the IoT on the basis of an algorithm
- Digital security threats and vulnerabilities

She emphasized that digital security is a significant issue for product safety policy as the IoT continues to develop. The maintenance of data integrity can be critical to ensuring the safe and proper functioning of products throughout their lifetime.

Ms Acoca also noted that a key challenge for regulators is the blurring of the distinction between “hardware” and “software”, or “goods” and “services”. The IoT does not obviously raise entirely new issues in this regard. However, it brings a greater level of complexity in the interaction between hardware and the software that drives it, with the behaviour of products in many sectors being increasingly dependent on changeable software and data that resides in both the product, and external to it. Moreover, because an IoT device or application can be a mix of goods and services, traditional notions of product safety and liability do not map cleanly onto the new world of IoT-connected devices and applications. The extent to which product safety and liability laws apply is an issue under consideration in a number of jurisdictions.

On the one hand, there is concern in the potential for such technologies to give rise to new safety risks, and questions about whether existing liability and product safety regulatory regimes are adequate. On the other hand, there is increasing interest in the opportunities afforded by such technologies to enhance the quality of products, to help prevent consumer product safety hazards or damage, and to create better ways to manage safety in the supply chain and in the marketplace. A key question is how to adapt current liability and product safety frameworks to better protect consumers while at the same not hindering innovation, especially in the area of health care.

Agencies responsible for product safety policy around the world are increasingly trying to understand the implications of the IoT for product safety regulation. In a growing number of jurisdictions, such agencies are engaging in a dialogue and partnerships with their counterparts addressing, among others, health, privacy and security issues, to establish a whole-of-government approach strategy around the IoT.

**Key points**

1. Transparency paradox: IoT technologies may allow for highly detailed profiles to be developed about individual consumers without their consent and may prey on their vulnerabilities.
2. Individuals have a tendency to go along with whatever the default (or status quo) consent choice or setting is, even when this may not be in their best interest, and even when they have the ability to make a different choice or opt-out of the default
3. How to deal with information asymmetry is a significant problem – users should be able to understand what information will be collected from them, how this information will be used, how the information will be shared with other actors, and how such information will be stored.
4. To sustain trust, new business models are needed to reduce exposure to advertising or make a business less reliant on this revenue source based on the collection of personal data.
5. Digital security of the IoT ecosystem needs to be end-to-end but it is not clear who would be held responsible for this.
6. Digital security is a significant issue for product safety, security professionals and consumer regulators will need to collaborate.
7. From a policy perspective, there is potential in the use of regulatory sandboxes and greater use of the precautionary principle.

Session 3: Health and Wellness Apps: Quality assurance Challenges and Solutions

Laura VanDruff, Assistant Director, Federal Trade Commission, Senior Attorney, Division of Privacy and Identity Protection; (US)

Josip Car of Lee Kong Chian School of Medicine and Nanyang Technological University Singapore discussed the need for frameworks to control the quality of apps used for chronic disease management reporting from a recent study of apps that aim to help diabetics self-manage their condition.

Over 400 million adults currently have diabetes, and this number is expected to increase by 50% in the next 25 years. The estimated global health care expenditure attributed to diabetes amounted to more than USD700 billion in 2017 and is set to increase in the next 25 years. Current models of care for diabetes are, however, not meeting the rising needs and studies have demonstrated the utility of smartphone apps in complementing diabetes care. This is particularly critical for low- and middle income countries where weakness of health care services and shortage of health care professionals are particularly serious.

Mobile apps could potentially provide unmet population health needs by increasing:

- Access to care
- Information and education
- Collection and analysis of data
- Decision support

1200 iOS and 950 Android apps were assessed against criteria developed with reference to the 2017 American Diabetes Association clinical guidelines of diabetes self-management. Josip Car noted that only a small number of apps covered all recommended areas of diabetes management.
Proportion of Diabetes Management apps with support for self-care domains.

