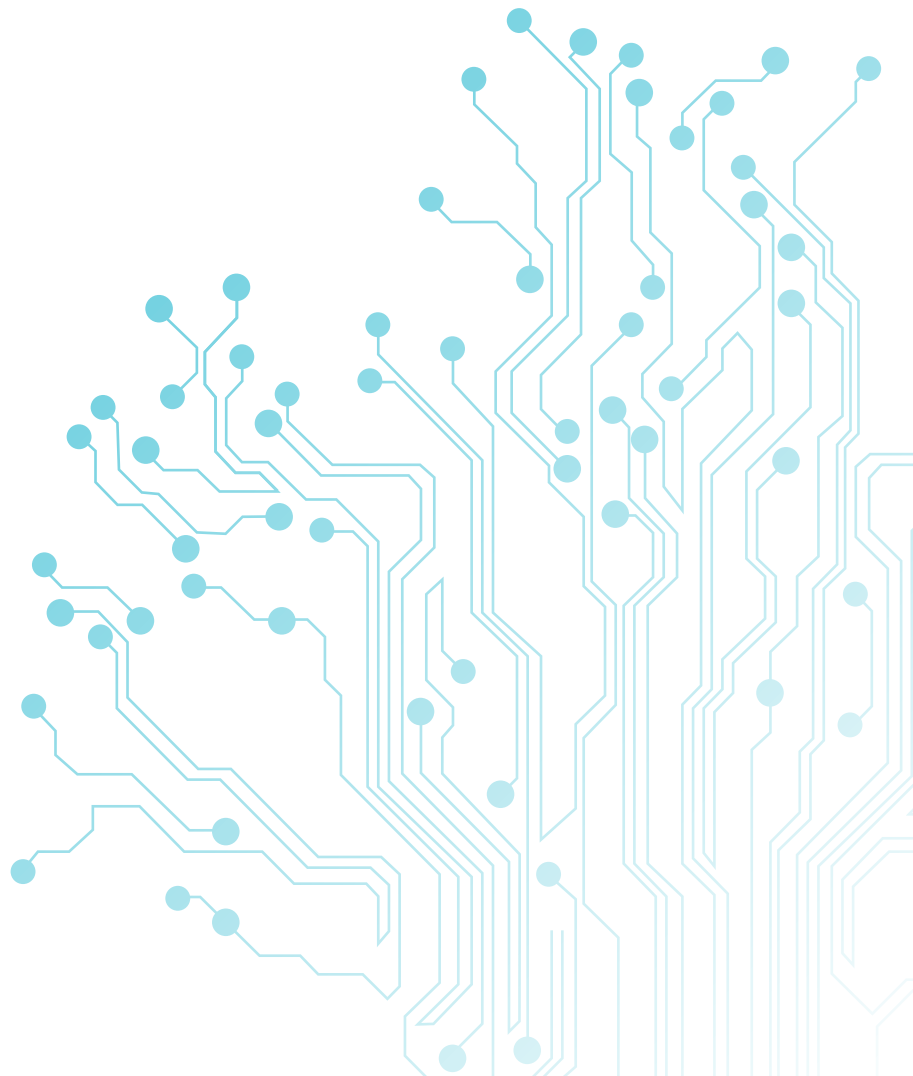



Reframing data transparency_

Centre for Information Policy Leadership and Telefónica
Senior Roundtable
30 June 2016





The objective of the Roundtable was to build on recent projects, initiatives and legal changes related to data transparency, such as the EU-US Privacy Bridges project which explores new approaches to data transparency and the enhanced transparency provisions of the General Data Protection Regulation.

Foreword



Bojana Bellamy
President, Centre for Information Policy Leadership

Data transparency is a foundation on which responsible organisations build trust and digital confidence in the modern information age. It enables individuals, organisations and society to benefit from data-driven innovation and ensures a more effective protection of individuals and their data privacy rights.

This paper is a call for action to organisations, data privacy regulators, policy makers, technologists and other experts to work together to enable a new user-centric and sustainable data transparency.



Chema Alonso
Chief Data Officer, Telefónica

We believe that data-driven services can be a powerful and positive force in society. As we lead the transformation of our industry, Telefónica's strategy is to give the data back to its customers.

Telefónica will empower its customers to better understand and manage their communications services, and to use their data to improve their daily lives eventually using hundreds of new, smart data-driven services on their own terms. Our mission is to build and sustain the trust of our customers and the communities in which we operate. We hope that this contribution to the development of a new model of data transparency will stimulate debate, and that you will join Telefónica on its journey to enable better digital lives.

Executive Summary

On 30 June 2016, the Centre for Information Policy Leadership at Hunton & Williams LLP ('CIPL') and Telefónica held a joint Roundtable in London, with senior business leaders, data privacy officers and lawyers, data privacy regulators and academic experts, entitled '**Reframing Data Transparency**'.

