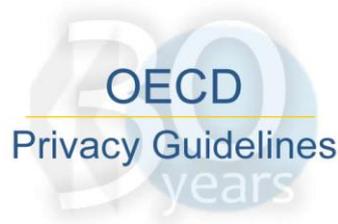


**Working Party for Information Security and Privacy (WPISP)
Working Party on the Information Economy (WPIE)**



Joint WPISP-WPIE Roundtable

**The Economics of Personal Data and Privacy:
30 Years after the OECD Privacy Guidelines**

**OECD Conference Centre
1 December 2010**

Summary of the Proceedings

ROUNDTABLE ON ECONOMICS OF PERSONAL DATA AND PRIVACY:

SUMMARY OF THE PROCEEDINGS

Paris, 1 December 2010

1. The Roundtable on Economics of Personal Data and Privacy was the last of three events organised by the OECD in 2010 to assess the evolving privacy landscape on the occasion of the 30th anniversary of the adoption of the OECD Privacy Guidelines. In particular, this event focused on the economic dimensions of the use of personal data. Understanding how personal data is collected and used in practice and measuring the economic and social benefits it generates can help inform consideration of the most appropriate governance frameworks for data protection and privacy.

2. Held at the OECD Conference Centre, the Roundtable was organised jointly by the Working Party on Information Security and Privacy (WPISP) and the Working Party on the Information Economy (WPIE). The discussions and findings from the Roundtable will be channelled as input to an OECD horizontal project on Intangible Assets and New Sources of Growth managed by the Directorate of Science, Technology and Industry (STI) and the review of the OECD Privacy Guidelines that is now underway.

3. The Roundtable agenda is attached as an annex. Along with speaker bios and presentations, it is also posted on the Roundtable website: www.oecd.org/sti/privacyanniversary. Also available on the website are three background papers commissioned for the Roundtable from leading researchers in this area. One is by Catherine Tucker (MIT Sloan School of Management) on "[The Economic Value of Online Customer Data](#)." The second one is by Michael A. Turner (Ph.D.) and Robin Varghese (Ph.D.) on "[The Economic Consequences of Consumer Credit Information Sharing: Efficiency, Inclusion, and Privacy](#)" The final one is by Alessandro Acquisti, (Heinz College, Carnegie Mellon University) on "[The Economics of Personal Data and the Economics of Privacy](#)." The Roundtable and background research have benefited from financial support from Industry Canada.

Opening Remarks

4. In his opening speech, Andrew Wyckoff, Director of Science, Technology and Industry, OECD set out the background and main themes of the Roundtable – to better understand how personal data is being used and the economic and social values generated by these uses. The 30 years since the OECD Privacy Guidelines have witnessed extraordinary developments in data storage capacity, high-speed networks to move data; and the rapid growth of computational power – all of which give the impression of a significant change in the way data is gathered and analysed to create economic value. But Wyckoff

cautioned that we do not yet have the economic indicators and data we need to be able to map this development. This is due to the large volume of data generated, but also to the variety of purposes and contexts in which personal data is used.

5. Noting that the Roundtable would not be able to focus on the privacy policies and practices that are essential to ensuring that uses of personal data are beneficial to individuals, Wyckoff highlighted that this event has been structured to better understand just how personal data is being used, and the increase or loss in economic and social value generated by those uses. Describing the orientation of the Roundtable agenda, Wyckoff expressed his hope that Roundtable participants would help identify areas for research and potential indicators that could help us understand the economic benefits of this data transformation.

Session 1: Big data and global flows

6. This panel looked at the extraordinary increase in the extraction and storage of personal data. From “big data” to metadata to “data exhaust” personal data is being used for a wide variety of purposes. Some examples discussed included the prevention of credit card fraud, elimination of deceased persons from voter rolls, identifying benefits fraud, tracking flu trends and even trends in dating. Panellists observed that one of the most important factors for making big data economically valuable is how it is matched and analysed in the information context. Also discussed were the implications for governance of big data and new methods of analysing and the potential measures to meet the emerging challenges.