In particular, only 18% of these apps provided information about diabetes with only 40% of that coming from accredited sources. No apps provided information from accredited sources on all aspects of diabetes.

In another study\(^3\), apps that calculated correct doses of insulin had errors, inappropriate warnings of dangerous levels, input and output issues. Of 46 apps examined, only 1 was issue free.

In conclusion, he noted that there is a real need for minimum quality standards and accreditation to ensure clinical quality and safety and greater awareness by health professionals.

Jonathan Obar Assistant Professor, Department of Communication Studies York University, Toronto discussed the misconceptions or “fallacy” of data privacy self-management drawing on his article "Big Data and the Phantom Public,"\(^4\) repurposing an argument from Walter Lippmann’s The Phantom Public, to emphasize the individuals’ inability to be self-governing in the Big Data ecosystem. In particular, Dr. Obar suggested that it is unrealistic to expect from individuals:

[1] Engagement and understanding of all terms of service and privacy notices
[2] Engagement, understanding and control of the Big Data deluge

“Yet he cannot know all about everything all the time, and while he is watching one thing a thousand others undergo great changes.”

---


https://journals.sagepub.com/doi/pdf/10.1177/2053951715608876
Dr. Obar cited Nissenbaum’s transparency paradox\(^5\). The paradox illuminates the considerable challenges that persist with presenting users consent materials that can ensure engagement and informed consent. One side of the paradox suggests too much information provided in consent materials will be overwhelming to users. Research suggests that consent materials are often too long, too numerous and too difficult to understand.\(^6\) On the other side of the paradox is the suggestion that if not enough information is presented, the dearth of information will fail to inform or educate users during consent processes. Indeed, research concurrently suggests that not enough detail is provided about data practices to fully inform users about Big Data management and implications.\(^7\) A perpetual inability to answer the questions posed by the paradox suggests the privacy notice model, as currently advanced by industry in particular, does little to support understanding of how personal data is used. As a result it can be argued that privacy notices are not an effective instrument for the average user to determine exactly how their information is used, or kept private.

Dr. Obar’s own co-authored research\(^8\) on “the biggest lie on the internet” (i.e. “I agree to the terms and conditions”) looked at individuals’ privacy policy and terms of service policy reading behaviour during the signup process for a fictitious social media service called NameDrop. The participants were university students who study Big Data and privacy issues. Of more than 500 participants, 74% agreed to the privacy policy without accessing or reading it. These participants chose NameDrop’s clickwrap – “a digital prompt that enables the user to provide or withhold their consent to a policy or set of policies by clicking a button, checking a box, or completing some other digitally mediated action suggesting “I agree” or “I don’t agree”\(^9\) Further research suggests that users like clickwraps as they help circumvent consent processes so that users can “enjoy the ends of digital media production (as quickly as possible), without being inhibited by the means”\(^10\) It should be added that clickwraps also serve a political economic function as they “direct users away from policies that might encourage dissent and ensure users stay in fast lanes to monetized sections of services,”\(^11\) suggesting that social media service providers may have an incentive to maintain the clickwrap functionality.


Returning to the “biggest lie on the internet” study, of the 26% of more than 500 participants who read the privacy policy, 81 percent took less than one minute to read it. For the terms of service, 86% spent less than a minute, and 12% read for fewer than five minutes. Based on average adult reading speeds, the policies together should have taken approximately 45 minutes to read. The study suggests users view “notice as nuisance” and tend to ignore consent opportunities in order to engage with digital services as quickly as possible – hence the appeal of the clickwrap. Within the terms of service there was a clause agreeing to assign the user’s first-born child to the site’s company. 98% of people who read the terms of service did not notice the clause. The study has been repeated with an older sample population and the preliminary results appear to be similar. When asked about engaging with policies for Facebook, Instagram, Twitter, Snapchat, iPhone Messenger, Gmail, Skype, Xbox Live, Yik Yak, and iTunes, 35–39% of the participants in the study said they ignore policies. For the participants that read policies, average reading time that was self-reported was approximately five minutes. The median reading time was about two minutes. Dr. Obar concluded that the results of the studies, in combination with ongoing results from the academic literature, suggest current approaches to delivering meaningful consent in digital spaces are highly problematic, and must be addressed if users are to realize protections.

