Citi GPS

ePRIVACY AND DATA PROTECTION

Who Watches the Watchers? – How Regulation Could Alter The Path of Innovation

Citi GPS: Global Perspectives & Solutions

March 2017

Authors

Thomas A Singlehurst, CFA
Head of European Media Research Team

+44-20-7986-4051 | thomas.singlhurst@citi.com

Catherine T O'Neill
European Media Analyst

+44-20-7986-8053 | catherine.oneill@citi.com

Mark Kelley
U.S. SMID Internet Analyst

+1-212-816-2638 | mark.kelley@citi.com

Mark May
U.S. Internet Analyst

+1-212-816-5564 | mark.may@citi.com

Benjamin Nabarro
Global Thematic Research

+44-20-7986-2056 | benjamin.nabarro@citi.com

Walter H Pritchard, CFA
U.S. Software Analyst

+1-415-951-1170 | walter.h.pritchard@citi.com

Ashwin Shirvaikar, CFA
U.S. Payments, Processors & IT Services Analyst

+1-212-816-0822 | ashwin.shirvaikar@citi.com

Dalibor Vavruska
Global Head of Digital Connectivity Strategy & CEEMEA Telecom Research

+44-20-7986-4276 | dalibor.vavruska@citi.com

Expert Commentators

Vivienne Artz
Managing Director,
Head of International Privacy for IP & O&T Law
Citi

Andrew Brem
Chief Digital Officer
Aviva

John Bowman
Senior Principal
Promontory Financial Group, an IBM Company

Andrew McClelland
Head of Industry Insight
IMRG

Simon McDougall
Managing Director
Promontory Financial Group, an IBM Company

Mikko Niva
Group Privacy Officer
Vodafone

Contributors:

Ronit Ghose, CFA
Josh Levin, CFA
Michael Rollins, CFA
Jim Suva, CPA
Jason Bazinet
Michael Goltsman, CFA
Andrew Light
Ian Sealey, CFA
Mark van't Sant
Andrius Budnikas
Dan Homan
James Oram
Ed Steele

ePRIVACY & DATA PROTECTION

Who Watches the Watchers? – How Regulation Could Alter the Path of Innovation

Mr. McGuire: I just want to say one word to you. Just one word.

Benjamin Braddock: Yes, sir.

Mr. McGuire: Are you listening?

Benjamin Braddock: Yes, I am.

Mr. McGuire: Plastics.

Excerpt from The Graduate, 1967

If The Graduate were to be re-released today it is almost certain that the career advice from Mr. McGuire to the film's main protagonist – recently graduated Benjamin Braddock – would be different. Indeed, we would go one step further and argue that it is almost certain that the one word offered by the 2017 version of Mr. McGuire would be 'data'.

An MIT Sloan Management Review report in 2015 bears this out. Forty-three percent of surveyed companies indicated that a lack of appropriate analytical skills is a key challenge.

And why is this? It is of course because the opportunity from big data, data analytics, machine learning, artificial intelligence, and the Internet of Things is perceived to be enormous and data scientists are the potential key to unlocking it.

But for data scientists to exist, we must have data. Indeed all of these opportunities rely on continued untrammeled access to significant underlying data sets — an assumption that we think investors can no longer fully take for granted.

In this report we look at how consumers are tracked, and how the data that is collected and analyzed is then used by organizations. We then look at how consumers themselves perceive the topic of privacy and why regulators increasingly feel the need to intervene. Finally we conduct a series of case studies with third-party contributors such as Vodafone, Aviva, and even Citi to assess the challenges associated with adapting to the new landscape.

The conclusions are quite stark. Focus on privacy and data protection is on the rise and forthcoming changes to regulation in the European Union (EU), to be implemented in 2018, will fundamentally alter the risk/reward of using data and with it, alter the perception of the long-term opportunity from data.

It's important to say that this does not necessarily unwind the longer-term upside from big data, data analytics, artificial intelligence, and machine learning. But we do think the path will be muddied by new regulation and that from a corporate perspective, this will require a systemic change of approach with respect to ePrivacy and data protection. And this is not, for the moment, properly understood or appreciated by many corporates or investors.

The Opportunity from Data is Huge, But What Are the Costs?

We generate an unimaginable and increasing amount of data…which potentially creates a big opportunity. But have the potential challenges to realizing the opportunity from big data been overlooked?

90%
of the data in the world today has been created in the last 2 years

Source: IBM

Every 2 days we create as much data as we did from the start of time until **2013**

Source: Eric Schmidt

22%
growth of IP traffic is forecast between 2015-2020 CAGR)

Source: Cisco

UK businesses are estimated to realize a benefit of
£240 billion
from big data between 2015-20

Source: CEBR

Adoption of digital operating models could potentially create
$1.2 trillion
in social value in consumer industries

Source: World Economic Forum

Consumers are increasingly being tracked online…

Mobile tracking generates approx. **100 data points** per user

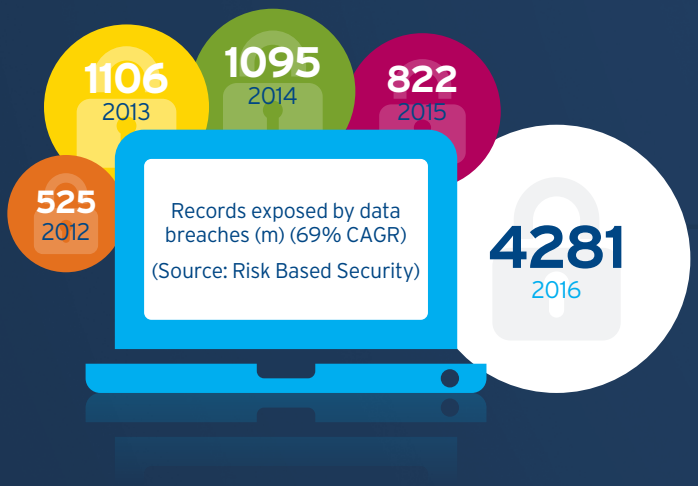
185% increase in Government requests to Google for user info and info removal over the past 5 years

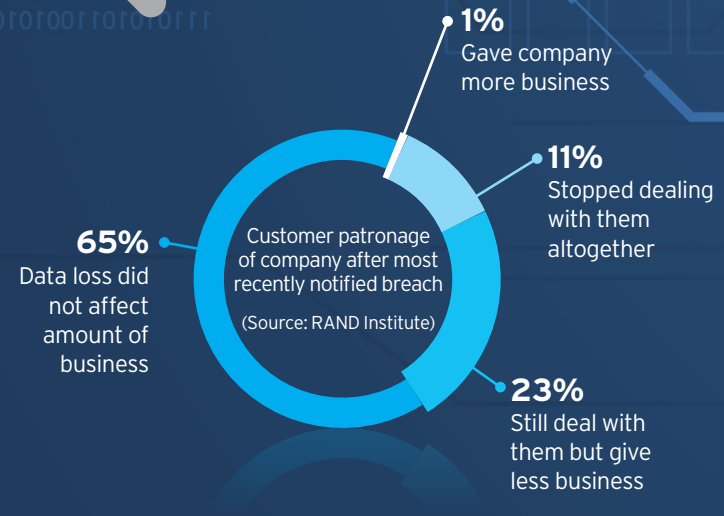
79% of cookies on media sites are third party cookies

Acxiom has on average approx. **1500 pieces** of data on about 96% of Americans

Source: PubMatic, Google, Article 29 Working Party, Eli Pariser 2011.

…But aren't changing their habits in the face of increasing data breaches and despite claiming to care about privacy.





Regulators are increasingly stepping in to protect consumers…the EU's GDPR is seen as the most stringent data protection regulation yet

>100
countries enacting data protection regulation since 1972

05/2018
EU's General Data Protection Regulation (GDPR) implementation date

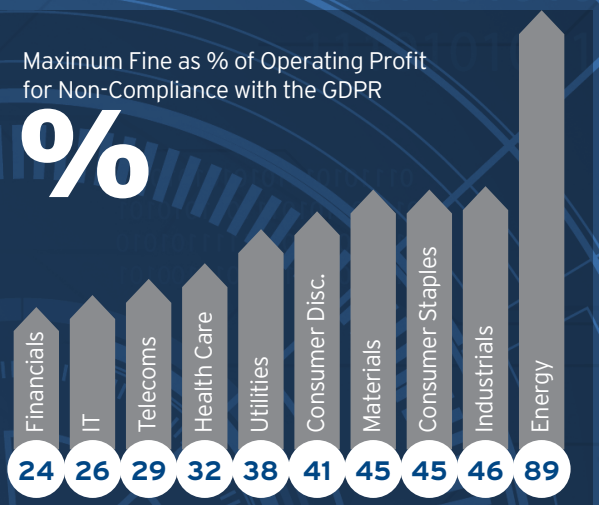
GDPR brings a risk of fines (4% of global turnover for non-compliance), which could wipe out an industry's operating profit upwards of

25%

Source: Datastream, Citi Research

Maximum Fine as % of Operating Profit for Non-Compliance with the GDPR

%



*Financials as % of profit before tax

What are the experts saying about GDPR?

"GDPR has taken the issue of data protection and e-privacy from somewhere in the bottom 20 of issues that corporates worry about and spend time on to somewhere in the top 10."

Vivienne Artz, Citi.

"The GDPR represents change for everyone, even if they have a good framework in place. If they don't have anything in place, then there's considerably more effort required."

Simon McDougall and John Bowman, Promontory Financial Group, an IBM company.

"The majority of the change needs to be cultural, rather than box ticking. Everyone needs to understand that this is important."

Andrew McLelland, IMRG.

"The difference is that before the GDPR, it was principally a question of regulation and company values; post-GPDR there are obviously more acute financial penalties associated with non-compliance."

Mikko Niva, Vodafone.

Contents

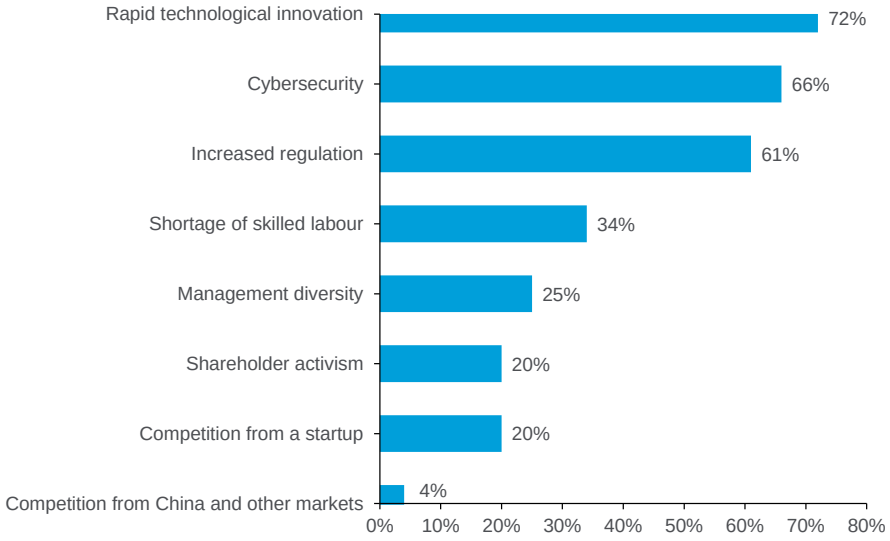
Executive Summary 7
15 Questions for Companies 11
How Consumers Are Tracked & How Data Is Used 13
Technological Challenges to Realizing the Opportunity from Data 34
Consumer Attitudes to Privacy 40
ePrivacy and Data Protection Regulation: A History 51
Deep Dive into the General Data Protection Regulation (GDPR) 54
ePrivacy Directive 2.0: Potentially as Game Changing as the GDPR 73
International Data Protection Regimes 80
Expert Views 89
A Conversation with Vivienne Artz 90
A Conversation with Mikko Niva 96
A Conversation with Andrew Brem 99
A Conversation with Andrew McClelland 102
A Conversation with Simon McDougall (MD) & John Bowman (Senior Principal) 107
Implications for Industries, Corporates & Investors 111
Implications for Industries 112
Key Issues for Corporates & Investors 127
Glossary 130

Executive Summary

The Opportunity From Data Is Huge, But What Are The Costs?

For virtually every consumer, corporation and government the opportunity from data and analytics is increasingly recognized, something borne out by a survey of Fortune 500 CEOs carried out by Fortune magazine in 2015. Asked 'What is your greatest challenge?' 72% identified 'rapid technological innovation' as their major priority.