Big data and data as a new economic asset

7. Kenneth Cukier, Japan Business and Finance Correspondent, The Economist, started off by pointing out that the cataloguing of data is not new and can be tracked back at least to ancient Syria. What is new, however, is that the data has become a new economic asset. Data is a raw material for almost all modern businesses – not just for the online services industry but also for the health care industry and so on. Organisations are driven to gather and share more of such raw materials. Jeff Jonas, Chief Scientist, IBM Entity Analytics Group and IBM Distinguished Engineer, addressed issues about the volume of data sharing, suggesting that by one measure some 144 copies are typically made of a piece of information as a result of a mature information back-up strategy. Then add internal and external information sharing between systems and then those systems’ backups. It is quite possible some data is copied over 1000 times. Information sharing between systems will continue to increase as organisations strive to improve efficiency, recognise opportunity, and mitigate risk. Marc Latouche, Director of Internet Business Solutions Group, CISCO, commented that the data traffic is set to increase further. In 2009, IP traffic amounted to 14.7 exabyte per month, but by 2014, it is predicted to increase to 63.9 exabyte per month, with 87% of the traffic generated by consumers. Furthermore, Latouche predicted that video would exceed 91% of global traffic source by 2014 and 56% of which would be video streaming.

Personal data processed in context

8. The value of big data is generated when pieces of data are put together in context. Jonas explained that as more personal attributes are combined, it becomes easier to make identity matches. He provided an easy to understand example of how matching various fields from a voter registration record, a department of motor vehicle record and a deceased person record (in the United States) could be done with analytics alone – no human review to accurately determine whether the registered voter is deceased or not. Data in context improves decision making.

9. John Boswell, Senior Vice President, Chief Legal Officer, SAS Institute, Inc, explained that analytics is in fact commonplace. Online banking and even recognising a family member are simple examples of analytics. Analytics provides huge economic benefits. Boswell provided some examples of

such benefits. The credit card financial model includes real-time transaction analytics that reduce the costs from credit card fraud by about USD400 billion per year. Gene therapy may be readily available as a result of reduced cost in genome sequencing. Fraudulent child care claims can be reduced with an expected return on investment of USD7 to USD30 million annually. These examples all require analytics and big data.

10. Data can extract further data from itself in the form of metadata. Viktor Mayer-Schönberger, Professor of Internet Governance and Regulation, Oxford Internet Institute, demonstrated the rise of metadata using the example of Flickr photos taken by iPhone. By uploading photos, the consumers are also uploading metadata, *i.e.* geo-location data of where the photos were taken and when. This data can be downloaded by anyone. Two billion photos uploaded via Flickr allow a creation of a map to track where tourists go and when. Mayer-Schönberger observed that the value embedded in metadata can be independent from the actual or base data. Even opt-out information becomes another set of information that may have value. For example, houses that opted out from Street View for security reasons may be targeted by thieves as potentially valuable properties to go after.

11. Mayer-Schönberger also discussed “data exhaust,” which is generated as a by-product from primary use and its value lies in the aggregate. A good example of a service built upon data exhaust is Google Flu Trend. By gathering data on when people are doing online search on flu, Google Flu Trend is able to provide a nearly real-time predictions of flu outbreaks. Another example is the use of indications of a change in relationship status on social networks, which can provide general trend information about when people tend to sever relationships, how long they last, and more. Metadata and data exhaust elevate the uses of personal data at another level, bringing new economic and social benefits.

Personal data governance and challenges

12. Panellists reckoned that the current regimes for information governance may not be adequate to an age of big data and global data flows. Jonas noted that the data breaches in a world of big data may result in new harsher laws and prosecution. Stricter rules may inhibit data from bringing values to the economy and society, as well as reducing transparency and accountability. Boswell also cautioned not to “throw the baby with the bath water” – suggesting that unwise regulations could make it so difficult to use and analyse data that the value of data may be lost.