Obar finally detailed that the public were not in a position to make informed decisions on data privacy involving big data. He concluded making the following recommendations:

1. Acknowledge the persistence of the unobtainable ideal in policy
2. Acknowledge disproportionate risk of Big Data discrimination
3. No clickwraps
4. No data use surprises in terms of eligibility decision-making
5. Distributive data justice
6. Infomediation from software or 3rd parties to achieve privacy deliverables

During the discussion period, workshop participants noted that the study had significant policy implications particularly at a time of considerable debate about the future of consent processes online, following the Cambridge Analytica data leak of, allegedly, 87 million user accounts.

**Effy Vayena (ETH Zurich, Switzerland) and Elettra Ronchi (OECD)** presented preliminary results of a review of good practice guidance for health app development in nine OECD countries. The study focussed mainly on national guidelines for health and wellness apps that are not considered medical devices. The work had been carried out in response to a 2017 OECD report that had concluded that the use of low-quality non-medical health apps raises a wide range of ethical, legal and governance issues, and pointed to the need for international agreement on minimum quality assurance standards.

In most countries, medical device regulation applies only to the subset of high-risk health apps that have well-defined medical purposes. However, the majority of health apps available on the market nowadays are non-medical. The main risks of these apps are:

- Loss of privacy
• Inadequate security
• Lack of accuracy and reliability

Generally, data protection authorities’ documents in this space were aimed at app developers and referenced available legislation that would be useful to app developers.

The overall conclusions from the review were that the principles were insufficiently operationalised, there was a lack of focus on health and wellness. Only two health authorities, the UK National Health Services (NHS) and the French Haute Autorité de Santé, had issued specific guidance. Although governments are developing regulation and guidance for app developers, the study indicated that this guidance is not necessarily comprehensive and is significantly fragmented.

Possible suggested actions included:

• The provision of good practices specifically for health apps
• Include other stakeholders such as app users and third parties
• Require certification or accreditation
• Promote the development of an international framework to address quality assurance, clinical safety, data protection, security and usability.

Key points

1. Privacy policy agreements are rarely read or understood. The requirement of detailed privacy notices has resulted in less understanding of how personal data is used.
2. Information asymmetry is a challenge in contract-based privacy agreements
3. There is an urgent need to identify and address challenges to effective data protection and privacy enforcement
4. Alternative business models to those based on monetizing users’ personal data are needed.
5. There is a window of opportunity to enable cross-country agreement on minimum quality assurance standards covering quality assurance, clinical safety, data protection, security and usability.

Session 4: Understanding the value and potential benefits of an IoT-based care

Moderators: Deborah Estrin, Associate Dean and Professor of Computer Science at Cornell Tech, (US); Louise Rosborough (Manager of the National Initiatives Unit, Health Care Programs and Policy Directorate, Strategic Policy Branch, Health Canada (Canada))

Dr David W. Bates Chief of General Internal Medicine at the Brigham and Women’s Hospital (USA) discussed success factors of innovation within a clinical environment. A wide range of different innovation centres have been created worldwide both within and outside of
Innovation, which is targeted at commercial success, generally falls into one of three categories: drugs, devices, and information technology. Innovation can also be directed at improving care delivery. Innovation can take different paths, and Dr Bates discussed approaches taken by a few successful clinical and academic centers to illustrate those paths including:

- **INVENT by the Cleveland Clinic taking ideas to commercialised products**
  Through INVENT, a trademarked process, inventors (either individuals or teams) submit their innovations to a large team of market analysts and medical product experts, who assess the innovation and guide the inventors whose ideas are selected to commercialization of the proposed product. The process encourages innovations, including new medical devices, health information technology, and care delivery technology.