The objective of the Roundtable was to build on recent projects, initiatives and legal changes related to data transparency, such as the EU-US Privacy Bridges project which explores new approaches to data transparency and the enhanced transparency provisions of the General Data Protection Regulation. The Roundtable brought together representatives of the European data protection authorities; the European Data Protection

Supervisor; business and privacy leaders from international corporations; small and medium-sized businesses; start-ups; academics and researchers to discuss new approaches to transparency that aim both to protect the fundamental rights and freedoms of individuals and enable data-driven economic growth and digital confidence in the modern information age.

Nine themes which were explored during the Roundtable:

1

The transparency deficit in the Digital Age which results from the growing **gap between legal and user-centric transparency**. On the one hand, **legal transparency** focusses on disclosing the data handling practices of companies to individuals through lengthy, complex and highly legalistic privacy notices and policies that are often not read or understood by individuals. On the other hand, **user-centric transparency** provides individuals with the right type and amount of information about the data practices of companies. User-centric transparency also provides individuals with effective tools which individuals can use to manage and/or control the disclosure of their personal information to companies;

2

The **transparency deficit** in the Digital Age negatively impacts on **customer trust**, customer participation in the digital economy and economic growth. As trust is a cornerstone of the digital society and data-driven economy, it is imperative to address the trust deficit by developing innovative and effective data transparency approaches that bridge the gap between legal and user-centric transparency;

3

The **challenges of delivering user-centric transparency** in a connected world where there may often be no direct relationship between companies and their end-users and where consent may not always be practical or effective;

4

In the Digital Age, **data transparency** is not just a legal challenge but rather a **multi-stakeholder challenge** which involves the participation of data privacy regulators, companies, individuals as well as new stakeholders, such as behavioural economists, social scientists, psychologists and user experience specialists;

5

Data transparency is a critical business issue as it drives customer trust, business and economic opportunity. Data-driven companies need to approach user-centric transparency as a **business goal and a business challenge**;

6

New, **user-centric transparency tools and approaches** are needed in order to achieve real transparency for individuals, generate and maintain trust in the digital economy and build customer relationships. To build loyalty and digital confidence, data-driven organisations must become more fluent in explaining the **value exchange** between them and their customers. They must also explain their own data practices to their customers as well as reassure customers about how they safeguard customer data;

7

Data protection authorities and other regulators have important roles in **fostering** new data transparency tools and approaches by adopting a **'smart' approach** to data regulation. This involves selective and effective enforcement action; improving legal compliance through dialogue, guidance and collaboration; recognising the multiple compliance motivations of companies and using such motivations as leverage to achieve compliance; and offering tangible benefits such as liability reduction to companies which deploy effective approaches to data transparency. Data privacy regulators should also highlight **'best data transparency practices'** by regularly showcasing and publishing general and/or sector-specific transparency practices and standards based on actual satisfactory transparency measures and tools;

8

There are close links between transparency and education. Individuals need to be **educated** so that they understand better the uses of data, the data management tools available to them, their rights as well as the benefits of personal data processing. Education should be delivered through multiple channels and actors, ranging from traditional education at schools and universities, to consumer education campaigns led by consumer bodies, government agencies, regulators and industry; and

9

Behavioural economists, social scientists, psychologists and user experience specialists will play key roles in helping companies deliver effective user-centric transparency. These stakeholders will help companies understand the most effective ways in which they can provide their customers with information about their data practices, when and how such communications should be provided and the type of information that individuals want to or should know.

1. Introduction

On 30 June 2016, CIPL and Telefónica held a joint round table in London, with senior business leaders, data privacy officers and lawyers, data privacy regulators and academic experts, entitled “Reframing Data Transparency” (“Roundtable”).¹

CIPL is a global data privacy and information policy think tank, based in Brussels, London and Washington DC. CIPL is currently conducting a number of research projects in the fields of data protection and privacy, including its two-year project on the consistent implementation, interpretation and enforcement of the General Data Protection Regulation (‘GDPR’).²

Telefónica is one of the largest telecommunications companies in the world, providing close to 330 million fixed, mobile and broadband connections in 21 countries around the world. Telefónica has a strong presence in Spain, Europe and Latin America, where its data strategy enables its customers to take back control of their digital lives.

Transparency is a fundamental concept and requirement in many data privacy laws around the globe. It requires organisations handling personal data to be open with and inform individuals of their data uses and practices.³ In the US, the Federal Trade Commission takes action against companies whose privacy policies are misleading, deceptive and in general do not correspond to their data practices. In Europe, the GDPR has realigned the role of transparency within data privacy and enhanced the transparency obligations of organisations.⁴

Transparency is also an increasingly critical **economic issue** as it drives trust in digital life or “digital confidence”. **Digital confidence** is a key enabler of digitalisation which in turn promotes economic growth.⁵ Moreover, transparency is a vital element of enhanced organisational accountability.⁶ Many organisations are developing new transparency approaches that go beyond traditional privacy notices and embed the information about their data practices and policies within the user experience itself. For example, many companies use dashboards, portals, apps and contextual information to provide information to their customers especially where consent is not practicable or effective. Such companies aim to reassure their customers that their data is being used responsibly and in ways which respect their fundamental rights and freedoms. These emerging approaches gain the necessary buy-in from the individuals and society whilst providing better digital services.⁷ Success requires the acceptance of a dynamic approach, in which different stakeholders continuously research and innovate to effectively maintain public trust and satisfy specific needs that may vary depending on the particular context, service or even territory.