13. Yoshiaki Tojo, Director, Information Services Industry Division, Ministry of Economy, Trade and Industry, Japan suggested that instruments such as guidelines, rather than harsh legislations, should be used to govern big data and global flows. Moreover, Tojo proposed that codes of conduct for information governance, privacy enhancing technologies (PETs), and privacy by design should be fully utilised. Mayer-Schönberger commented that we have reached the point where the states-based international approach of reaching international agreement might be too slow to address this issue. Both Mayer-Schönberger and Tojo agreed that the issue of personal data governance should be discussed not only in the context of data but also as an economic activity as a whole. Boswell indicated his expectation for the government to develop a sound personal data governance framework and provide certainty for the environment business can play.

14. The panellists also discussed tools and systems that may augment current information governance approaches. Tojo commented that there is a need for a platform for companies to share data without the fear of negative implications of privacy and corporate secrets. Tojo also suggested that the data should be collected and stored using subject identifiers to make it more secure. Business neutral players can manage such subject identifiers and put in place secure systems to re-identify personal data. The risk of unintended disclosure can, according to Jonas, be mitigated to some degree using central indexes, analytics in the anonymised data space, immutable (tamper resistant) audit logs and real-time active audits. Such tools can

help in allowing economic and social benefits from the use of personal data and protection of personal data, while at the same time improving information governance approaches.

Session 2: Valuing personal data in online and financial services

15. In this session, the panellists explored various practices of data collection and use in the financial services and online services sectors. The financial services industry has long been a leader in the use of data analytics. In recent years, it has further evolved to take advantage of the latest advances in information technology and vast data sets are now available. It has been joined by an online services industry, taking advantage of the large data sets and heavy analytics to minimise cost and maximise return on investment. Both have become skilled at generating value out of data aggregation and analytics, Strategically using data for product innovation and improvement as well as operational efficiency. Leading data brokers are now multi-billion dollar firms. Balancing consumer privacy concerns with better customer experiences is a common challenge both industries face as they enhance business models that are substantially reliant on personal data.

New players – online services

16. Catherine Tucker, Douglas Drane Career Development Professor in IT and Management, MIT Sloan School of Management, pointed out that there is nothing new about firms collecting and using data. However the methods in which they collect data have dramatically changed in the past decade or so. Companies now collect data online through cookies (Flash and HTML), beacons and packet inspection, which allow the online services sector to gather massive volumes of data through click-stream. Thanks, in part, to this capacity to extract value from large data sets, the online services industry has grown rapidly. As Tucker noted, search engines, online videos, social networking sites and content sites permit data collection practices not possible in the offline world. According to McKinsey's survey in 2010 quoted by Tucker, the overall value of the consumer-facing online services industry in the United States and Europe was EUR100 billion. These online services are generally free supported by the Internet advertising industry.

17. Gabriel de Montessus, VP Strategy & Corporate Finance, Hi Media, stressed that all the free services provided to the consumers by online services do not come free. The key to sustain free online services is optimised advertising, such as behavioural targeted advertising. People who create content need to be paid, as do those who provide the hosting services. De Montessus stated that the Internet is fragmented with myriads of websites and users, and therefore it is imperative for the advertisers to identify which websites and users they want to target in order to continue their business.

18. The online services industry has been capturing value of data beyond developing and offering services to consumers. Data can be used for organisational strategic purposes and even for public policy objectives. Tucker provided examples of how the online services industry uses clickstream data to optimise operations. Clickstream data allows optimisation of website content and increases sales by 20%. One example is Expedia, an online travel agency. The company was able to save USD12 million by using clickstream data to identify a flaw in the website design that was leading customers to insert the wrong billing address. Clickstream data allows companies to reallocate resources internally so that they can achieve better business outcomes.