Figure 1. Greatest Challenge According to CEOs



Source: Fortune

For the most part, however, commentary on this topic has been framed only in terms of the opportunities greater usage of big data and analytics might bring. As we discuss below, McKinsey has estimated that the use of big data in the U.S. healthcare system could create $300 billion of value every year. Not to be outbid, the World Economic Forum has separately estimated that greater adoption of digital operating models could create as much as $1.2 trillion in social value in consumer industries.

The question we examine in this report is the extent to which commentators – and therefore investors and other stakeholders – have potentially overlooked some of the challenges associated with successfully realizing this opportunity. The key questions we ask are:

- Has the development of technology, and the realization of how data can be used, led to an imbalance of power tilted in favor of corporates vs. individuals?
- How does the rise of hacking impact corporates' approaches to privacy and data protection?
- What do consumers think about privacy and how is their behavior impacting the way regulators approach the topic?

- What does the regulatory landscape look like at present and how could this change?
- What are the challenges for corporates in ensuring compliance with new regulatory standards when they come into force in the near future?

Roadmap to this Report

We break this report into 10 main sections. Going through them in turn:

- In the first section we look at **how consumers are tracked and how data is used**. The main conclusion is that pretty much everything we do online is tracked in some way, shape, or form and that the modes of tracking have significantly advanced since the days of the simple cookie. Of course, in many cases enhanced tracking has not only been a factor driving better outcomes for consumers but also part of a recognized bargain between consumers and organizations, but this is not universally the case.
- In the second section we look at the **technical challenges associated with data collection/analytics** and conclude that in the rush to exploit the data opportunity not all companies have paid enough attention to or fully factored in sufficient safeguards for data privacy/cyber security.
- The third section looks at **consumer attitudes to privacy** and highlights the paradoxical behavior of consumers across the world who simultaneously profess to be concerned about privacy issues but also appear not to significantly moderate their behavior accordingly. Internet-connected devices have become increasingly embedded in our everyday usage, especially for the younger generations, which is likely to be a factor behind this inconsistency. With the perception of limited consequences for poor performance now firmly established, this has engendered an approach from companies that use data that is largely (a) reactive and (b) cosmetic. Regulators, meanwhile, appear to have taken the consumers' stance as a signal that an external agent will need to hold companies/organizations that use personal data to account.
- In the fourth and fifth sections we look at the **history of data protection regulation** and **the implementation of the European Union General Data Protection Regulation (GDPR)**, which will become legally binding in all EU member states on May 25, 2018. We conclude that while the number of data protection standards has been steadily rising across the world since the 1970s, the GDPR is by some measure the most stringent regulation yet put in place, with significant enhancements/changes in terms of the (a) scope of the regulation (to whom it applies); (b) the required changes to regulatory practice (both in terms of consents and rights for consumers; (c) the sanctions for non-compliance; and (d) the impact on international data transfers.
- In the sixth and seventh sections we look at **how the GDPR will co-exist with other EU level regulations/directives** as well as other **international regimes**. On the former, we note a real risk, which is that combined with the proposed ePrivacy Regulation (draft published in January 2017), constraints on organizations hoping to use personal data of EU citizens could actually end up even more stringent. This stands in sharp contrast with international data regimes, in particular in Asia Pacific, where a more laissez-faire, principles-based approach has taken root.

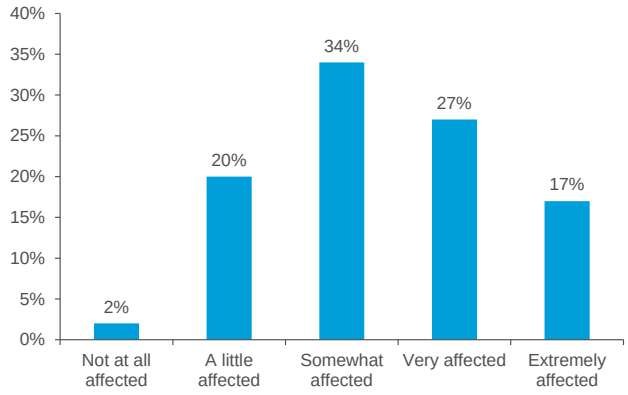
- In the eighth section we attempt to bring many of these topics to life via a number of **in-depth interviews with experts in the privacy space across a range of industries**. This section includes conversations with senior executives at Citi, Vodafone, and Aviva as well as industry consortia (the Interactive Media & Retail Group (IMRG) retail industry body in the U.K.) and consultants (Promontory Financial Group, an IBM Company).
- In the ninth and tenth sections we include **commentary from our Citi Research colleagues on the potential impact on their sectors**. We follow this up by considering a list of key issues for corporates and investors to consider ahead of implementation of the GDPR (and potentially the revised ePrivacy Regulation) in the next 12 months.

Headline Conclusions

We reach five main conclusions on the back of this work:

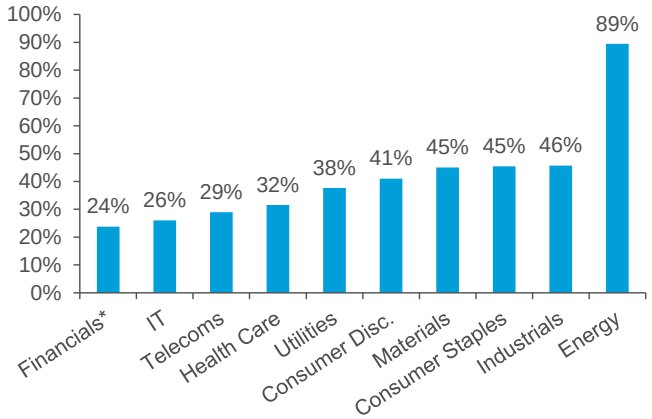
- Although the opportunities from data are significant, **a lot of commentators have underplayed and potentially underestimated the challenges associated with ensuring ePrivacy** and adequately protecting personal data.
- **The implementation of the GDPR in May 2018 represents one of the most significant events in ePrivacy/data protection regulatory history.** The regulation is a game changer in terms of not only its scope and ambition, but also the significant penalties for non-compliance. According to a survey by the DMA 98% of companies expect to be affected by the GDPR to some degree. The fine for non-compliance will be up to 4% of global annual turnover (sales).

Figure 2. To What Extent Do You Think Your Organization Will Be Affected By the GDPR?



Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2'. Survey run Sept-Dec 2016

Figure 3. Impact on Operating Profit From Maximum Fine (MSCI Global Sectors)



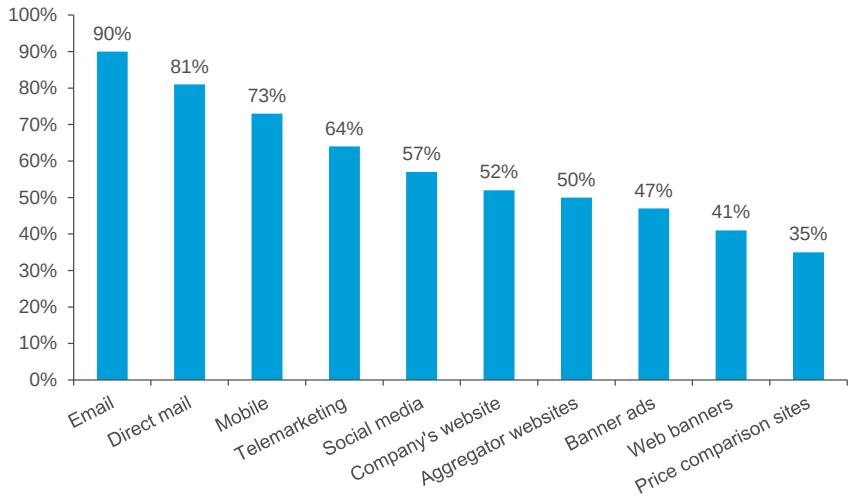
*Financials is based on a percentage of profit before tax (PBT)

Source: DataStream, Citi Research Estimates

- **Changes in technology are disruptive.** In the past, some established business models have been challenged, and almost entirely sidelined, due to advances in technology and the ability to utilize data e.g. online search led to the decline of the Yellow Pages. The aim of the evolving data protection regulation in Europe is to shift power back to the consumers, and ultimately increase transparency and trust in how companies use consumer data. Best case, consumers become more trusting if they are better educated on how data is used. The outcome being that the quality of the data corporates are given access to improves, and data as an

asset increases in value. However, there is a risk that in attempting to achieve its aim, Europe's approach is too heavy-handed, resulting in a vast reduction in data being shared with companies, particularly in relation to third-party tracking. The advertising technology (adtech) space and online advertising-funded media rely on the ability to track consumers using third-party trackers (to place value on an ad and for measurement).

Figure 4. What Channels Do You Think Will Be Affected By the GDPR?



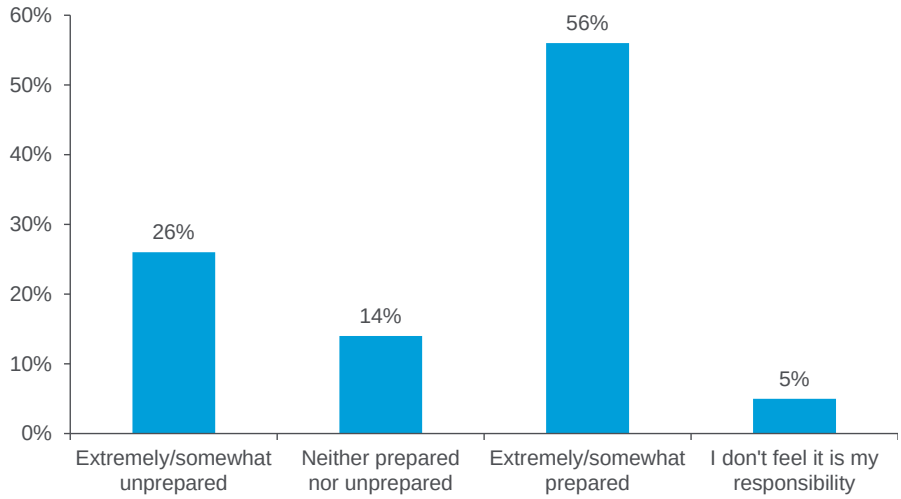
Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2'. Survey run Sept-Dec 2016

- **There will be winners from the change, but mainly losers.** There is a whole ecosystem of companies that have developed on the back of the privacy concerns and/or tightening regulatory requirements. These range from expertise and technology that helps companies to monitor and audit on-site trackers and vendors, to consumer focused technology and services that enable consumers to manage their identity (blockchain technology may come into play here). Software security and cyber security technologies are likely to benefit from the growing need to secure personal data. For most companies it is more of a challenge in terms of compliance. There are two key points:
  - Ironically, the very companies that the GDPR was potentially designed to constrain will probably end up being least affected. Of course there will be increased regulatory costs associated with compliance, but those larger companies that already have consumer trust and the necessary resources to remain compliant with much stricter and more complex EU rules, will likely be less disrupted than smaller enterprises.
  - For all companies, it will likely require a cultural change in relation to how personal data is collected, stored and used.
- **The asymmetric approach toward regulation between different regions** (contrast the dirigiste approach of the EU vs. the more laissez-faire, principles-based approach of both the U.S. and Asia Pacific) could lead to a similar level of asymmetry in terms of access to investment and 21st century consumer services – artificial intelligence, machine learning, the Internet of Things. In other words a world of digital-haves and digital-have-nots where, ironically, 20th century notions of borders and citizenship are the primary factors determining where people sit.

15 Questions for Companies

With little over a year to go, it is surprising that readiness for the data protection regulatory change coming in Europe in 2018 is not higher.

Figure 5. How Prepared Is Your Company for These (GDPR) Changes?



Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2' Survey conducted Sept-Dec 2016

Given the rising importance of ePrivacy and data protection, and the associated risk from regulatory changes, we have prepared a list of 15 questions investors should ask companies to gauge preparedness for the new data protection landscape:

1. Are you aware of the EU General Data Protection Regulation (GDPR) and the proposals associated with the first draft of the proposed ePrivacy Regulation?

2. If so, are you aware of the requirements of the new regulations and of the sanctions in the event of non-compliance?

3. What kind of framework, security, and training do you have in place in relation to data protection? Do you have an official privacy/data protection team in place? If so, does your Chief Privacy Officer report to the board/senior management? What is his/her name?