¹ See Appendix.

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
The GDPR will apply on 25 May 2018.

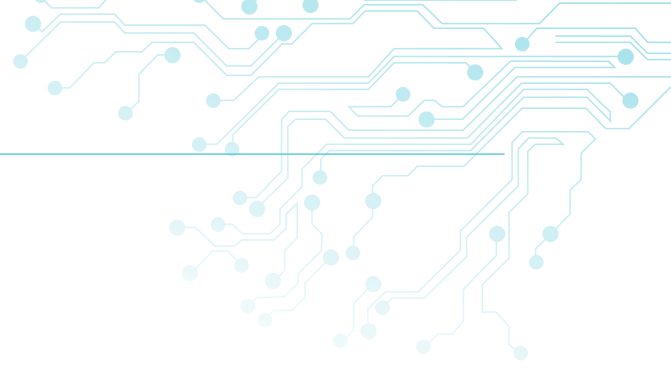
³ See, section 5 of the Federal Trade Commission Act. 15 USC § 45(n).

⁴ For example, Articles 12, 13, 14 and 15, GDPR.

⁵ For example, by Telefónica's Index on Digital Life, <http://indexdigitallife.telefonica.com/>

⁶ CIPL, “The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society” (October 2015) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/protecting_privacy_in_a_world_of_big_data_paper_1_the_role_of_enhanced_accountability_21_october_2015.pdf

⁷ Bojana Bellamy and Markus Heyder, “Empowering Individuals beyond Consent” (IAPP, 2 July 2015) <https://iapp.org/news/a/empowering-individuals-beyond-consent/>



As explained in Section 2, it is widely accepted that current approaches to data transparency which revolve around lengthy, complex and legalistic privacy notices are not effective in delivering a meaningful education to users about the data practices of companies. The mission to deliver effective and user-centric transparency as well as user controls, is at the heart of many current initiatives. For instance, various projects at the Data Transparency Lab,⁸ dashboards and apps from companies, such as Google⁹, Facebook¹⁰, Vodafone¹¹ and Movistar,¹² enable customers to review, monitor, download or analyse how their data is used.

The Roundtable and this report seek to build on recent policy discussions, initiatives and laws on transparency. In particular, the EU-US Privacy Bridges project¹³ aimed to identify areas for common action that would be practical, would not involve legal or constitutional amendments and would have a positive impact on the level of data privacy on both sides of the Atlantic. The EU-US Privacy Bridges project specifically recommended “user controls” and “new approaches to transparency” as two key areas for further development. Equally, the new GDPR places an increased emphasis on transparency, and makes it essential for organisations to develop and refine their approaches to transparency.

To build on this momentum around data transparency, the Roundtable aimed to explore new and effective approaches to transparency which protect the fundamental rights and freedoms of individuals and enable data-driven economic growth. The Roundtable brought together over 50 participants including representatives of the European data protection authorities (“EU DPAs”); the European Data Protection Supervisor; European and US multinational companies; small and medium-sized businesses; start-ups; academics; and researchers.

In this report, we explore the main takeaway points from **nine themes** which were explored during the Roundtable, namely:

- 1 The **transparency deficit** in the Digital Age;
- 2 The impact of the gap between **legal and user-centric transparency**;
- 3 The **challenges of delivering user-centric transparency** in a connected world;
- 4 Data transparency as a **multi-stakeholder challenge**;
- 5 The **roles of data protection authorities (DPAs)** in promoting and incentivising innovative and useful data transparency approaches and tools;
- 6 The **roles of companies** in researching and developing new and effective approaches to data transparency;
- 7 The importance of **empowering individuals** by providing them with clear, meaningful and effective information about the uses of their data and user-centric controls; and
- 8 The roles of **technologists, behavioural economists, social scientists and psychologists** in delivering new transparency measures and bridging the gap between legal and user-centric transparency.

⁸ <http://www.datatransparencylab.org>

⁹ <https://myaccount.google.com>

¹⁰ <https://www.facebook.com/help/131112897028467/>

¹¹ <http://www.vodafone.co.uk/explore/apps/vodafone-netperform/>

¹² <http://www.movistar.es/particulares/movil/servicios/app-mimovistar/>

¹³ <https://privacybridges.mit.edu/>

2. Data transparency: Framing the challenge

All Roundtable participants agreed that **data transparency** is a core element of any data protection law framework in the Digital Age where swathes of online and offline information about individuals are being gathered, shared and analysed by an increasing number of organisations for various purposes including research, analysis, product development, marketing, operational efficiencies as well as delivering benefits to the society and the individuals.