19. Betsy Masiello, Policy Manager, Google, shared some examples of how Google provides public policy-oriented services based on the aggregated data collected from search results. Google Flu Trend analyses five years of search history to help predict outbreaks of flu. Google Flu Trend's accuracy in predicting flu outbreaks demonstrates the value of utilising data extracted from live data for secondary uses. Another example of data use for public policy purposes is Google Domestic Trends. Google

Domestic Trends tracks Google search traffic across specific sectors of the economy. Using historical and geographical data, it shows certain economic trends in specific regions. By drawing intelligence from vast amounts of loosely connected information, according to Masiello, it is possible to monitor social problems. Google Flu Trend and Google Domestic Trends offer examples of how data can not only be used to provide commercial services to customers but also to offer insights for organisational improvements and social issues.

Traditional players – financial services

20. One of the pioneers in developing data sharing systems and analytics is the credit reporting industry. Martin Abrams, The Centre for Information Policy Leadership, described the evolution of the credit reporting industry, noting that data sharing for marketing purposes goes back at least as far as the 1930s, with the automation of credit reports and credit scoring emerging in the 1960s. This automation allowed the financial services industry to not only become skilled at collecting, sharing and observing data, but also making faster predictions and decisions based on shared observations. Five exabytes of data is being collected every two days, an amount equal to all the data collected from the dawn of history until 2003. Data is not only contributed but observed and the observation becomes another valuable data. More predictive science and analytical models are applied to these observations as they increasingly become the basis for businesses. Abrams argued that observations and analytics are redefining the relationship of communities to markets.

21. Chris Gration, Head of External Relations, Veda Advantage, mentioned that information and its value are created by collection, processing and cleansing, analysis and interpretation of data as a part of the workflow of credit granting. It is the information derived from data that has economic and social value. The value of data lies in the data set, and therefore it is often unclear when the data are collected what the future value of the data will be. Another aspect of the value of data sets is that the consequences of individual decisions may be small but the value captured by credit reporting agencies and credit providers are large. According to Gration, the value generated from data collection and analytics in the credit reporting industry are two-fold. First, the economic value, which is the value derived from improved decisions made out of information. Second, the social value, which is generated from better identity verification, improved customer experience and access, increase in trust and social capital.

22. Gration also pointed out that regulation is a constraint and creator of both economic and social value for the credit industry. This is evidenced by the fact that data regulations match with the procedures for collection, data quality, use and disclosure. Regulations place discipline on the data management practices of the credit reporting agencies but they also provide incentives for the credit bureaus to create new data services that assist compliance with the regulations. In Australia, the net present value of the Credit Reporting Law Reform was estimated at USD1.7 billion. This figure is a testament to the dual nature of regulation for the credit reporting agencies.

23. Retail banks are increasingly using data-based predictive models for decision-making regarding customer acquisition campaigns, risk management and identity management. Joonhwa Choung, Team Leader of Customer Relationship Management, KB Kookmin Bank, described the extensive data collection and analytics systems for marketing campaigns that KB Kookmin undertakes. As the largest retail bank in South Korea, KB Kookmin Bank sends about 1 million marketing messages to its potential customers daily by mobile phone emails, computer emails, and phone calls. Thanks to the targeted marketing campaign based on the data analytics, the campaign boasts about 7.3% success rate. Data is fed from each branch real-time, which makes the data rich and up-to-date. The types of data collected range from demographic characteristics data to lifestyle characteristics data, customer needs data, customer awareness data, customer attitude data, customer intention data, post-purchase data, transaction data, contact history data and analysis data. KB Kookmin also conducts credit card marketing campaigns based on various types of

personal data and geographic information. This allows cluster analysis and regional market analysis that are utilised for better targeting and more efficient allocation of resources. Gration commented that such marketing solutions allow banks and credit reporting agencies to better quantify their return on investment (ROI) and offer value-based pricing.