4. How reliant is your business on the use of personal data? How central would you say use of data/data analytics is to your business model?

5. How do you monitor what data you hold? What consumer data do you currently hold and in what format (physical/electronic)? Do you know where the personal data you hold is stored (especially if it is in the cloud) and who has access to it?

6. Do you have an accurate picture of what consents you have for your existing data resources? How will you go about obtaining necessary consents post implementation of the GDPR? To what extent are you currently able to inform customers of what data you hold and erase it on request? How do you think about the balance between utilizing data while maintaining consumer trust longer term?

7. Does your company sell or share data with third parties in any way? Do you process all consumer data yourself or do you hand off data to third-party processors?

8. If the latter, to what extent are you comfortable that contracts with outsourcing partners (including providers of cloud services) have sufficient provisions for ePrivacy and data protection and what resources are you putting in place to make sure commitments are met?

9. To what extent is data circulated within your institution, i.e., between business lines in the same geography and/or between different geographic regions?

10. To what extent are there competing regulations (e.g. anti-money laundering screening for financial institutions) that potentially come into conflict with new ePrivacy/data protection regulations?

11. With all of this in mind, what are you doing to ensure that you are going to be compliant with the GDPR by May 2018? Are there any areas where you see implementation challenges?

12. The regulator appears to be pushing for a cultural change in the approach to data protection – how do you go about instituting that cultural change? Does there need to be a change in incentive structures within the organization?

13. Financially, how do you think about the costs associated with data protection and privacy – do you expect a material change? Are there any financial benefits from the requirements of the GDPR?

14. Does the idea of more stringent rules on data protection and ePrivacy (and significant fines for non-compliance) make you think differently about the importance of data protection to your organization? Will any of your operations (that handle data) have to fundamentally change how they operate in order to comply with the upcoming regulation, or be materially impacted by the regulation?

15. Is there anything you use data for currently that you will have to stop doing? Any areas of business/product/service development that appear unworkable in light of the regulation? Does the GDPR make you reconsider what services/products you offer within the EU (relative to other regions/geographies)?

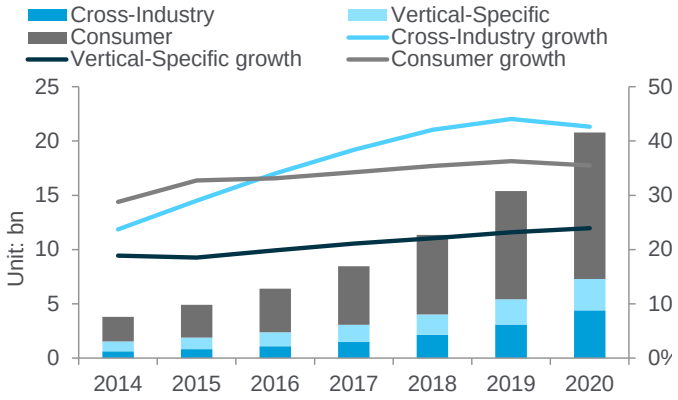
How Consumers Are Tracked & How Data Is Used

Assessing the Data Opportunity

Much has been written about the rise of data, the transformational impact it has had, and the value it creates for society, the economy, corporates, and individuals.

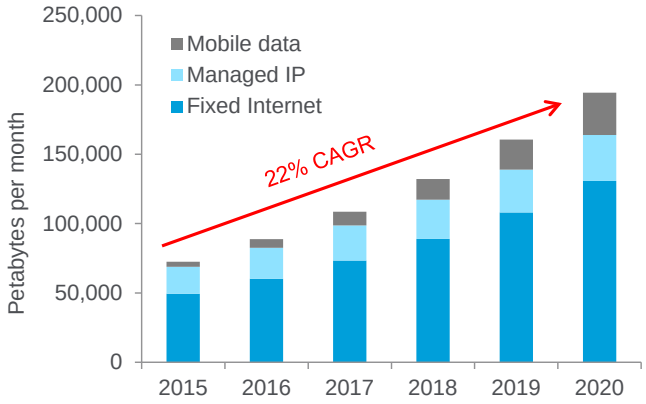
Technological advancements, falling technology and storage costs, increasing connectivity, and a rise in the number of devices have all contributed to ever increasing amounts of data being generated. It will continue with the rise of the Internet of Things and connectivity in emerging markets.

Figure 6. IoT End Point Installed Base by Category, 2013-20



Source: Gartner

Figure 7. Global IP Traffic Forecast by Connection Network



Source: Cisco VNI Global IP Traffic Forecast, 2015-2020

To get a handle on the amount data we generate it is worth considering the following:

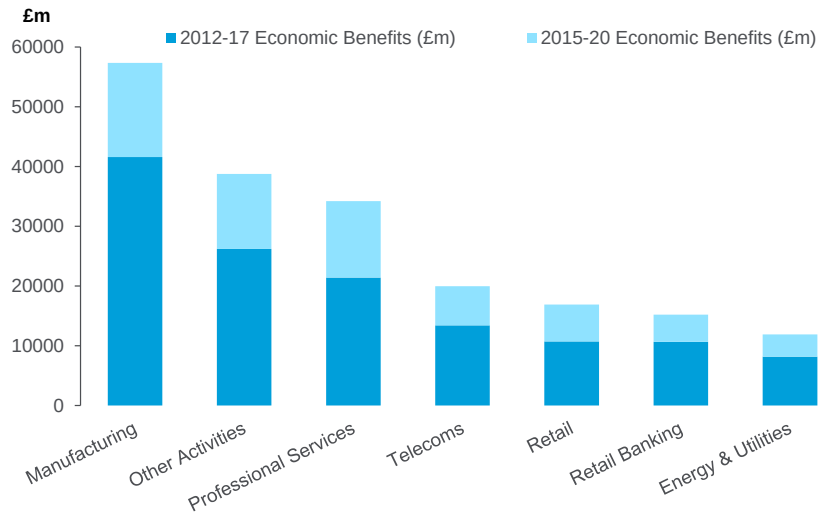
- IBM has previously said that 90% of the data in the world today has been created in the last two years;
- Every two days we create as much data as we did from the beginning of time until 2003;
- There are over four million Facebook posts and over 300 hours of new video uploaded to Facebook every minute;
- Six billion hours of video are uploaded to YouTube every month.

Moving beyond simply the volume of data, let's also consider the value that could potentially be generated by data (and the application of big data analytics) via reduced risk and uncertainty, and increases in efficiency and productivity:

- McKinsey states that the U.S. healthcare industry alone could generate more than $300 billion in value every year through big data; data from connected smart devices/wearables could accelerate the treatment (and possible cure) of diseases;
- Maximizing analytics of a retailer could increase its operating margin by more than 60%, according to McKinsey;

- The World Economic Forum predicts that the adoption of a digital operating model could be worth as much as $1.2 trillion in social value in consumer industries alone;
- The World Economic Forum estimates 5% of all factories are to be Smart by 2025, with cost savings of £70 billion;
- Accenture estimates that EBITDA/Employee is 51% greater for platforms than for market incumbents.
- An MIT Study (Brynjolfsson et al. 2011) of 180 large public companies concluded that businesses that emphasize data-driven decision making typically saw 5-6% higher output and productivity than would be expected;
- The Centre for Economic & Business Research (CEBR) estimates that in the U.K., the economic benefit of big data 2015-20 could equate to £241 billion.

Figure 8. Top 7 Sectors to Potentially Benefit From Big Data in the U.K.



Source: CEBR

Monetization of Data Has Driven the Evolution of New Business Models

The rise of data is already evident in the market capitalization of companies today versus 10 years ago. Looking back 10 years, there were only three companies in the list of top 10 firms by market capitalization that are still in the top 10 now, and only one of them, Microsoft, is a technology company. Half of the current top 10 are technology / Internet companies, and at the core of their operations has been the ability to successfully utilize and monetize data at scale.

Figure 9. Top 10 Global Companies by Market Capitalization, 2017 vs. 2006

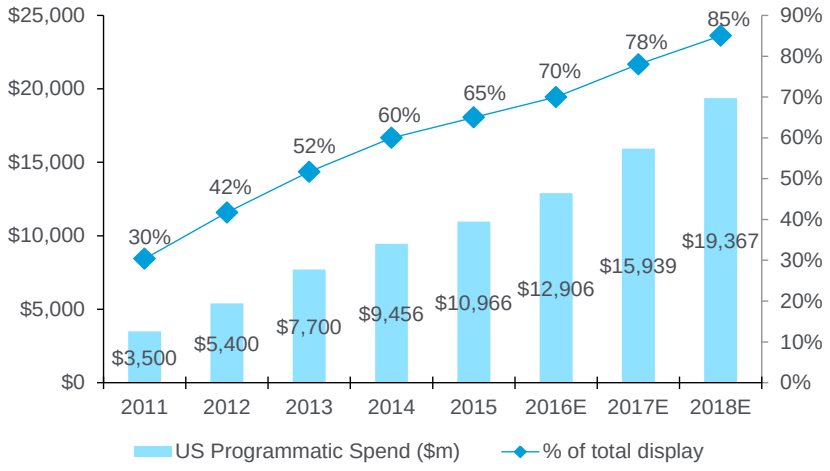
Largest Companies 2017*	Largest Companies 2006
Apple	ExxonMobil
Alphabet	General Electric
Microsoft	Gazprom
Berkshire Hathaway	Microsoft
Amazon	Citigroup
Facebook	Bank of America
ExxonMobil	Royal Dutch Shell
Johnson & Johnson	BP
JPMorgan Chase & Co.	PetroChina
Wells Fargo	HSBC

Source: DataStream (based on prices as of 23 January 2017)

The likes of Alphabet (Google), Facebook and Amazon are capital and asset light, and their biggest asset is arguably the data they have garnered from consumers, and successfully monetized. In turn, this has often led to, and will continue to lead to, disruption across industries.

Technology and data have enabled new models to emerge within existing industries. Within the world of advertising, the rise of programmatic buying is an interesting example. Programmatic media buying represents the use of data and technology to better inform media buying decisions and allows decisions to be taken in real time. At the heart of this is the ability to track consumers online and overlay demographic and behavioral attributes so advertising can be bought on a targeted basis, rather than being bought based on the site genre, thereby reducing wastage (in this instance, advertising to individuals who use the sites but don't fit the specific target group). In the past five years programmatic buying has moved from a 30% share of digital display advertising to 70% in the U.S.

Figure 10. U.S. Programmatic Display Advertising Spend ($m) & Share of Display Advertising



Source: Magna, IAB, PWC, Citi Research estimates

This is just one example. There are many more across industries.

We, as consumers, already see the benefits from technology advancements and our data being utilized, mostly in the form of convenience.

In many developed markets, every day activities can now be conducted without leaving our homes, e.g., shopping, banking, on demand video viewing. We also benefit from improvements in monitoring within the area of health and wellbeing, and from more personalized recommendations of content to consume and products to purchase.

And this is only the beginning. In the future, artificial intelligence and machine learning – both heavily reliant on data for their insights – will increasingly lead to tailoring of services, pricing and products.

However, increasing personalization relies on us (the consumers) handing over access to copious amounts of data, some of it personal. So, what is personal data? What are the means by which companies get their hands on our data?

What is Personal Data?

Personal data tends to be relatively broadly defined and is technology neutral. It often refers to data that can be used to identify an individual, directly or indirectly.

European Data Protection Directive (1995): *Personal data shall mean any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity*

Types of data which are directly personal are:

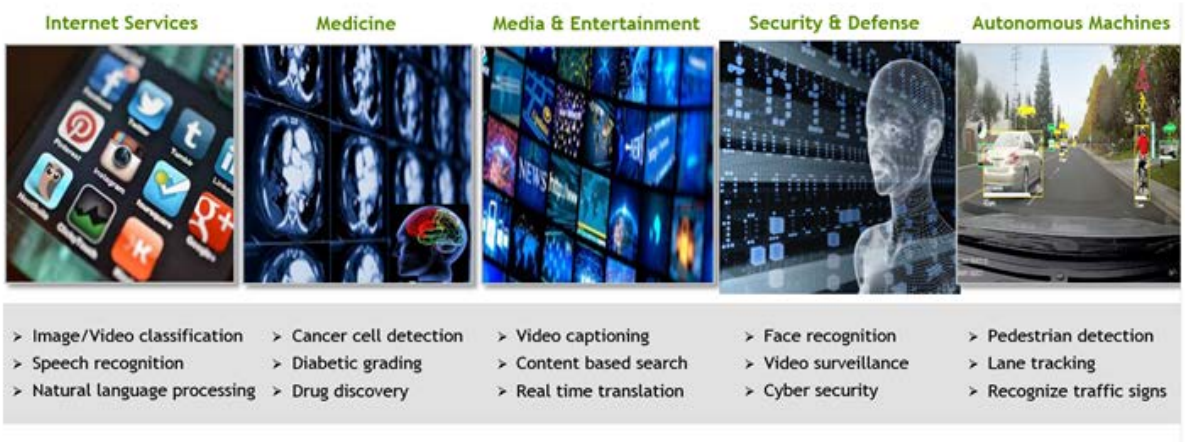
- Name
- Email address
- Home address
- Phone number
- Work history

Data which may be deemed indirectly personal could be a description of someone that still enables identification, e.g., the lead European Media Research Analyst at Citi.