- **University of Pittsburgh’s Center for Medical Innovation co-investing and co-developing in small companies**
  The Center’s mission is to identify small companies that offer services beneficial to the University of Pittsburgh health system’s enterprise. The health system often invests in the companies and sometimes codevelops innovations with them. One such company, dbMotion, helped the University of Pittsburgh Medical Center meet its need to share data within its large network, which had been relying on many disparate information technology systems.

- **Geisinger’s ProvenCare sells care improvement tools to other organisations**
  Geisinger turned its innovation group into a for-profit entity called ProvenCare, which sells its care improvement tools—many aimed at improving value—to other organizations. These tools are essentially road maps for redesigning specific clinical systems, including those for acute care, chronic disease management, and primary care.

Dr Bates then reported on the major challenges in carrying out innovation within an operational clinical environment including the following:

- The innovation group may still be involved in day-to-day operations
- Under-investing in innovation
- Failing to set up methods to reinvest innovation profits
- Taking a short-term view

Dr Bates then reported on a study of continuous patient monitoring using IoT at Brigham and Women’s Hospital in the United States. The IoT system, “EarlySense”, consisted of a bed sensor that together with machine learning-based analytics of data from the device could create early warning and alerts of patient events. This application dramatically reduced false positive alerts: traditional methods of monitoring including pulse oximetry, cardiovascular monitors and telemetry produce 161-730 alerts per 100 hours compared to 2.2 alerts for the “EarlySense” system. The study indicated that the system was associated with a significant decrease in the length of stay time in Intensive Care Units.

Bates concluded with a view that while health innovation is needed across a continuum

- Every organisation needs to improve efficiency

---


A portfolio of activities and approaches to innovation is needed
To succeed, innovation needs to be enabled by:
- Easy data access
- Open APIs
- Regulatory Sandboxes

Chris Madsen Co-founder and CEO Aegon Bluesquare related issues around health care and innovation from a private health insurer’s perspective. Big Data can provide data to bring greater accuracy to calculation of risk to insured people and potentially also allow the insured greater choice in levels of coverage for services. A range of different sources of data could be used in making these calculations, including the makeup of the microbiome and genomic data.

Insurers are also increasingly getting involved with influencing beneficial behaviour and monitoring this through IoT and wearables. Customers can work to reduce their premiums on a sliding scale by showing that they are improving on their unhealthy behaviours. The sale of insurance policies with monitoring seems to be popular with customers. Insurers also use Big Data to tackle fraudulent claims through profiling and predictive modelling. Variables within each claim are matched against the profiles of past claims which were known to be fraudulent. When specific matches which are known to be indicative of likely fraud show up, the claim is flagged up for further investigation.

Mei Wa Kwong, Executive Director Center for Connected Health Policy detailed US Medicare reimbursement rules for remote patient monitoring. Recent regulatory developments in the United States shed light on possible successful policy actions.

The Centers for Medicare and Medicaid services are responsible for US State health insurance using a mix of state and federal funds. Medicaid is federal health insurance aimed at people who are 65 years and older and younger people with disabilities.

Various budgets have provided a very limited telehealth policy that has not changed much in recent years. The last policy update for these services was in the year 2000. Medicare coverage for telehealth services was authorized in 2000 as part of the Medicare, Medicaid, and SCHIP Benefits Improvement and Protection Act (BIPA). BIPA specified however that Medicare covered telehealth only for beneficiaries receiving services in a facility in a rural area, defined as a facility located in a rural health professional shortage area or a county that is not included in a Metropolitan Statistical Area.
In addition, video services are the only services reimbursed. Asynchronous store and forward services are limited to demonstration pilots in Alaska and Hawaii. There are proposed changes that would expand services to include chronic care physiologic monitoring, brief communication technology-based service (Virtual Check-in), remote evaluation of pre-recorded patient information and interprofessional internet consultation.