Value of personal data and trust

24. As both the financial sector and the online services sector strive to further develop data analytics for the large data sets they maintain, they inevitably face challenges related both to legal compliance and the preservation of customer trust. Tucker emphasised that companies have always collected customer data but the ease, cost and scope of doing so has dramatically changed, including for sensitive information. In this context, anonymisation and strong data security management are pivotal for both industries that rely heavily on big data and data analytics. Masiello explained that Google anonymises search history data so that the company cannot track back to individual search history. Furthermore, Masiello highlighted the importance of avoiding the loss of value by data breach and security infringement. Choung shared details about KB Kookmin's comprehensive data security system and data protection procedures. According to Chuong, effective internal control and outflow prevention systems are vital to business and a security awareness programme and education should not be overlooked.

25. One of the participants to the Roundtable suggested that the cost of measures which are being taken to protect privacy (including security measures) is an important indicator for the value of personal data (since data are being collected for free). Gration argued that the biggest intangible asset is trust and the cost of losing trust when data are being lost is extremely expensive. Credit reporting agencies have a long history of being under tight regulatory control and have devoted considerable resources to data management and regulatory compliance. Gration noted that regulations can assist companies by providing incentives for them to preserve trust in their data dealings, but can also diminish the value of data by being overly prescriptive. Abrams analysed that the OECD Privacy Principles are roughly right in this regard. On the other hand however, Abrams mentioned that the restrictions on automated decisions by way of purpose specification and use limitation by the EU Directive may hamper the generation of economic and social values of data. Gration cautioned that often it is not clear how the data is collected and this fact should be taken into account when designing regulations on data use.

Session 3: Valuing personal data in the health sector

26. Panellists in Session 3 considered the overall landscape for health data use. The discussion included the need for effective use and sharing of health data for optimised provision of care, both in terms of greater potential for personalised treatment and in reducing overall health care costs. Panellists emphasised the need for approaches that recognised both the importance of protecting this sensitive data, but in ways that minimised the barriers to using health data to improve the quality of health care delivery, and efficient allocation of resources to improve the financial stability of the health care system.

Personal data in health care and electronic health records

27. Peter Desmond Singleton, Director, Cambridge Health Informatics and Principal Research Fellow, University College London, argued that information should be the lifeblood of medicine. Personal data in health care is not just about prescriptions and consultation notes. It includes demographics, entitlement and insurance, clinical communications, checklists and protocols, pathways and treatment plans, treatment and interventions, outcomes, orders and invoices and comparative performances. Frederike Diersen, Senior Legal and Policy Advisor, Ministry of Health, Welfare and Sport, the Netherlands, explained the important role that electronic health records can play in health care. Some of the values that electronic health records may bring, according to Diersen, are relevant information on the

spot at the right time; prevention of avoidable errors; prevention of recurring examinations due to an information-gap; safe and reliable exchange of medical data; increased perusal and influence from patients; and improved quality of health care and patient safety.

28. According to Diersen, electronic health records of 2.5 million citizens are available in the Netherlands as of 30 September 2010. There are several important features to the national electronic health records system in the Netherlands. First the data remains in local systems and there is no central database. The National Switch Point with corresponding technical, communication and content standards shares the data and there is no smart card with medical records embedded. A number of protections have been built into the process regarding, for example, what data is included, who has access rights and when, and patient consent.

29. One example of an international initiative to share health data for better medical care is the European Patients Smart Open Services (epSOS) project. Diersen explained that epSOS is designed to develop a practical e-health framework and an infrastructure to enable secure access to patient health information between different European healthcare systems. A patient summary and e-prescription will be available through epSOS. Ongoing challenges for the programme include issues related to access to the data for research purposes, consent (opt-in vs. opt-out) and differing privacy legislative requirements in different countries.