Data classified as sensitive personal data, such as race/ethnic origin, political views, religious beliefs, sexual orientation, and health conditions, are subject to more stringent regulatory requirements.

In some cases consumers voluntarily provide information, e.g., when registering for a service, requesting price quotes etc. In other cases data is observed, e.g., location data, search history, online purchases, or inferred, e.g., credit scores, consumer profile. The latter two are expected to grow fastest as the Internet of Things will generate a significant amount of observed data, and artificial intelligence and machine learning will drive inferred data. The consumer also has less control over the latter two forms of data.

Figure 11. Key Uses of Artificial Intelligence



Source: NVIDIA

Pseudonymized data: A process by which commonly recognisable identifiers, such as names and addresses, are replaced with artificial pseudonyms, such as ID numbers. Here, in contrast to anonymization, the data could, hypothetically, be manipulated to identify individuals, but for most this is impossible. This process can, however, be reversed.

Data on its own may not stand out as being personal data, but when combined with other data it may be deemed personal if it identifies information about an individual. More recently the EU and the U.S. Federal Trade Commission (FTC) have broadened out the definition of personal data. The GDPR is clear that online identifiers and location data are personally identifiable information, and pseudonymized data may count as personal depending on the context. The outgoing Chairwoman of the FTC, Edith Ramirez (24 August 2016), appears to concur, stating "*We now regard data as personally identifiable when it can be reasonably linked to a particular person, computer, or device. In many cases, persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers meet this test.*"

The ability to de-anonymize data has increased due to the numerous ways data can be obtained online. According to Jonathan Mayer, Federal Communications Commission (FCC) chief technologist, '*the idea of personally identifiable information not being identifiable is completely laughable in computer science circles.*" In 2013, researchers[1] published a report in which they analyzed 1.5 million mobile phone users in Belgium over 15 months and found they could identify 95% of them using just four points of reference when information is provided hourly from mobile antennas.

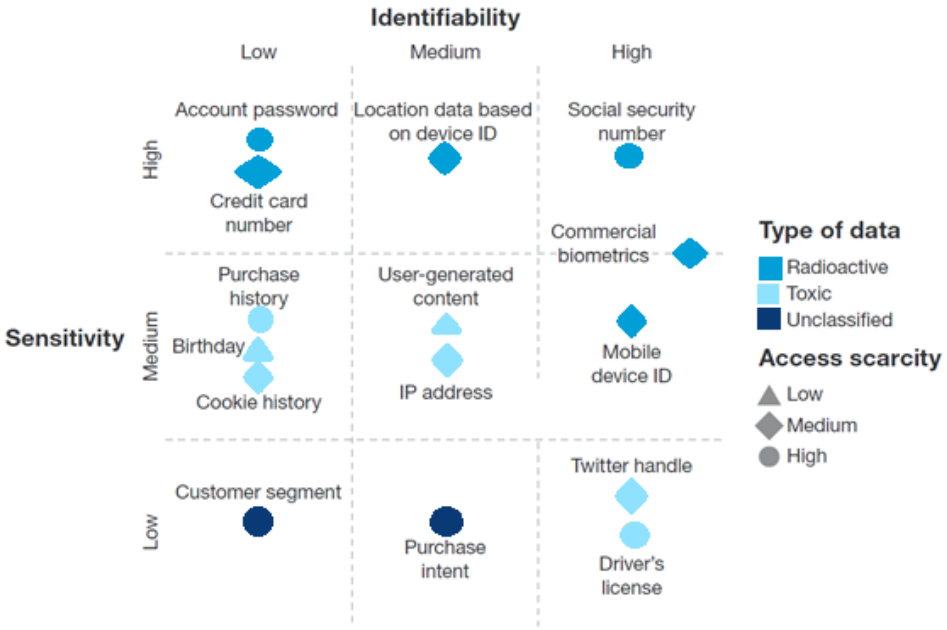
IP address: A numerical value assigned to each device on a network to identify a device and locate it.

As the lines between what may be personal data and what might not be begin to blur, Forrester has created a matrix to help marketers classify data based on risk as it believes marketers have become too liberal in the collection of consumer data. It describes radioactive data as customer data e.g. personally identifiable, which could violate a business agreement if lost, and should be protected aggressively and obtained only with customer consent. Toxic data is data which could harm the customer, cost the company and cause brand damage, and opt out should be used. Unclassified data could be treated as public information with low risk of harm.

What is interesting about this is that there are few data types included as unclassified i.e. low risk of harm. Of the 15 data types 6 data types are considered radioactive and 7 considered toxic (including IP address and cookie history).

[1] Yves-Alexandre de Montjoye, Cesar A. Hidalgo, Michel Verleysen and Vincent D. Blondel. 'Unique in the crowd: The privacy bounds of human mobility', March 2013.

Figure 12. Forrester's Customer Marketing Data Classification Matrix



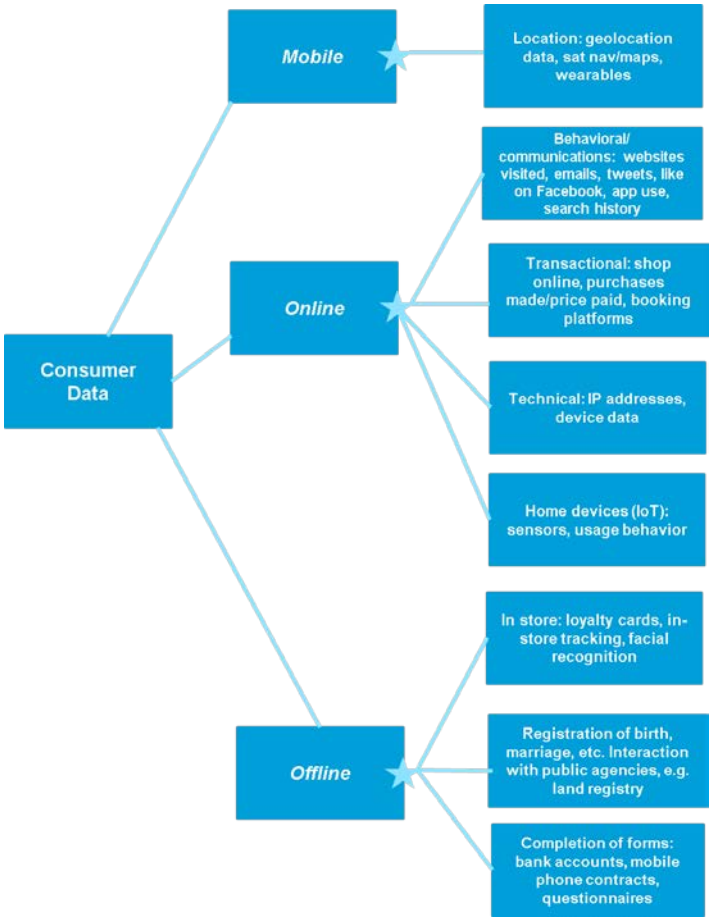
Source: How Dirty Is Your Data?", Forrester Research, Inc., May 3, 2016. https://www.forrester.com/report/How+Dirty+Is+Your+Data/-/E-RES73121#figure2

How Consumers Are Tracked Online

There are many data trails that we leave as consumers, online and offline. This is growing as the use of technology becomes more engrained in everyday life. In Figure 13 below we show some of the ways in which personal data is captured both online and offline.

One of the key points here is that technological advances have resulted in a significant increase in the ways in which we can be tracked online.

Figure 13. Ways Consumer Data is Tracked, Online vs. Offline



Source: Citi Research

Until the mid-1990s, users could only be tracked during a single browser session. Storage-based cookies have since become the most common means of tracking. As the data is stored on a user's computer, the user can delete/clear the cookies and block some cookies. Over the past five years, cache (on the browser's cache) and fingerprinting-based tracking have developed. Fingerprinting does not rely on the storage of the user's computer and can be used regardless of browsing mode.

Below is a list of various online tracking mechanisms. Consumers are generally well informed about the existence of cookies (since the 2009 ePrivacy directive introduced the concept of cookie consent banners), but may be surprised at the numerous other means of online tracking.

Figure 14. Online Tracking Mechanisms

Tracking mechanism	Technologies	Scope
Session-Only		
Session identifiers stored in hidden fields	Web server session	Session ID
Explicit web-form authentication	Web server session	User ID
window.name DOM property	HTML5, JavaScript	Session ID
Storage-based		
HTTP cookies	HTTP headers, JavaScript	Browser instance ID
Flash cookies and Java JNLP PersistenceService	Flash/Java	Operating system instance ID
Flash LocalConnection object	Flash	Operating system instance ID
Silverlight Isloated Storage	Silverlight	Browser instance ID
HTML5 Global, Local, and Session storage	HTML5, JavaScript	Browser instance ID
Web SQL Database and HTML5 IndexedDB	HTML5, JavaScript	Browser instance ID
Internet Explorer userData storage	JavaScript	Browser instance ID
Cache-based		
Web cache		
Embedding identifiers in chached documents	HTML5, JavaScript	Browser instance ID, browsing history
Loading performance tests	Server-side measurements, JavaScript	Browsing history
ETags and Last-Modified headers	HTTP Headers	Browser instance ID
DNS Lookups		
DNS Lookups	JavaScript	Browsing history
Operational Caches		
HTTP 301 redirect cache	HTTP headers	Browser instance ID
HTTP authentication cache	HTTP headers, JavaScript	Browser instance ID
HTTP Strict Transcript Security cache	HTTP headers, JavaScript	Browser instance ID
TLS Session Resumption cache and TLS Session IDs	Web-server session	Browser instance ID
Fingerprinting		
Network and location fingerprinting	IP address, server-based geolocation techniques, HTTP headers, HTML5, JavaScript, Flash, Java	IP address, user's country, city and neighborhood
Device fingerprinting	IP address, TCP headers, HTTP headers, JavaScript, Flash	Device ID, IP address (entire or part), operating system, screen resolution, timezone, list of system fonts, web browser, information about hardware (mouse, keyboard, accelerometer, multitouch capabilities, microphone, camera), TCP timestamps
Operating System instance fingerprinting	JavaScript, Flash, Java, ActiveX	Operating system instance ID, operating system version and architecture, system language, user-specific language, local timezone, local date and time, list of system fonts, color depth, screen dimensions, audio capabvilities, access to the user's camera, microphond, and hard disk, printing support, hard disk identifiers, TCP/IP parameters, computer name, Internet Explorer product ID, Windows Digital Product ID, installed system drivers, operating system instance ID stored by a Java privileged applet
Brower version fingerprinting	HTML5, JavaScript, CSS	Detailed browser version
Browser instance fingerprinting using canvas	HTML5, JavaScript	Browser instance ID
Browser instance fingerprinting using web browsing history	Servere-side measurements, HTTP headers, JavaScript	Browser instance ID, browsing history
Other browser instance fingerprinting methods	HTTP headers, JavaScript, Flash	Browser instance ID, detailed browser version, supported formats of images and media files, preferred and accepted languages, list of browser plugins, browser user's language, browser dimensions, Flash version, screen resolution, color depth, timezone, system fonts, IP address, accepted HTTP headers, cookies enabled, supercookies limitations
Other tracking mechanisms		
Headers attached to outgoing HTTP requests	HTTP headers	Customer's ID
Using telephone metadata	Smartphone malware	Health condition, religious beliefs
Timing attacks	HTML5, JavaScript, CSS	Boolean values dependent on the look of the website, stealing any graphics embedded or rendered on the screen
Using unconscious collaboration of user	HTML5, JavaScript, CSS, Flash	Browsing history, browser instance ID, user's location
Clickjacking	HTML5, JavaScript, CSS	User's email and other private data, PayPal credentials, spying on a user via webcam
Evercookies (supercookies)	Web server session, HTTP headers, HTML5, JavaScript, Flash, Silverlight, Java	Operating system instance ID, browser instance ID

Source: Citi Research

Use of Cookies

Cookies: small text files storing details of user's interaction with sites. They are made available to the site during subsequent visits, allowing sites to recognize the users and keep track, e.g., recall items placed in an online shopping cart or username/password.