Roundtable participants framed the challenge of data transparency in the following terms. Traditional data transparency approaches focus mainly on the aspects of transparency prescribed by the **applicable data privacy laws**, such as the fair processing obligations¹⁴ or the need for organisations to provide individuals with detailed privacy policies and notices about the uses of their data to avoid deceptive behaviour and regulatory enforcement.¹⁵

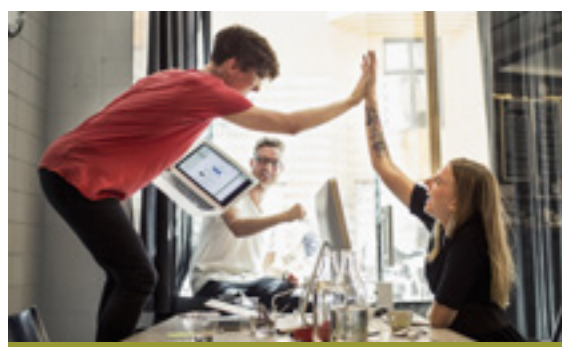
Generally, most organisations discharge these informational obligations by informing their customers of their data practices in **lengthy, complex and highly legalistic privacy policies and notices**. Most individuals do not read these privacy policies and notices.¹⁶ Consequently, whilst such notices and policies demonstrate compliance with data privacy laws, they do not help companies to build digital confidence. In many cases, these policies and notices are also bundled with the terms and conditions of the service or the product that companies offer. Thus, if a consumer wishes to buy the related service or product he or she has little choice but to 'accept' the privacy policies and notices.



In the Digital Age of connected homes, smart cities, ubiquitous mobile devices, artificial intelligence, machine learning, ingestables and wearables, it is difficult for service providers to meaningfully and effectively inform people of their data practices using traditional privacy policies and notices and related tick-box approaches.

Most stakeholders agree that in order to deliver real and user-centric transparency, organisations must find new ways, which are more suitable to the service or product in question, to achieve the necessary data transparency. Early examples include notices in simpler language or rich media. More transformational approaches aim to embed transparency and choice within the user experience by using dashboards, control panels, custom build apps and interfaces. Many of these approaches go beyond the parameters of **legal transparency** and enable companies to distinguish themselves from their competitors and effectively build and maintain **consumer trust**.

All the Roundtable participants agreed that trust and digital confidence are the cornerstones of the digital society and the data-driven economy. At present, the lack of user-centric transparency impacts on the individual's trust in the data practices of some organisations and impedes their full participation in the data economy. This trust deficit may be addressed by new and engaging approaches to data transparency which bridge the gap between legal and user-centric transparency.



¹⁴ E.g. Article 5(a), GDPR.

¹⁵ E.g. USC § 45(n).

¹⁶ Aaron Smith, "Half of online Americans don't know what a privacy policy is," (Pew Research Centre, 4 December 2014) <http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/>

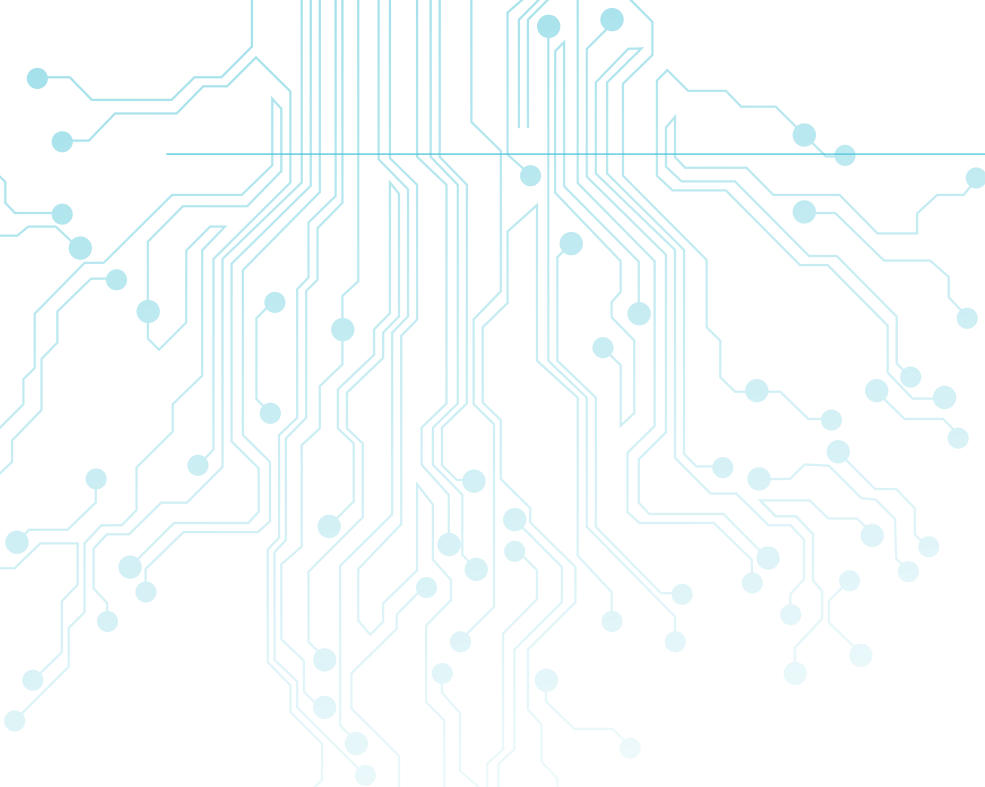
3. Data transparency: A multi-stakeholder challenge