30. The shift towards electronic health records is also evidenced at the clinical data level. Anne Bahr, Deputy R&D Data Privacy Officer, Sanofi-Aventis, shared the results of recent pilot projects that Sanofi-Aventis has been exploring: the possibilities to use electronic health records for clinical research and “pharmacovigilance.” The projects follow strict privacy rules preventing the sponsor from directly accessing patient data. Data is automatically pseudonymised before transfer to the sponsor. Adverse events are directly detected and transferred to the sponsor and the health authority after approval by the doctor. Digitalisation of health records at both administrative and clinical levels seems to be the way forward for efficient and effective health care.

Trend towards personalised medicine

31. Singleton asserted that the 21st century healthcare will require much more data analysis to determine what works and what doesn't. Bahr explained that there is a trend away from “universal” medications towards “personalised medicine.” The same drug can be effective with one person and cause severe adverse reactions in another. Research is ongoing to identify biomarkers that help identify how a patient will react to a certain drug. The presence of certain genes or the identification of certain signs on medical images will help find the right drug for the right patient. According to Bahr, in order to study which biomarkers are linked with which reaction of a patient, there is a need for analysing how genetic data correlates with diseases and drugs. In clinical trials, increasing amounts of genetic data will be collected for this purpose. Genetic data will need to be stored in electronic patient records format in order for the doctor to prescribe the right medication. More data, not less, will be needed for more personalised treatment for patients.

Increased emphasis on cost efficiency and performance

32. Gerrard Abi-Aad, Policy Analyst, Directorate for Employment, Labour and Social Affairs, OECD, explained that personal data in health care can be used to indicate whether care is accessible, effective and safe. In terms of effectiveness, a recent UK study shows that over 40% or nearly 1.9 million hospital emergency admissions would have been avoidable if a better primary care had been provided. Regarding health care safety, recent Nordic data shows that over 12% of hospitalised patients experience adverse events, 70% of which were preventable, over half of which lead to disability and increased length

of stay. With OECD countries facing continued upward pressure on health spending brought about by demographic change and increased costs of medical technology, there is a greater need than ever to utilise health data to measure quality and cost effectiveness.

Sharing health data and privacy

33. Elliot Maxwell, President, E-maxwell and Associates, reiterated the importance of better mobility and access to the information in a health care system that is under severe financial constraints. However, conflicting regulations and disparate data management policies by institutions are hampering the sharing of health data. Singleton reckoned that privacy of health data is critical, but for most people it is secondary to health itself. Implementing privacy principles like use limitation and consent can impose costs on the delivery of costs-effective health care. There is definitely a strong need for improved understanding among patients as to what the data sharing choices are related to their healthcare and their implications. Not sharing information may mean poorer care. Maxwell added that improvement of the quality of health care would also depend in part on the transferability of data from country to country, and that steps are needed to facilitate these exchanges. National policies encouraging greater openness will facilitate using personal health information to improve healthcare but we still need to wrestle with issues of de-identification of large data sets.

Session 4: The business of privacy

34. This session examined how data protection and privacy management have become strategic business drivers and identified a number of tools and schemes that been developed as a result. There have also been studies on the behavioural economics of privacy which reveal that some common perceptions regarding notice and choice may not match observed behaviour, and that different approaches may be needed to encourage consumers to act in a way that protects their privacy.

Privacy – good business

35. David Smith, Deputy Information Commissioner, United Kingdom, opened the session by saying that privacy makes good business sense. By making sure that personal data is properly collected and managed, the value of the data itself will go up and thus it is beneficial for business to see data protection as the enhancement and protection of an economic asset. J. Trevor Hughes, Executive Director, International Association of Privacy Professionals, added that privacy has become a comparative differentiator for businesses. There has been a shift in the role of privacy professionals from one of mere legal compliance to one that reflects a more holistic view of data as an important strategic asset for organisations. The protection of personal data is no longer seen as simply a cost centre, but rather as an important part of managing a valued organisational asset.