Cookies are the most common means of tracking/collecting data which usually contain a string of text as a "unique identifier". Storing relevant details about a user's interaction with a site and preferences in this way helps facilitate a more user-friendly experience.

When a user returns to a particular website, cookies enable the website to recognize a user's web browser (e.g., Google Chrome, Internet Explorer, Firefox) and recall certain information about the user. Without cookies, surfing the Internet, making transactions and communicating with friends on social networks would be a different experience. The examples below demonstrate the role that cookies play in enabling regular internet activities:

- Help remember customized settings, such as user names and passwords;
- Allow a website to display the contents of the user's shopping basket when they move to the 'check out stage' on a retail website;
- Help remember preferences on a site and how people use the site (to help with design and layout);
- Allow the web browser to remember family-safe modes set by parents wanting to protect their children from inappropriate website use;
- Help to improve the web experience with increased personalization, e.g., Netflix or Amazon recommendations, a news site listing stories by the type of stories that may be of interest.

There are different types of cookies:

- **Session cookies:** These cookies allow websites to link the actions of a user during the browser session. They are created temporarily in the web browser and expire as soon as the visitor leaves the site. They remember information for as long as the visitor operates the web browser. These are typically used to keep track of movements across pages, to identify the user logging on, saving items in a shopping basket, and for security.
- **Persistent cookies:** These are saved on the device allowing user information and settings/preferences. They are read by the browser each time the visitor goes back to the website that sent the cookie. Persistent cookies also include ones from websites other than the one a user is visiting, known as third-party cookies, which can be used for targeted advertising. The browser will delete them based on a duration period within the cookie file.
- **First- and third-party cookies:** Whether they are first or third party refers to the website or domain placing the cookie. First-party cookies are set by the website being visited and third-party cookies are set by companies other than that being visited. The third-party cookies often relate to web analytics and advertising and can track a user across different sites.

It is normally the persistent, third-party and tracking cookies which are of most concern from a privacy perspective. These cookies can be harder to delete and have expiration dates that can be extended by the website itself.

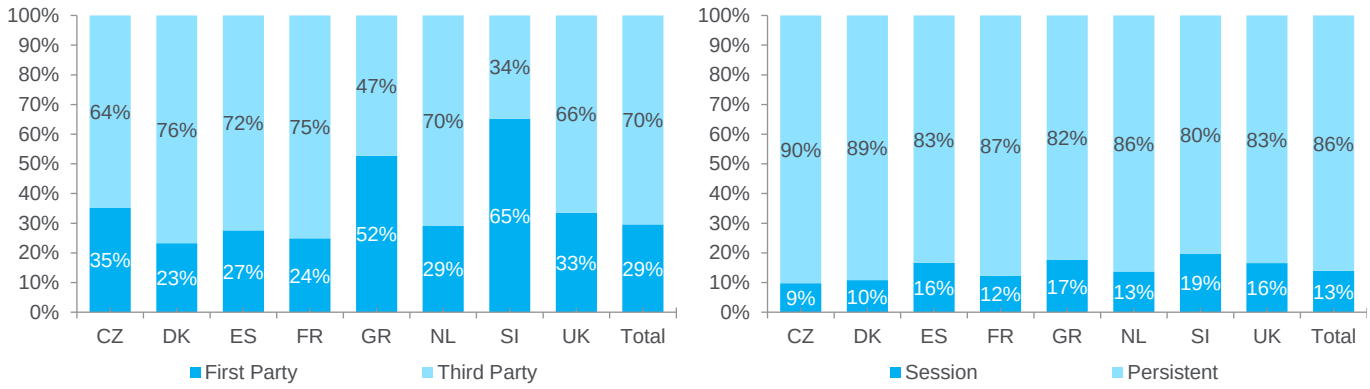
Flash cookies (or locally shared objects) have also become popular. These are pieces of information that Adobe Flash might store on a computer which is designed to save data, e.g., scores on games. It is harder to delete them in the same way as other cookies, which means some companies use them to reload other cookies back onto a computer. We have also seen the appearance of a 'Super Cookie' and 'Zombie Cookie'. A Super Cookie is designed to be permanently stored on a user's computer, and is more difficult to detect and remove than regular cookies. A Zombie Cookie is designed to return to life after being deleted.

Article 29 Working Party: A technical, advisory, body within the European commission comprised of representatives from all European national data regulators. They issue advisory opinions and clarifications on data protection and privacy.

In February 2015 the Article 29 Data Protection Working Party (European advisory body on data protection and privacy) published 'Cookie Sweep Combined Analysis' in which it did a sweep of 478 websites in the eCommerce, media, and public sectors across eight Member States (Czech Republic, Denmark, France, Greece, Netherlands, Slovenia, Spain, U.K.). There were 16,555 cookies set across the 478 sites with a mean number per site of 28.9 (23.5 on eCommerce sites and 49.8 on media sites), and only seven sites with no cookies at all. Overall, third-party cookies

made up 70% of cookies on the site, and 86% of cookies were persistent cookies. The average cookie duration of the third-party cookies was 1.77 years.

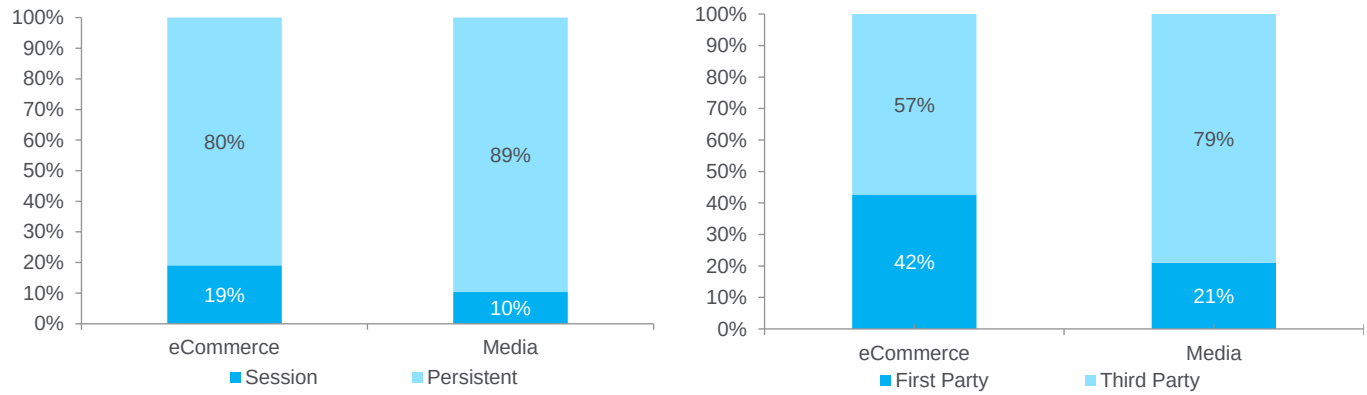
Figure 15. Cookie Type by Country in the European Union, 2015



Source: Article 29 Working Party 14/EN, WP 229

By sector, third-party cookies made up 79% of cookies on media sites but 57% on eCommerce sites. Persistent cookies were close to 90% of cookies on media sites but 81% on eCommerce sites.

Figure 16. Cookie Types: eCommerce vs. Media Sites



Source: Article 29 Working Party 14/EN, WP 229

Other Tracking Technologies

According to a report published by Viant, two-thirds of connected devices do not enable cookies and 50% of cookies expire within five days. As consumers and regulators cottoned onto the use of cookies to track users, and technology advanced, there have been new forms of tracking that have developed:

Fingerprinting

Fingerprinting: This is a form of data tracking that identifies a specific device by corroborating a range of different settings and characteristics that, when combined, are specific to that device. Once the device is identified, browser and behaviour data is then stored and used to develop a profile

This involves collecting unique identifying patterns of information to identify a specific device, or application. This often includes browser type, operating system, plugins, time zone, font preferences etc. More recently there are claims that battery status API, which was introduced in HTML5 to allow site owners to see percentage of battery life left so they can serve low power versions of sites, could also allow tracking of users. This means users can be tracked even if cookies are deleted and IP addresses are being hidden.

A study by Nikiforakis and Acar in 2014 found that 400 of the one million most popular websites have been using JavaScript-only fingerprinting, which works on flash-less devices like the iPad. It was also being used when users had requested 'Do Not Track' in their browser settings. A study by the Electronic Frontier Foundation found that more than 94% of Flash- and Java-enabled browsers can be uniquely identified.

Sites like panopticlick.eff.org allow you to see how well guarded your browser is against tracking:

Figure 17. How Secure Is Your Browser? – Screenshot from www.panopticlick.eff.org

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is…

Mixed results: you have **some protection** against Web tracking, but it has some gaps. We suggest re-configuring your protection software, or consider **installing extra protections**. Privacy Badger isn't available for your browser / OS, but **adding tracker protection lists EasyList and Easy Privacy** may work for you.

Test	Result
Is your browser blocking tracking ads?	⚠ Partial protection
Is your browser blocking invisible trackers?	⚠ Partial protection
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ No
Does your browser protect from fingerprinting?	✗ Your browser has a unique fingerprint

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

RE-TEST YOUR BROWSER

Thanks Fingerprint2 for various fingerprinting tests, Aloodo for portions of the tracker test, browserspy.dk for the font detection code, and to breadcrumbs for supercookie help. Send questions or comments to panopticlick@eff.org.

Source: Electronic Frontier Foundation - www.panopticlick.eff.org

Web Beacons / Pixel Tags

Web Beacons: This is an unobservable graphic image that is placed on website or email, often used in conjunction with cookies. Among other things, they read and place cookies, monitoring the behaviour of users

These are small objects embedded into a webpage or email which are not visible to the user (known as 'tags', 'tracking bugs', or 'pixel trackers'). When a page with one of these objects loads, it will make a call to the server for the object and this allows the company to know that someone has loaded the page. This is often used to see if readers are opening emails from companies and advertisers will often embed web beacons in their adverts to get an idea of how often an advert is appearing.

Mobile Tracking

There are several ways consumers can be tracked on mobile:

- **Advertising ID:** Apps downloaded on a phone show advertising based on advertising IDs. These include Apple's Advertising Identifier (IDFA), Android's Advertising ID and Facebook App User IDs. Users can opt out.
- **Wi-Fi:** When a phone is linked up to a Wi-Fi network, sensors can use the phones media access control (MAC) address to track movement, e.g., around a store.
- **Carrier:** The mobile carriers may provide de-identified data to third parties for advertising and other purposes, e.g., Telefónica provides mobile data to JCDecaux, which it uses to build up a more accurate picture of the audience around its outdoor sites.
- **GPS:** Geolocation tracking (via GPS satellites), e.g., if you pass a particular restaurant on a regular basis, the restaurant could use the information to offer a coupon. Google and Apple, for example, use GPS to track the location of users. If you have an iPhone, you can access the tracking details (and turn off location tracking) at Settings > Privacy > Location Services > System Services > Frequent Locations. If you have Gmail linked to your phone, and location tracking turned on, Google can track your location, which you can access on the timeline page.
- **iBeacons/Antennas:** Small wireless devices that use radio signals to communicate with mobiles/tablets. If a user has the app of a particular retailer on their smartphone, the user can be tracked if they enter a store or just walk by. In France, technology (developed by Retency) integrating antennas is being tested which can pinpoint the unique frequencies of individual smartphones and enables them to track the consumer as they enter the store (and it can calculate who entered after seeing a display), through to purchase.

Facial Recognition

Facial recognition uses biometric software which identifies individuals in a digital image. For example, Facebook's Moments product applies facial recognition technology to identify people in photos, and Yahoo filed a patent in March 2015 to use biometric data, including image recognition technology, to collect data on passersby of billboards.