Roundtable participants agreed that in the Digital Age, data transparency should not be approached simply in terms of legal compliance. Data transparency is a **multi-dimensional challenge** which should be tackled by a wide range of stakeholders. In particular, the following actors have key roles to play in solving the transparency gap and deficit:

1 For all organisations, data transparency must become a **critical business issue, an economic opportunity as well as a driver of business and trust**. Within the wider and increasingly strategic role of privacy, transparency should take centre-stage in the customer experience. Transparency is also a cornerstone of organisational accountability and digital responsibility.¹⁷ Businesses must not only deliver legal transparency, but also adapt their customer experience to achieve meaningful and user-centric transparency. This will require input from behavioural economists, social scientists, psychologists and user experience specialists who will assist businesses operating in this new paradigm to deliver this intangible yet crucial consumer, business and societal benefit;

2 **DPA's and other regulators** should establish and promote incentives for the creation, development and rollout of new and more meaningful approaches to data transparency. They could highlight and socialise "best practice" as well as facilitate the exchange of ideas about and new insights into transparency developed by industry, academia and other researchers; and

¹⁷ See n 6.



3 Transparency and **consumer education** go hand in hand. Individuals need to be educated in digital literacy. In general, people need to understand better the uses of data, the control and data management tools available to them, their rights, as well as the benefits of personal data processing. Education should be delivered through multiple channels and actors, ranging from traditional education at schools and universities, to diverse education campaigns led by consumer bodies, government agencies and regulators, as well as businesses. The media has a special role to play in demystifying the behind-the-scene data practices and flows and championing the benefits of data-driven innovation and the digital society.



4. Data transparency: Empowering the individuals_

The data-driven economy often means that there is more reliance on organisations to protect the individual without his or her input and less opportunity for, and emphasis on, consent. New and effective approaches to transparency are essential to instil full confidence that organisations are handling personal information as expected by customers and regulators.¹⁸

Roundtable participants agreed that new data transparency approaches can be more effective if individuals are educated about the following three key matters.

Firstly, given public concerns regarding corporate and State use of data and surveillance, more work should be done to ensure that individuals understand the **benefits of processing personal data**. Data processing can often deliver benefits to consumers, the economy and the wider society. For instance, real time Big Data analytics can help in the early detection of medical conditions such as pancreatic cancer, which have a high mortality rate and are generally untreatable by the time of diagnosis. Other examples include smart city services like video cameras and sensors, which allow city administrations to respond immediately to crime, accidents, power outages and natural disasters. There should be greater emphasis on the potential benefits of data analytics for society whilst respecting fundamental rights and freedoms.

Secondly, individuals should be educated about the **emerging tools and features** which they can use to manage third-party access to their personal data including self-reported data (such as an email address submitted upon signing up to a website), digital exhaust (for example location data and browsing history created when using connected technologies or mobile devices) and profiling data (using profiling data to, for example, predict the purchasing habits of individuals).

Innovative technologies, such as ad blocking and encryption tools, help individuals to proactively manage and control third-party access to their information. Such technologies empower individuals to make **informed and context-specific decisions** about data disclosure. For instance, some individuals may not object to one company processing a specific type of personal data if such processing provides them with a benefit that they value. However, the same individuals may object to another company using their data for other purposes, which they do not value as much. Organisations should be given sufficient latitude and flexibility to innovate and develop user-centric controls.

Finally, individuals should also be educated about their rights under data privacy laws and should also be provided with **simple, user-friendly and effective ways** to exercise their rights. For example, organisations can develop cutting-edge tools and features that enable their customers to exercise their access rights and view the data held by organisations at the click of a button. For example, Facebook users can download a copy of the data which Facebook holds about them including posts, messages, photos, clicked on advertisements and IP addresses. Similarly, Acxiom has rolled out 'Aboutmydata.com' in the US which enables individuals to know which information the company has about them as well as update and correct the information.¹⁹

¹⁸ See n 6.