Medicare services are varied and differ from state to state:

- Live video is supported in 49 states
- Store and forward is supported in 15 states
- Remote patient monitoring is supported in 20 states.

It is not clear how the federal and state policy changes have impacted remote patient monitoring utilisation.

*Shana Vijayan from the Innovation, Research and Life Sciences Group of the Strategy and Innovation Directorate (UK)* presented data from the UK’s NHS Test Beds Wave 1 programme. The programme included real-word trials testing ‘combinatorial’ innovation (new combinations of products and processes) aiming to improve patient outcomes and at the same reduce costs of current practice; whilst supporting economic growth.

In Wave 1 of the Test Beds programme was unprecedented in scale- it included 7 sites piloting 5 health and care Test Beds and 2 IoT Test Beds with 40 innovators and 8 evaluation teams. There were 51 digital products tested and 75 partner organisations (including innovators, NHS, local authorities and third sector) involving 4,000 patients. The seven Test Beds are identifying solutions to support the transformation of clinical areas highlighted in the Five Year
Forward View including: primary care, urgent and emergency care, mental health, dementia and long term conditions.

The Test Beds programme was established to tackle barriers to innovation that included:

- Islands of innovation – isolation from each other and the infrastructure on which they function
- Lack of robust evidence – this is a major barrier to adoption
- Innovation in settings that do not have the work practice and infrastructure to support it.

Lessons learned from Wave 1 were around building effective partnerships, information governance and the importance of real-world evaluation.

Partnerships are effective when values of the partners are aligned, and relationships are formed before contracts are agreed. The set-up phase and project definition are critical in establishing an effective partnership.

Information governance relies on early agreement with experts being involved, an effective communication strategy and the use of information governance strengthening technologies.

Real-world evaluations rely on establishing evaluation criteria at the start of the project. There is not a one size fits all approach for all innovations and the understanding the context of the implementations is critical. Getting the Test Beds set-up took longer than anticipated.

Building in the future product viability from the start is also important. This includes: outlining a business case for interventions and reviewing as testing develops to ensure scalability.

The findings from Wave 1 will now be built into the Wave 2 programme. Early results shows that the innovations are having a positive impact on the quality of life of people living with a long term condition and changing the way they interact with their healthcare professionals.

Wim Rullens, Head International Organisations, Ministry of Economic Affairs and Climate policy in the Netherlands presented the results of a joint workshop with the OECD on Digital Health Innovations. The workshop was held in the Netherlands in April 2018.

Mr Rullens presented three topics from the workshop: Data sharing challenges; the creation of innovation hubs for health innovation in the Netherlands; challenges in building the connectivity infrastructure (5G).

The Netherlands has established the Dutch Smart Industry Field Labs – which aim to enable and support SMEs in developing ICT-related innovations. These facilities are of easy access for SMEs, which need to test and develop products and services for markets with high-speed innovation cycles, and have become an important complement to other more traditional research and innovation instruments. Some examples of smart industry field labs include the
3D Medical in UMC Utrecht, the Philips Innovation Center and the Holst Smart Industry Field Lab.

Mr Rullens reported on the challenges that policy makers face in stimulating the development and diffusion of smart health innovations and practices that rely on data-driven technologies. One of the topics of the discussion concentrated on the need for international standards for the sharing of (patient) data to facilitate AI-based diagnostics.

Policy makers also face important challenges in stimulating private investment to provide futureproof, secure and competitive connectivity, notably 5G-networks. The Netherlands has started 5G field lab pilots in 2017 including different industry sectors. For broadband and mobile communication infrastructure, the government in the Netherlands has in addition set the following goals:

- Good quality connectivity and service
- Competitive rates
- Support demand diversity
- Universally available

Some observations about innovation that arose from the workshop include new models of collaboration that are built on:

- Data Sharing
- Open innovation
- Innovation ecosystems
- Start-ups to pilot new products and processes
- Platforms leveraging crowds and networks

Mr Rullens concluded by noting that while privacy is important, it should not hinder innovation. Establishing rules around governance of patient data is critical. The transformation of national healthcare systems will require research and innovation measures as well as private sector product and services innovation.