Facial recognition is also a technology increasingly used in stores. In the U.K. a survey by Computer Services Corp of 150 retailers in 2015 found that a quarter of shops use facial recognition, rising to 59% amongst fashion retailers. This can be used for retail loss prevention, but at the same time it can be used to capture customer movement in-store, which could ultimately be linked up to other data, e.g., loyalty card.

Facial recognition technology can be joined up with other information to identify users. Alessandro Acquisiti, a behavioral economist at Carnegie Mellon University, took snapshots with a webcam of nearly 100 students on campus in 2011. He identified about a third of them with facial recognition technology in minutes. For a quarter of those he found out enough information on Facebook to guess at least a portion of their social security numbers.

It is worth noting that under the GDPR, facial recognition is classified as biometric data which is treated as sensitive personal data and therefore requires individuals' explicit consent.

Cross Device Tracking

Cross-device tracking: Techniques used to detect single internet users when they use various devices in order to create a seamless picture of the user.

What companies really want to master is cross-device tracking to pull together disparate datasets in order to create a complete seamless picture of consumer behavior/usage as device proliferation has increased. According to a study by GfK, 60% of online Britons switch between at least two devices in the same day, and 40% start an activity on one device and finish it on another.[2] Cross-device tracking ultimately involves being able to unify first-, second-, and third-party data sources. Deterministic and probabilistic methods are both used to attempt to identify a user across devices. Deterministic uses known data, e.g., email address or log ins used to log into a site on multiple devices. This is fairly easy for a site like Facebook. For marketing, registered user data is seen as the pinnacle, as it allows cross-device, or 'people-based campaigns', offering real people, across devices and across channels. The probabilistic approach applies machine learning algorithms to anonymized data generated via fingerprinting, mobile IDs, and cookies to create connections between devices as all of this data has unique IDs.

Audio beaconing is also used (by a company called SilverPush) for cross-device tracking, which involves the advertiser dropping a cookie on the computer while playing an ultrasonic audio through the use of speakers, and the inaudible code is received by other smart devices with the software development kit installed. This then links the devices as being used by the same person.

The interest in cross-device determination is evident in the activity in this space. In April 2016 Oracle acquired Crosswire; Google Ventures has partially funded Adelphic; Cisco is an investor in Adbrain; advertising agency WPP launched [m] platform to address the need for cross device data/tracking. All of these are cross-device-based technologies/technology companies.

Who Are the Trackers?

There are several anecdotes about how many data points are collected and how many trackers are in place:

- According to TRUSTe, the top 100 most widely-used sites are monitored by over 1,300 firms.
- PubMatic claims tracking on mobile gleans about 100 data points per user compared to 50-70 on desktop.

There is a high concentration of cookies deployed amongst a relatively small number of operators. A Princeton University study conducted in January 2016 of the top one million sites, found that there were 81,000 third-party cookies present on at least two first-party sites, but only 123 of those third parties was present on more

[2] GfK, Finding Simplicity in a Multi-Device World, 2015.

than one percent of sites. Google, Facebook, and Twitter are the only third-party entities present on more than 10% of sites, and 12 of the top 20 third parties are Google owned-domains (and all of the top five are Google owned). Google's doubleclick.net was the most prolific cookie-syncing third party, sharing 108 different cookies with 118 other third parties (based on the top 100,000 sites). [3]

According to the cookie sweep performed by the Article 29 Working Party, there were 25 third-party domains setting 53% of the third-party cookies.

Figure 18. Key Sources of Cookies on the Internet

Third party domain setting cookies	Owner	Count sites	Total number of cookies set
doubleclick.net	Google	213	247
adnxs.com	Appnexus	114	320
scorecardresearch.com	Comscore	98	198
rubiconproject.com	Rubicon Project	80	903
yahoo.com	Yahoo	64	167
gemius.pl	Gemius	61	112
360yield.com	PubliGroupe	59	282
twitter.com	Twitter	59	83
turn.com	Turn	58	133
adform.net	Adform	56	252
mathag.com	Mediamath	52	177
mookie1.com	Akamai	52	167
adtech.de	AOL	51	124
pubmatic.com	PubMatic	50	176
openx.net	OpenX	47	49
google.com	Google	46	49
serving-sys.com	Sizmek	44	183
criteo.com	Criteo	43	140
adformdsp.net	Adform	38	77
smartadserver.com	Smartadserver	37	153
casalemedia.com	Index Exchange	36	213
adscale.de	Stroeer	34	124
atemda.com	Wide Orbit	33	148
abmr.net	Akamai	33	33
254a.com	YD	30	32

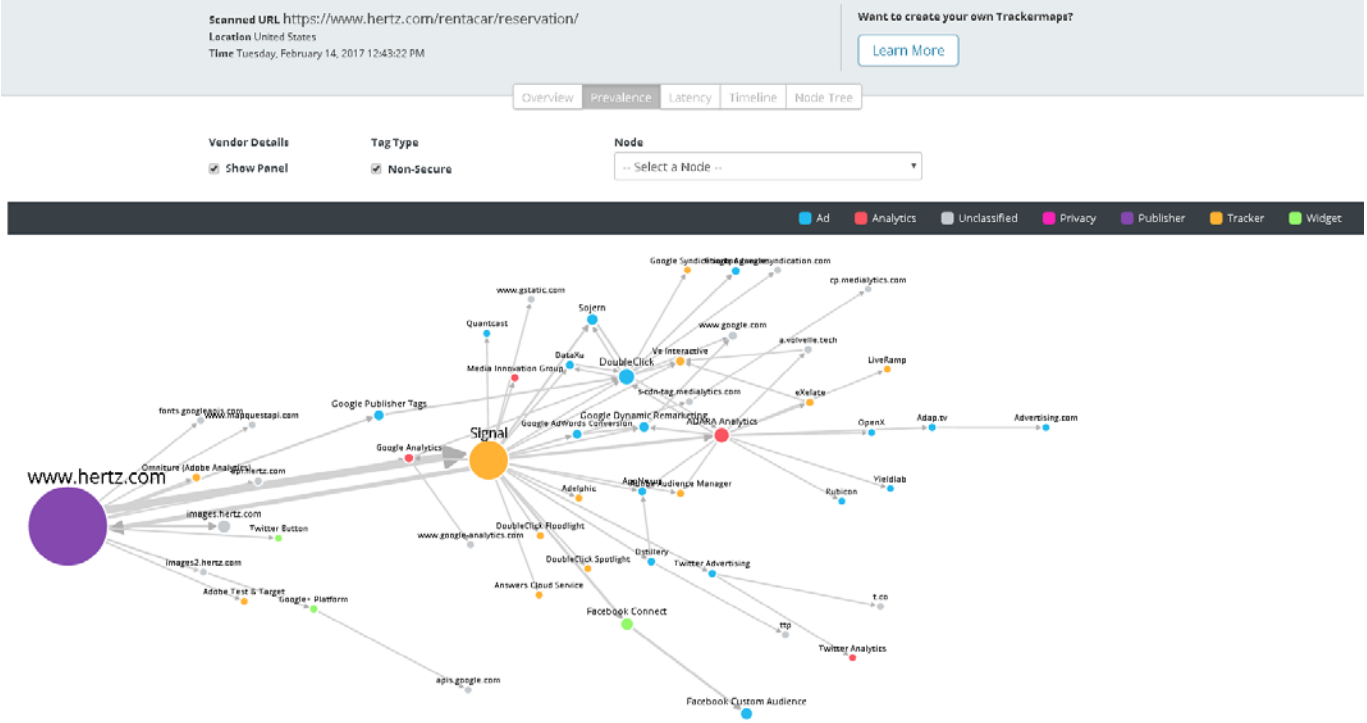
Source: Article 29 Working Party

Another means of looking at who is setting trackers is Evidon's Trackermap, which shows the number of trackers, who they are set by, and the type of tag.

Below is the analysis for Hertz. There are 52 unique tags in total. Of the tag calls, 41% are advertising-related (and typically third party). There are also some long chains, e.g., from Signal to Advertising.com, which can increase issues caused by latency and raise the risk of data leakage.

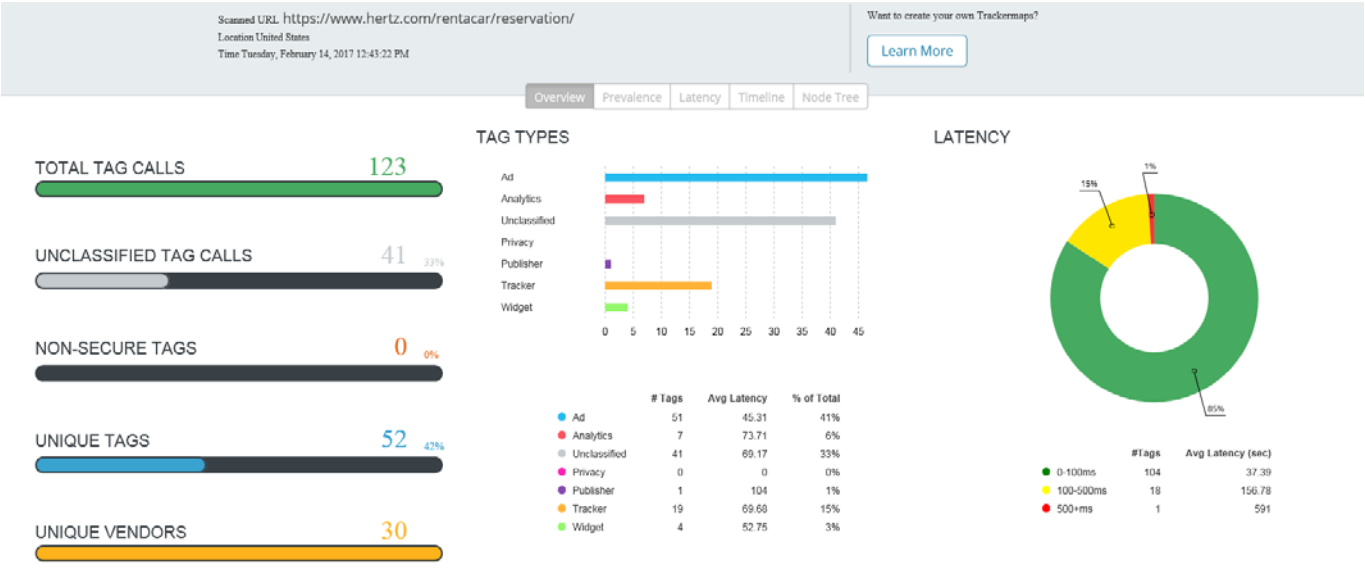
[3] 'Online tracking: A 1 million-site measurement and analysis'. S. Englehardt, A. Narayan, July 2016.

Figure 19. Trackermap of www.hertz.com/rentacar/reservation/ – Part 1



Source: Evidon

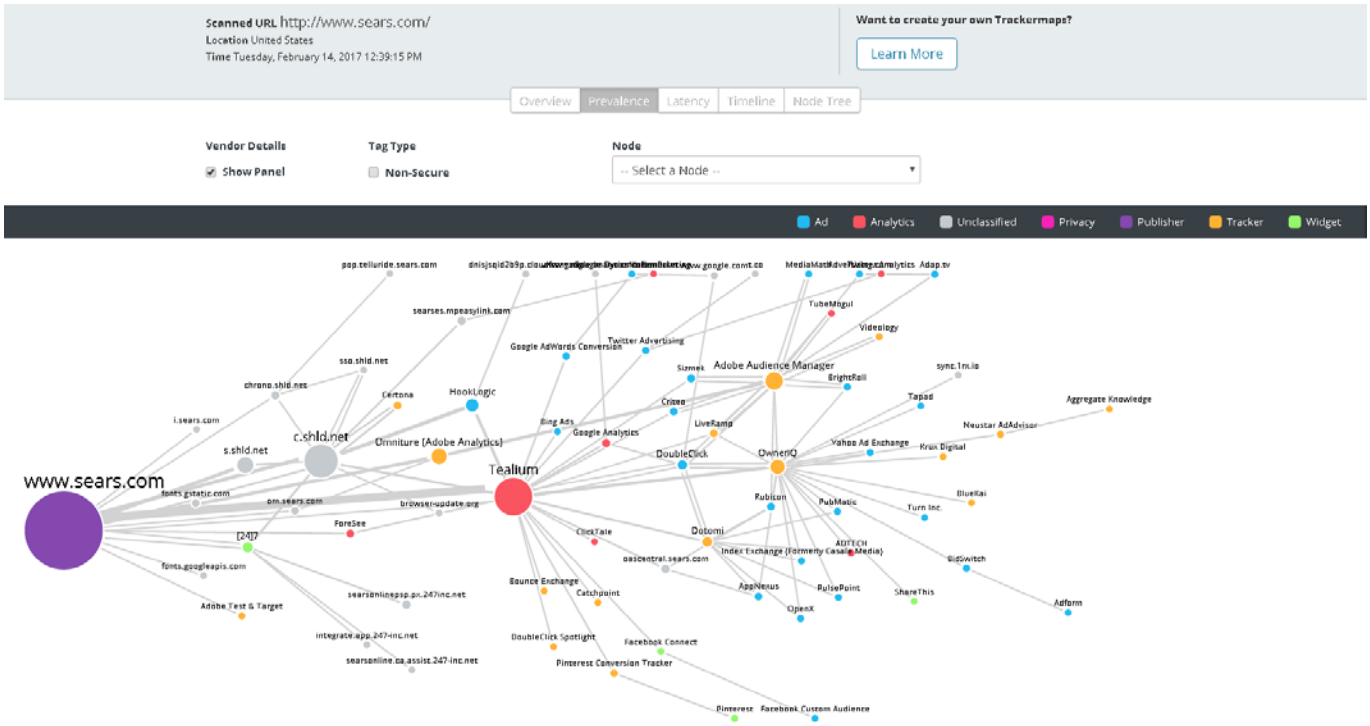
Figure 20. Trackermap of www.hertz.com/rentacar/reservation/ – Part 2