¹⁹ <https://aboutthedata.com/portal/registration/step1>

5. DPAs and data transparency

DPAs will play a key role in promoting and fostering new data transparency tools and approaches in three main ways.

1 Firstly, the Digital Age requires **'smart' data regulation**. This means not only progressive and future-proof rules and laws, which both effectively protect the fundamental rights and freedoms of individuals and enable data innovation and digital society, but also "smart" regulators who are overseeing these rules. This also involves DPAs using their enforcement powers selectively in order to be effective, and adopting a more open and collaborative approach to legal compliance. DPAs must also recognise the multiple compliance motivations of organisations and adopt an incentive-based approach to compliance that responds to such motivations.

In the context of transparency, this means that **DPAs should incentivise and engage** with organisations to develop new and effective approaches to data transparency by offering tangible benefits such as liability reduction, or allowing data to be used more freely to drive innovation, growth and societal benefits. Flexible and holistic implementation of data privacy laws will mean that DPAs should consider the spirit and objectives of the law as well as outcomes when determining if an organisation has fulfilled its transparency obligations. User-centric transparency delivers better results for individuals. It empowers them and protects their fundamental rights and freedoms more effectively. This is pivotal in digital contexts where it is often hard, if not impossible, to comply fully with rigid privacy notices requirements.

2 Secondly, DPAs should be effective when using their enforcement powers, such as investigation, audit and inspection, to **assess how companies meet and deliver their transparency obligations to their customers**. DPAs should evaluate if and to what extent the processing operations of the organisations are in line with their internal and external data privacy policies. They should also understand the transparency challenges that new technologies create for organisations and individuals. This will involve collaborative and consultative engagement between DPAs and organisations before, during and after enforcement.

3 Thirdly, DPAs should take a leading role in supporting and highlighting **'best data transparency practices'**. They should regularly showcase and publish examples of general and/or sector-specific transparency practices and standards, based on actual successful transparency measures and tools that have been developed and deployed by various organisations. Highlighting best-in-class data transparency would have positive effects on the organisations being praised, as well as their peers and competitors. This would also enable DPAs to achieve economies of scale as the market and specific sectors move on to emulate best practices. Similarly, DPAs can reserve the **strongest sanction** for deliberate, wilful, unscrupulous or grossly negligent breaches of data transparency.

6. Delivering user-centric transparency: Information challenges

Behavioural economists, social scientists, psychologists and user experience specialists are some of the new stakeholders who will play important roles in bridging the existing gap between legal and user-centric transparency by enabling organisations to understand the following:

What:

The **types of information** which organisations should provide to individuals about how their personal data is processed. In other words, what are the really important facts and information that the individuals actually want to and should know? The contents of transparency tools should be driven by the concerns of individuals, the data processing context and use as well as be based on what individuals really want to or should know, rather than on strict legal requirements. Equally, individuals should be informed about the use of data that they do not know about, or do not expect but should know about, or should expect. They should also be more informed about any data use that may threaten their fundamental rights and freedoms and how such risks and their negative impacts are mitigated. What individuals really want to know must be determined by taking into account research, cultural and geographical differences.²⁰

It is also important to explore further the **limits of transparency**. Transparency cannot be absolute and impede on other fundamental rights and legitimate interests. Commercial considerations, such as trade secrets, intellectual property rights

and know-how, may mean that in many cases companies cannot fully disclose all their data handling practices. Moreover, certain forms of transparency, such as disclosing the data or processing algorithm, may be counter-productive as it is debatable to what extent such disclosures would actually lead to a better understanding of the data handling and decision making processes.

The public's legitimate concerns and lack of understanding about algorithm-driven processing operations should be addressed by other means. For example, individuals could be provided with meaningful information and reassurances about the safeguards which apply to algorithm-driven processing operations. Organisations can also develop and apply strong accountability frameworks. Companies can also bake in adequate safeguards and controls in cases of algorithm-driven data processing operations. Finally, companies can also develop simple and seamless ways in which individuals can easily exercise their rights of access, correction and redress, where appropriate;

²⁰ See Ilana Westerman and Gabriela Aschenberger, "Brick-and-Mortar Retail: The Design Challenges of Communicating Consumer Data Collection" (23 July 2013) <https://iapp.org/news/a/brick-and-mortar-retail-the-design-challenges-of-communicating-consumer-dat/> Timothy Morey, Theodore Forbath, Allison Schoop, "Customer Data: Designing for Transparency and Trust" HBR (May 2015) <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>

How:

The most **effective ways** in which organisations can provide user centric transparency and meaningful information about their data practices to individuals in the new landscape where there is a shift from traditional and layered transparency notices to new forms of contextual and embedded transparency measures and tools; and



When:

The **timings of transparency communications and measures**. Currently, many organisations provide individuals with information about their data practices at the time of first contact or transaction - the “tick-box moment”. Most individuals do not have the option to make an informed decision about whether or not to share their personal data with companies at that point in time. For instance, some customers may also feel pressurised in accepting the data practices of the company at the tick-box moment given that many companies bundle their general terms and condition with their privacy notices. One possible solution would be to deliver transparency by using several transparency measures at various key times before and during data collection, but also importantly during the lifecycle of data use. Transparency tools should be designed so that they are permanent tools which are available to individuals at all times.