**Key points**

1. **New innovation platforms are emerging:** triple helix in the Netherlands, NHS Test Beds in the UK, and successful examples of clinical and academic innovation centers in the United States
2. **Innovation of health care services is possible but there are challenges to overcome**
3. **There is growing evidence that RCTs are possible and produce clear evidence of financial and health benefits**
4. **Payment schemes from countries are evolving to meet the needs of new models of care but too slowly to keep pace with innovation**
5. **There are lessons to be learnt from the modernization of medicare physician payment schemes that recognize services furnished using ICTs in the United States.**
6. Use of big data for predictive risk modelling by insurers is increasing; there are however, significant ethical and privacy concerns that need to be adequately addressed to ensure consumer trust.

Session 5: Beyond the Hype: Use cases for new models of care

Moderator: Michael Hodin, CEO, Global Coalition on Ageing

Jeff Schwartz, Principal at Deloitte Consulting talked about the impact AI, robotics and automation will have on the future of work and society. The points he made included:

- Automation, cognitive technologies and AI and new talent models (including freelancers and crowds) are changing all aspects of work, workforces, and workplaces
- Exponential technologies are dramatically changing the pace at which work, jobs, and careers are being re-designed
- Longevity— and the “100 year life”— are changing the nature of careers and changing the game for ongoing reinvention and learning
- Augmented work and shifts of organization models to networks and teams are creating new opportunities for all workers
- All jobs will likely change in the coming decade focusing on human-machine partnerships and a new emphasis on essential and enduring human capabilities

Surya Kolluri, Bank of America Merrill Lynch related Bank of America’s response to financial services to an ageing population. In particular there is an unacknowledged but enormous population of informal/family caregivers. In the US, there are 40 million informal caregivers with $190 billion in annual expenses and out-of-pocket care costs.

Caregivers responsible for physical care (64%), financial care (92%) and emotional/social support (98%). Financial caregiving includes contributing financially, paying bills on a person’s behalf and monitoring of bank accounts.

At an individual level, this means US $7,000 annually spent on caregiving that has an impact on their own lives. This includes direct financial, emotional and social impacts on these individuals.

Banks and financial advisers are becoming aware of this problem and tailoring advice and services to meet their customers’ needs.

Steven Locke, Founder and CMO of iHope Network talked about the iHope Network which provides on demand mental health services to patients through videoconferencing.
Established with $1.4 million of NIMH funding, it concentrates on cognitive behaviour therapy (CBT) using established diagnostic and treatment protocols.

An important aspect of iHope is the selection and training of specific counsellors to provide the service rather than allowing any CBT specialist to provide care (as would happen for a platform service-oriented approach). There is a collaborative care model with safety protocols an important part of the care. The service is covered by most private health insurance policies and by Medicaid in most US states.

**David Weigelt, VP of Innovation for Home Instead Senior Care** presented an innovation project using tablets tailored for seniors. He outlined the challenges of innovation at scale for an organisation that is not experienced in innovation. Yet, given that Home Instead serves more than 75,000 senior clients each year and focuses its care on developing relationships that encourage independence and functional ability, the company clearly understands how seniors are able to and want to engage with technology.

**Key points**

1. IoT may potentially generate revolutionary changes in health care services for an aging population with significant impacts on health care
2. Remote caregiving changes financial and social models – the magnitude of the impact is only starting to be understood
3. It is important to recognize that the digital divide is still very real and it is possible that IoT-based services and mHealth, could potentially deepen this divide. The key is to stay focused on the needs of the end users.