Source: Evidon

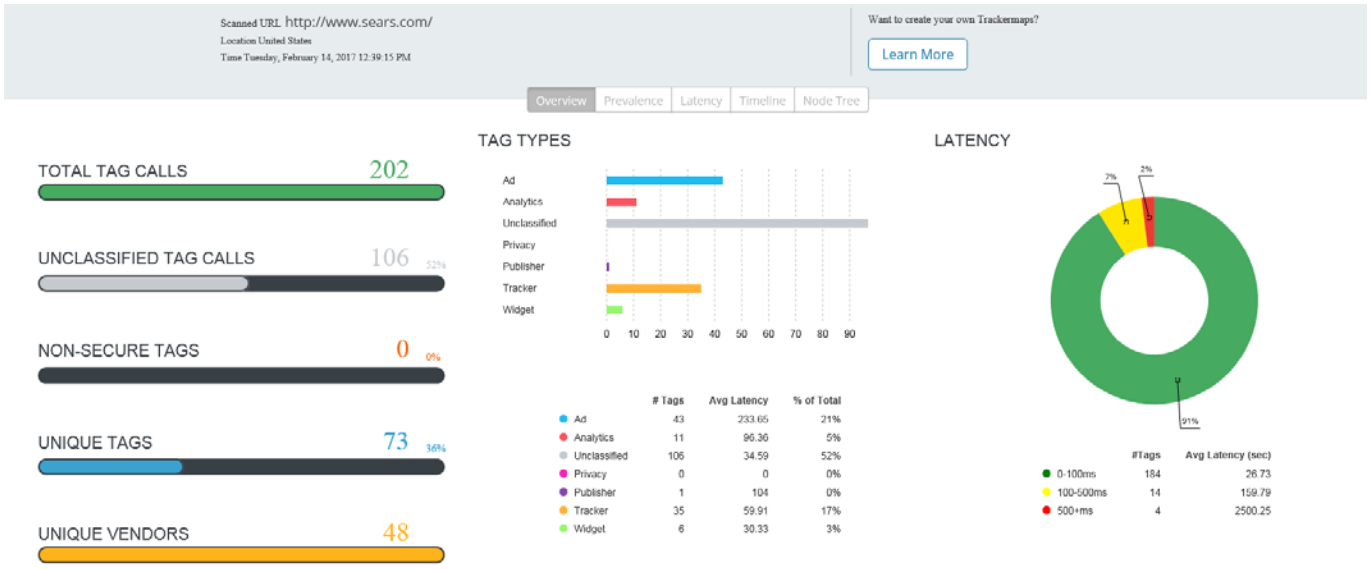
Taking the Sears home page, for example, there are more unique tags than on the Hertz page at 73 overall; 21% of tag calls are cited as advertising. Adobe and Google feature heavily on the Trackermap. Similarly, the Trackermap highlights a number of long chains. There is also the presence of the cross-device tracking companies, such as Tapad and Krux (Salesforce.com).

Figure 21. Trackermap of www.sears.com – Part 1



Source: Evidon

Figure 22. Trackermap of www.sears.com – Part 2



Source: Evidon

What is the Data Being Used For?

There are eight main purposes of tracking/data collection.[4] The following are identified as the most common:

Online/Targeted Advertising

One reason for collecting user data is it provides the ability to deliver more targeted advertising to consumers based on consumer traits and demographics. Programmatic advertising, which was highlighted earlier as a means of buying advertising inventory, has evolved as a result of tracking consumers. We have also seen the rise of cookie leaking/syncing which means that cookies will be passed from one domain to another, thereby enhancing the ability to target. In June 2016 Google updated its privacy policy so it can combine information from Gmail, YouTube, and other applications, with information it collects via browsing data from DoubleClick. The change is optional for existing users and default for new Google account users.

Cross device (people-based marketing), using a combination of registered data and other third-party sources, is a growth area. According to a report published by Viant,[5] 83% of digital marketers it surveyed found people-based campaigns perform better than cookie-based campaigns and the respondents expect to spend 40% of their digital advertising budgets on people-based marketing campaigns in 2017 (and 75% invest in this way in social media).

Personalize and Improve Products/Services

User data is utilized by site hosts to improve website performance, as well as to increasingly personalize content and products that are shown and offered to individual users. Examples of this include:

- Amazon recommending products based on shopping history on the site;
- Grocery retailers that also offer motor insurance using purchasing data from loyalty schemes to draw inferences about risk levels;[6]
- Social listening, i.e., picking up commentary from social media enables companies to react to public views and adapt and develop products/services;
- In the area of healthcare, the combination of patient data and other data sources, e.g., data from wearables could be used to identify illness/disease early and develop tailor-made medicines.

Fraud Prevention

Analysis of data is used to detect fraud and to identify suspicious activity. Both fraud and the incidence of “false positives”, i.e., the rejection of a valid transaction, can be a significant (and costly) problem for financial institutions and merchants.

[4] 'Web Tracking: Mechanisms, Implications and Defenses' Tomasz Bujlow, Valentin Carela-Espanol, Josep sole-Partea and Pere Barlet-Ros, July 2015.
[5] Viant ‘Power of the People’ report commissioned Censuswide to survey 251 brand side digital marketers in the U.K. in December 2016.
[6] DotEcon and Analysys Mason, ‘The Commercial Use of Consumer data – A Research Report for the CMA’, June 2015.

Allowing a fraudulent transaction can cost the merchant financially but it can cost the financial institution as well, depending on the nature of the transaction – certain transactions like remittances carry a regulatory requirement for Anti-Money Laundering (AML).

Similarly, a false positive translates into an unhappy consumer and lost sales. Javelin Strategy & Research published Annual Surveys on this topic in 2015 and 2016. The first report estimated that 15% of all U.S. cardholders have experienced at least one false positive in the last year, representing a loss of $118 billion annually – equally importantly, 39% of declined cardholders abandoned their card after being falsely declined.

Machine learning and other computationally intensive artificial intelligence techniques can be used to improve fraud detection as well as reduce the incidence of false positives. However, such techniques, which are being used by companies like PayPal and Square, rely on data that is inferred based on a much larger number of variables and data-points than the traditional techniques that banks have used in the past.

Business Efficiencies and Processes

By retaining customer data, an online retailer can pre-fill forms, e.g., delivery and card details. Data can also be used to decide what products to stock by location according to localized demand. McKinsey predicts that applying early success of big data in healthcare could reduce healthcare costs in the U.S. by over $300 billion.

Data Brokers: Organizations that fuse data from a range of different sources. The data is usually sold on to other organizations.

The remaining four reasons relate to a combination of data selling, leakage, sharing, and discrimination. Data brokers have been at the center of this historically. The likes of Datalogix (owned by Oracle), Acxiom, and Experian will obtain data from public records, lenders, surveys, and other providers and sell lists based on categories e.g. motor insurance companies may buy lists of people with insurance renewals coming due. A commonly quoted datapoint is that Acxiom has on average about 1500 pieces of data on about 96% of Americans[7] and 700 million people globally. Data brokers were a topic of review by the FTC in the U.S. in 2014, which culminated in the 2015 'Data Brokers: Transparency and Accountability' legislation.

Anonymized data: Personal data is irreversibly changed so the specific individuals cannot be identified at any point.

Several companies sell anonymized data to other parties, e.g., telecom companies may sell data for geolocation tracking and credit card companies sell anonymized data to advertising companies. First-party data may also be shared with other parties to complete transactions, conduct surveys, prevent fraud/for security, or for marketing.

One study found that 56% of over 100 non-social networking websites leaked information to third parties, and that rose to 75% for instances including the user identifier.[8] The U.K.'s CMA[9] study of commercial uses of consumer data in June 2015 provides some interesting examples of sharing data between first and third parties:

- A restaurant contracts a developer (third party) to build apps that share data about consumer preferences, and it uses customer responses to improve the app;
- Price comparison sites may share information on consumers e.g. insurance renewal dates, vehicle etc. with insurance companies (third party).

[7] 'The Filter Bubble: What the Internet is Hiding From You', Eli Pariser, 2011.
[8] 'Privacy Leakage vs. protection measures: the growing disconnect', B. Krishnamurthy, K. Naryshkin, C. Wills, 2011.
[9] CMA is the Competition Markets Authority – public U.K. regulator that aims to ensure sufficient levels of market competition

Assessing Financial Credibility and Insurance Risk

Traditional lenders tend to rely on credit scores from third parties (from companies like Experian). There are several examples of how the availability of various sources of data has transformed the way that credit and insurance risk is being assessed:

- According to CNN (August 2013), there are tech-based financial start-ups using a breadth of data to assess creditworthiness, including information from social media, e.g., Lenddo which takes into account if you are friends on Facebook with someone else who has repaid a loan late to Lenddo, and Kreditech which claims it uses up to 8,000 data points, including data from Facebook, eBay, and Amazon. It will also use location data to determine if your computer is located where you said you live or work. These are niche providers but they provide examples of how personal data can be used to assess credit risk. In countries in Africa, the use of social media profiles to assess creditworthiness has become commonplace due to the difficulty in obtaining adequate data.[10]

- Many motor insurers now use telemetry-based packages or mobile apps (taking into account actual driving information) to develop an accurate profile of a driver, and to allow consumers to trade information for discounts (Usage Based Insurance). There have also been reports about insurance companies using other personal data to inform prices. In November 2016 it was reported by the BBC that Facebook blocked insurer Admiral's planned trial in the U.K. to use motorists' posts (with permission) to judge risk levels, which would be reflected in discount levels of 5%-15% if the driver was judged to be low risk.

- Accenture research found that a third of health insurers offer services based on the use of wearable technology tracking activity e.g. discounts to premiums for showing improving lifestyle, measured through higher activity levels. Vitality Health, for example, offers an Apple Watch to those with healthcare plans and the monthly payment level depends on the user's level of monthly activity.

World Privacy Forum: U.S. based, non-profit, research group that works to educate and explore issues surrounding data privacy.

Privacy groups have raised issues around the use of personal data for the above purposes. The World Privacy Forum has investigated a shift to consumer scores, which is a computer generated number that attempts to predict the likelihood of someone falling ill or paying off debt. Pam Dixon, executive director of World Privacy Forum, says "*A major national health plan came to the quants wanting to know how they could figure out how much to charge people. If a woman did a lot of online shopping, she was predicted to be a much higher health risk. If a couple bought hiking boots, that was considered a good factor. I doubt that when someone goes online to buy a scarf they think, 'This is going to affect my healthcare.' People could be paying more for healthcare, but we'll never know. Acxiom and Experian sell lists of people with diseases. They claim it's a propensity [instead of a numeric score], but there's your name.*"[11]

[10] BBC.co.uk, 2 Nov 2016.
[11] 'The Secretive world of Selling Data About You', Newsweek. 30 May 2016.