36. Despite the recognition of privacy as a good business, Smith pointed out that privacy enhancing technologies (PETs) have not been widely adopted by businesses. In many companies it is still difficult to convince management to invest in PETs, while there is still no obvious and immediate correlation with profits. Andreas Krisch, President, European Digital Rights, stressed that the business of privacy is about building and meeting trust between data processors and data subjects and that fundamental rights are sufficiently protected.

Tools for Enhancing Privacy

37. Paolo Balboni, Executive Director of the European Privacy Association, agreed with the panel that privacy compliance is a business asset. As an example he cited cloud computing service providers, who are increasingly using data protection as a promotional point. He also discussed trustmarks, which can be a tool for businesses to communicate legal compliance as well as trustworthiness. Trustmarks are easier

to understand than privacy notices and fairer to the consumers. However, according to Balboni, many current trustmark schemes are not reliable due to problems with certifier independency, impartiality in auditing, and limitations on monitoring and enforcement. On the other hand, the programmes that are more trustworthy are not necessarily successful, because by making it more difficult to obtain a seal, they end up with fewer participating organisations and reduced brand awareness. Nevertheless, there are some opportunities for trustmarks to evolve as a reliable tool, building on momentum from recognition in the Digital Agenda for Europe and the opinion of the Article 29 Working Party on accountability.

38. Krisch introduced to the audience the privacy seal for data protection compliant IT services and applications developed by the data protection authority in the State of Schleswig-Holstein, Germany. Privacy seals give businesses competitive advantage for certified products and services. They may even attract interest from businesses that do not have a relationship with the State of Schleswig-Holstein. Krisch also explained the European Privacy Seal – EuroPriSe. EuroPriSe certifies IT products and services as compliant with the data protection regulations. Criteria for the certification are based on the EU Data Protection Directive and the seals are valid in all member states. Evaluation is carried out by legal and technical experts and the seals are awarded by an independent authority. For Krisch, privacy seals are a useful tool for consumers to discern which products and services are safe, but also for businesses to promote themselves and gain competitive advantage.

Consumer behaviour and privacy protection

39. Alessandro Acquisti, Associate Professor, Heinz College, Carnegie Mellon University, presented some economic perspectives on privacy. First, he outlined theories from the Chicago School of Economics, which predicted that too much privacy might lead to inefficiencies and distortions in the marketplace. Under the Chicago school, market forces alone could lead to an economically optimal level of privacy protection, but only if consumers are fully informed, sophisticated and forward looking. Then, Acquisti presented alternative economic theories that come to the opposite conclusion: without privacy protection, consumer and social welfare may suffer.

40. Secondly, Acquisti discussed some empirical studies involving the role of privacy-related information in individual decision making processes, which often produced paradoxical results. For example, the greater the privacy reassurances provided to individuals before they are asked to complete a sensitive questionnaire, the greater their reluctance to reveal personal information in the questionnaire – because the strong privacy reassurance primes the individuals about the sensitivity of their data. Acquisti suggested that the apparatus offered by modern behavioural economics, provides growing evidence that consumers' privacy decision-making is adversely affected by incomplete information, bounded rationality, and cognitive and behavioural biases – elements that had been ignored or discounted in the Chicago School studies. Recognising these biases can help inform regulatory policy and technology design to improve decision-making.

41. Owen Tripp, Co-founder and Chief Operating Officer, Reputation Defender, described a new pay-for-privacy model that is giving rise to a new set of companies that can monetise and advocate for their customers' preferences. Consumer-driven solutions to privacy management can offer an excellent return to the businesses that sponsor them. There is a growing demand from consumers to know what information there is about them on the Internet. Private individuals will pay for a public-utility type of service to communicate their preferences to firms willing to honour the privacy wishes of their end users. Reputation Defender provides a full dossier of information about what is available online and adds that interest in this kind of service is on the rise. Choices on privacy are almost always contextual and consumers tend to undervalue what it is really worth in exchange for free service – they don't really understand how the data will be used, not by the organisations that offer these free services, not by others.