7. Data transparency and organisations: Business goals, data privacy tools and framing the value exchange

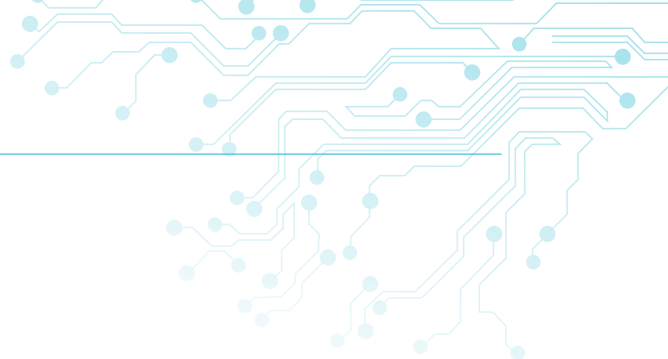
Organisations need to develop and implement **innovative, user-centric transparency tools and approaches** for several reasons, including generating and maintaining trust in the digital economy as well as building and sustaining customer relationships. Companies that succeed in this regard will benefit from more engaged customers, customers who trust their data processing operations and practices as well as customers who are more comfortable with sharing their data.

Such organisations will be able to make the most of their data assets and realise the full potential of the data-driven innovation whilst protecting the fundamental rights and freedoms of their customers. In the long run, this will enable social and economic growth.

Other than including behavioural economists, social scientists and psychologists to understand and develop effective approaches to user-centric transparency, **data-driven organisations** can make four additional contributions to data transparency:



All organisations, and especially those with data-driven business models, should consider **user-centric transparency as a business goal and a business challenge**. Data transparency should not be an issue which is exclusively addressed by the legal teams, but should be a strategic business goal that is shared much more widely across the organisation. This will enable companies to align their processing operations and practices with their business strategy, policies, legal and social obligations. Equally, as a multidisciplinary business challenge, transparency will have to be addressed, designed and delivered by cross-functional and multi-skilled teams in an organisation.



Data-driven companies should pioneer the development of **technological tools and features** that will deliver real transparency to individuals and enable them to fully understand and manage how their data is handled by such organisations. These tools should be designed and built to respond to the specific sectorial, commercial and data processing characteristics of the organisation. An important challenge is how such tools would work across complex data ecosystem. In many data-driven contexts, such as machine-learning, smart mobile devices and the Internet of Things, there is often no direct relationship or interaction between the end-users and the organisations that use their data. Yet, such companies will still need to deliver effective transparency, become aware and respect the data preferences of the end-users.

Overall, all organisations, including those developing technologies and systems, will need to keep ahead of the curve by continually developing transparency approaches, tools and practices which respond to technological advances and the end-users' needs. They will need to seek solutions that embed transparency as a part of the technology, user experience, service or a product, rather than add it as an afterthought. Embracing privacy by design will ensure that the essential component of privacy protection and digital trust – transparency – is addressed and baked into the technology, products and services early on.

Data-driven organisations must become more fluent at explaining the **value exchange** between them and their customers in order to build loyalty and digital confidence. In part, this means that companies should be able to clearly and simply articulate the benefits of personal data processing to the individuals and society. For instance, data-driven tools tell farmers when to optimally plant crops, provide medical information to front-line health practitioners in remote settings, manage people and traffic flows, contain the spread of infection and reduce their pollution levels.²¹

Organisations will also have to explain to and reassure their customers about their own data practices and the safeguards that they deploy to protect customers' data and privacy. **Organisational responsibility and accountability** remain vital foundations which companies can use to drive trust by adopting new approaches to data transparency.



²¹ See <http://dynamicinsights.telefonica.com/2013/10/30/big-data-and-social-good-nuria-oliver/>

8. Conclusion

The Roundtable discussions have emphasised that **traditional approaches** to transparency which focus only on legal requirements do not empower individuals in the sense of providing them with meaningful information about how and why companies use their data as well as user-friendly data control tools.

In recent times, reliance on legal transparency delivered through lengthy, complex and highly legalistic privacy notices and policies that are often not read or understood by individuals, rather than user-centric transparency, has impacted negatively on digital confidence, the participation of individuals in the data economy and economic growth.

Roundtable participants agreed that **user-centric transparency** can often be problematic in various cases such as when there is no direct relationship between the companies and end-users.

Roundtable participants also agreed that in the digital age, data transparency is no longer simply a legal problem but rather a **multi-stakeholder challenge** which can only be resolved by involving a broader range of actors.