This lack of understanding how data can and will be used is the reason why we see the paradoxical behaviour of consumers towards privacy.

Conclusion: examining the implications for privacy governance and mapping future work

42. The final session focused on the role of government and the need to ensure consumer privacy protection while also protecting the free flow and beneficial uses of personal data. Daniela Battisti, Agency for Inward Investments and Business Development, Italy (Chair of the WPIE), highlighted the importance of addressing the role of governments in striking a good balance between protecting personal data and promoting economic growth via use of personal data – a recurring theme during the Roundtable.

43. Steven Lett, Deputy Coordinator for International Communications and Information Policy, Department of State, United States, highlighted that governments need to make sure that consumers are confident about their privacy. Multi-stakeholder policy-making is key to creating trust in the system (which is important for sustainability and continued growth). However, the governments must not create regulations that are too prescriptive which undervalue the use of data and also run the risk of running behind the technological curve.

44. Sophie Nerbonne, International and IT Department, CNIL, France, laid out three key themes that CNIL has been focused on in order to establish effective rules that protect consumers, yet promote the value of personal data. First, reinforce the rights of individuals and use technology better. Enable individuals to protect their own rights, especially online. Second, introduce Privacy by Design and promote the use of PETs and privacy impact assessments (PIAs). Lastly, simplify and adopt rules at the global level. Adoption of an international framework for data protection is key to achieving this and Nerbonne believed this should be achieved by an extension of the Madrid Standards on the Protection of Privacy and Personal Data

45. Mark Lange, Senior Policy Counsel, Microsoft Corporation, explained the massive economies of scale that cloud computing offers, but also raised some policy challenges. These include control of data, clarity of the legal rules that apply, and transparency issues regarding privacy policies that are crucial for cloud computing. In this context, Lange suggested possible areas of examination by the OECD could include gaining a better understanding of the context of data use, the measurement of benefits and risks; and potential benefits for further harmonisation.

46. Anna Fielder, Steering Committee Member, Civil Society Information Society Advisory Council, reminded the audience that privacy is a fundamental human right and questioned why so little attention had been paid to the costs of the detriments from privacy breaches, both for individuals and for businesses. Fielder further commented that there should be more information on the value of personal data. She further encouraged the OECD to take a more detailed look at alternative business models and their economic value. Noting that PETs had been discussed repeatedly during the Roundtable and the OECD already did some work in this area in the past, she called for an examination of how PETs can be more widely promoted and marketed.

Closing remarks

47. Keith Besgrove, First Assistant Secretary, Department of Broadband Communications and the Digital Economy, Australia (Chair of the WPISP), closed the Roundtable. He said that we need to think about data quite differently in the future. Not just governments but also markets are which are being regularly surprised by new possibilities. Besgrove commented on two themes that have emerged as key changes in the 30 years since the Guidelines were adopted. The first relates to the changing role of the individual. Individuals can now create, share and publish data about themselves, families, friends, in ways

that could not have been contemplated or imagined when the Guidelines were drafted. This is a theme that was explored in some depth at the OECD conference in Jerusalem. The second key theme, he noted, was the focus of the Roundtable: the sheer scale of data generation, storage, flows and use, and the kinds of analytical processes and predictive outcomes that are now possible.

48. Besgrove explained that the Roundtable was the kick-off of a new work stream on measuring and valuing the role that personal data is already playing in the economy. He commented that the OECD is very well placed to do this work and the Working Party for Information Security and Privacy is pleased to be working jointly with the Working Party on the Information Economy on this matter. The economic insights gained in the work will in turn help ground the policy work for the delicate task of reviewing the Privacy Guidelines which the WPISP will be undertaking. Although the outcome of the review is not yet known, Besgrove concluded that it will certainly benefit from a more sophisticated understanding of what is at stake in terms of the underlying economics of the role that personal data plays today.