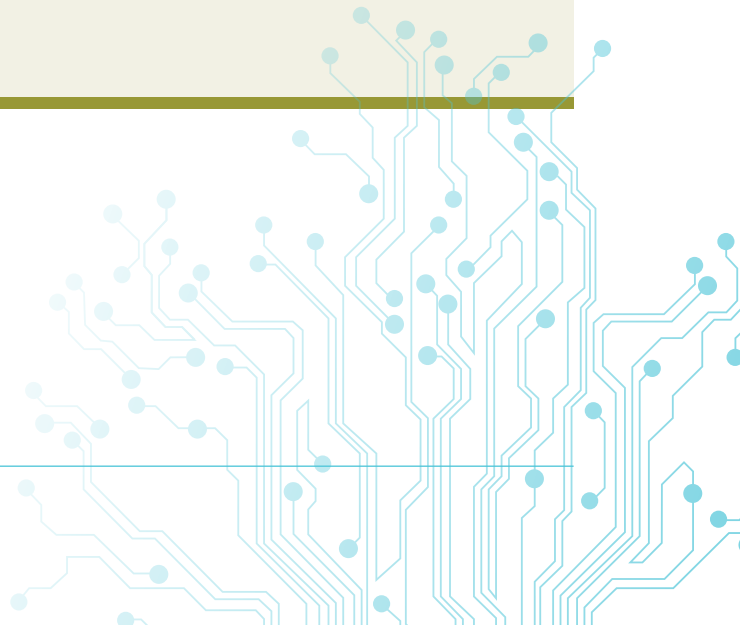
Organisations still have a pivotal role in driving trust and digital confidence. In the digital world this has become an important strategic issue. Digital and data-centric organisations must challenge themselves to deploy context-appropriate user-centric transparency tools and approaches and to better explain the value exchange to customers. This will boost trust in digital services and allow people to fully participate and benefit from digital life.



DPAs and other regulators have significant roles to play in fostering new data transparency tools and approaches. They should be “smart regulators”, selectively use their stronger enforcement powers, promote compliance through guidance, dialogue and collaboration, highlight “best practices” and incentivise new approaches to data transparency.

Individuals must be educated about the data practices of companies, ways in which they can use to control and manage their data and the benefits of personal data processing.

Finally, data-driven and digital organisations should engage more with **behavioural economists, social scientists, psychologists and user experience specialists** who can enable them to better understand the most effective types and forms of transparency and user control.



Appendix

Roundtable Participants

Vivienne Artz	Citi
Nina Barakzai	Sky
Bojana Bellamy	Centre for Information Policy Leadership
Emma Butler	RELX Group
Nathan Coffey	JPMorgan Chase
Sinead Connolly	Centre for Information Policy Leadership
Tim Cooper	Accenture
Paul Copping	Digital Greenwich
Stephen Deadman	Facebook
Belinda Doshi	Pearson Group
Jarmo Eskelinen	Future Cities Catapult
John Foster	Telefónica
Stefano Fratta	Telefónica
Jana Gary	Telefónica
Fedelma Good	Barclays
Krishna Gummadi	Max Planck Institute
Adrienne Harrington	Department of the Taoiseach, Ireland
Alex Hazell	Axiom Corporation
Shirin Huber	UPS
Kara Iselin	The Net-A-Porter Group
Jacob Kohnstamm	Dutch Data Protection Authority
Nikolaos Laoutaris	Telefónica
Caroline Louveaux	MasterCard
Rosie McGlynn	Energy UK
Jed Mole	Axiom Corporation
Rachel Mulligan	eBay
Kirsten Mycroft	Lloyds Banking
Mikko Niva	Vodafone

Chris Payne	The LEGO Group
Dragan Pendić	Guardtime
Ross Phillipson	Procter & Gamble
Julia Porter	Guardian News & Media
Richard Poston	Telefónica
Jonny Shipp	Telefónica
David Skelton	Google
Ian Small	Telefónica
Josephine Smart	BBC
Gavin Starks	Open Data Institute
Nick Stringer	European Interactive Digital Advertising Alliance & NJ Stringer Ltd
Richard Thomas	Centre for Information Policy Leadership
Louise Thorpe	American Express
Monika Tomczak-Górlkowska	Shell International Limited
Claudia Trivilino	Application Developers Alliance
Asma Vranaki	Centre for Information Policy Leadership
Wojciech Wiewiórowski	European Data Protection Supervisor
Melanie Wiseman	The Society of Motor Manufacturers and Traders Ltd
Boris Wojtan	GSMA
Chad Wollen	Smartpipe Solutions
Steve Wood	UK Information Commissioner's Office
Helen Woollett	Barclays
Steve Wright	John Lewis
Kimon Zorbas	Nielsen

Telefonica

Published in October 2016.
Telefónica S.A. Ronda de la Comunicación s/n, 28050 Madrid, España.
www.telefonica.com