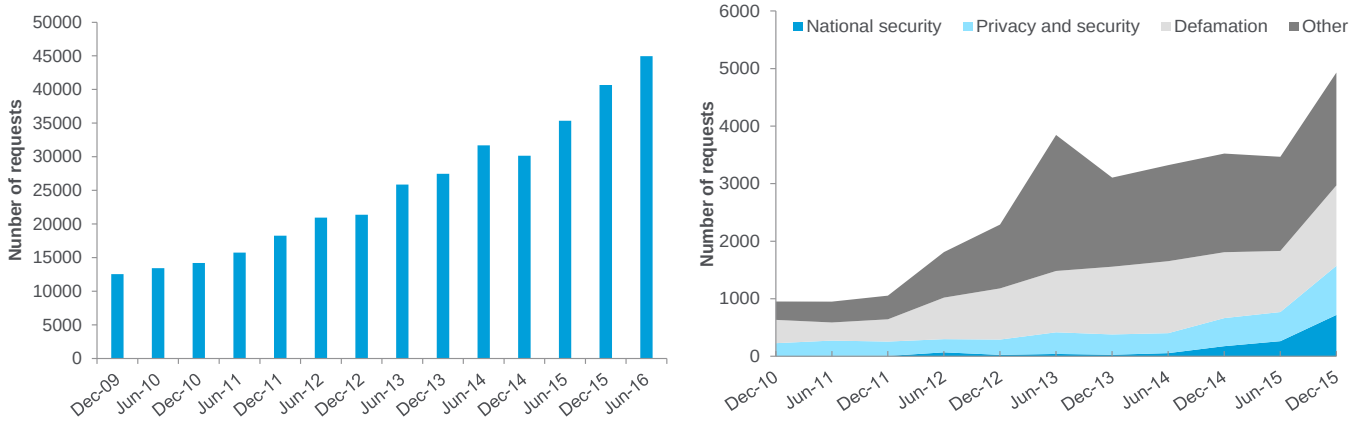
Adapting Pricing

Some may call it pricing discrimination, but tracking and segmenting can be used to modify the price of a product based on the user. Geographical location can have a significant impact on displayed pricing — up to a 166% differential in price, and up to 400% based on the affluence of the user.[12] A 2012 article in the Wall Street Journal highlighted an example of this, reporting that Orbitz advertised more expensive hotels to Mac users than PC users as it found that Mac users spent ~30% more on hotel bookings than PC users. Uber is a more transparent example of a company using an algorithm for dynamic pricing as it applies 'surge pricing' when demand is high in particular areas.

Government Surveillance

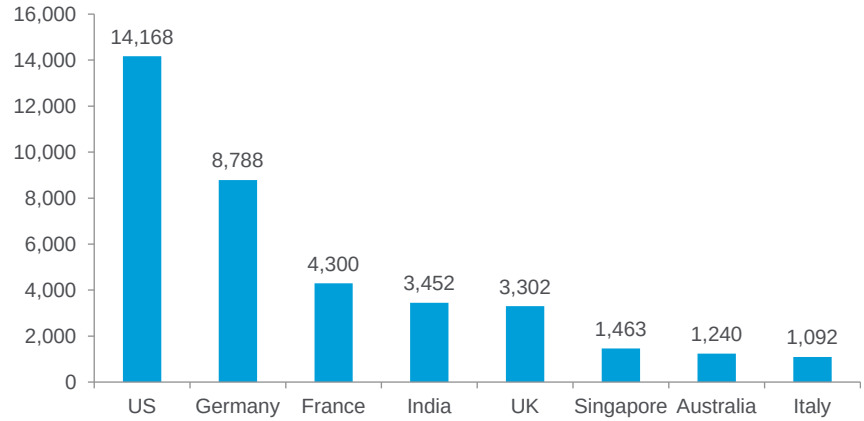
This has been a controversial topic since Edward Snowden revealed the mass surveillance by a variety of national security agencies in 2013. Google reports the number of requests for user information data and data removal every six months from governments globally and, in the past year, the number of requests has risen by 27%. The governments of the U.S., Germany, and France made the most requests to Google January through June 2016.

Figure 23. Google: Government Requests for User Information and Requests For Information Removal



Source: Google

Figure 24. Google & YouTube: Number of Data Requests by a Law Enforcement Agency by Country Jan-June 2016 (for >1000 requests)



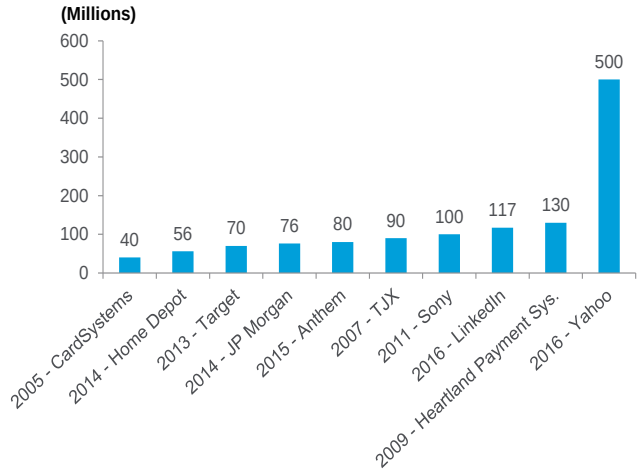
Source: Google

[12] 'Detecting price and search discrimination on the internet', J. Mikians, L. Gyarmati, V. Erramillie, N. Laoutaris, October 2012.

Theft (Identity, Financial etc.)

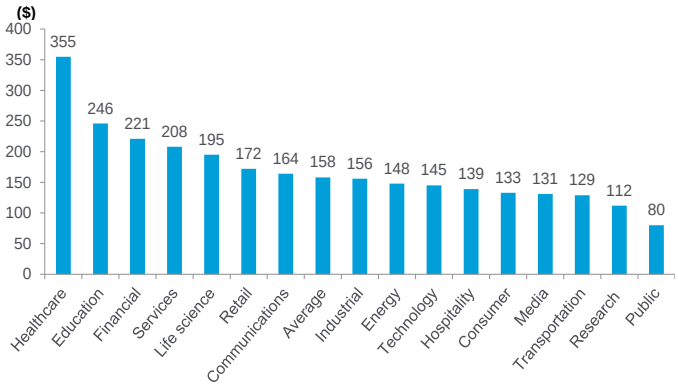
There are an increasing number of examples of cybercrime in which passwords, money, medical data, etc. are stolen online. For companies this presents various risks to the business, from reputational damage to the risk of litigation and fines, and for individuals the implications can also be far reaching. A Morrison & Forrester consumer survey in the U.S. found that 52% of consumers cited identity theft as their biggest privacy concern in 2015, which was up from 24% when the survey was conducted in 2011.

Figure 25. Selected High Profile Data Breaches, 2005-2016



Source: Wall Street Journal

Figure 26. Per Capita Cost of Data Breach by Industry ($)



Note: Calculated using activity based costing assigning a cost to activities to discover a breach, escalate/notify data subjects, amending controls/procedures and lost business. Does not include cost of fines.
Source: Ponemon Institute '2016 Cost of Data Breach Study: Global Analysis', June 2016. Sponsored by IBM.

Implications: The Cookie Is Crumbling But You Are Still Being Watched

The fact is that pretty much everything we do as consumers online is tracked in some way, shape, or form. Cookie tracking is clearly the most widely known technique, but as we have shown above, there are many other ways users can be tracked.

Now for many consumers this will be part of an accepted value exchange whereby information is knowingly surrendered in return for a valued good or service. This said, most consumers may not fully appreciate how much of the data they generate is being collected and how this ends up being used. Many would, we suspect, probably be surprised that their ability to get credit may be impacted by who they are friends with on social media, for example.

Before considering how strongly consumers feel about this, it is briefly worth considering some of the technological challenges associated with data collection and analytics. It is this we turn to in the next section.

Technological Challenges to Realizing the Opportunity from Data

There are three parallel forces at a high level driving the opportunity in data, as well as the challenges. The first is of the bottom-up technical variety (advances in hardware and software); the second is the pressure businesses of all sizes and nearly all industries are under to use data to achieve competitive advantage; the third is the rapidly evolving risk and regulatory environment, wherein there is a desire to exploit newer agile processes to reduce risk and satisfy regulators. Ironically here, the companies that are oldest and are sitting on the largest data asset (because of the time element) are in the more challenging position to gain value from their data, as they lag behind from a technical perspective.

Technology Is Evolving Quickly

We noted earlier the commoditization of computing and storage with price points for processing and storing data coming down by order of magnitude. Also, related, the standardization of smart phone architecture has driven a rise in sensors and Internet of Things applications. This has enabled the technologies that underlie this data opportunity and that have given birth to scrutiny around data protection and ePrivacy. These technologies represent one of the most significant new generations of data management technology we have seen in more than a decade.

Traditional data management architectures have been based on and evolved from relational database technology invented in the 1970s and that went mainstream in the 1990s. Relational databases continue to house the majority of traditional corporate data, especially of the transactional variety. The explosion in the growth of data in recent years, however, has been of a different sort and altogether different magnitude. This has resulted in the "renaissance" in data management technologies that we have witnessed over the last decade.

Non-Relational Structured Query Language (NoSQL): A NoSQL model/database provides a mechanism for storage and retrieval of data that is not structured in a tabular way, and which is seen as more flexible than relational database tables.

Structured Query Language (SQL): This is a special purpose language used in programming for data management in either a relational database or data stream system.

The explosion in data has been characterized by data that is unstructured or semi-structured (versus structured / transactional data). Also, the order of magnitude of data has increased in not only volume, but also velocity (rate of change) and variety (inherent in the data being semi or unstructured). The relational database is not well-suited to this new data landscape, as relational database instances generally only "scale up" and have fixed schemas for classifying / categorizing data. While this broader data opportunity will result in more data in traditional relational databases, we see the front-line of new data management technology based on scale-out architecture and with more flexible classification / categorization systems.

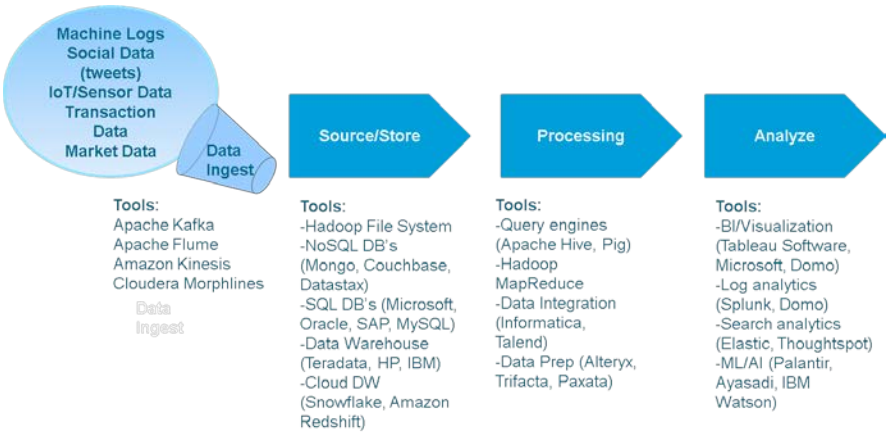
Figure 27. Relational vs. Non-Relational Databases

	NoSQL	SQL
Data Model	Non-relational	Relational
Data Storage	Stored in documents (JSON), key value stores, column stores or graphs	Stored in a table.
Data Properties	Flexible. Records can have different properties (and be modified easily).	Designed for data with same properties. Modification is difficult (alter schema).
Examples of Types of Data	Semi/unstructured data: IoT, social, web, mobile, video, audio, images.	Structured data: 'organized' in rows/columns: Excel, data marts, most enterprise databases.
Database Schema	Schema-agnostic and flexible. Can be dictated by application.	Strict schema. Must be maintained and synced between application and database.
Transaction Support	Transactions (ACID) typically not enforced. Can be flexible.	ACID transactions supported/enforced.
Performance	Typically faster (at equal scales).	Typically slower (at equal scales).
Scale	Scale out (partitioned across multiple servers).	Scale up (adding more CPUs/RAM)
Application Examples	Search recommendation, personalization engine, emerging big data/machine learning	Enterprise transaction systems (payments, orders, etc.), reporting, finance/accounting apps.

Source: Citi Research

The innovation here has come from the consumer Internet market, where many of the large players (notably Google and Yahoo) were amongst the first to be in a position to leverage this new data opportunity. Technologies such as the Hadoop file system, NoSQL databases and eventual consistency combined with the Map Reduce and Spark processing technology. The “big data” architecture is still evolving and maturing with a very fragmented landscape of technologies.

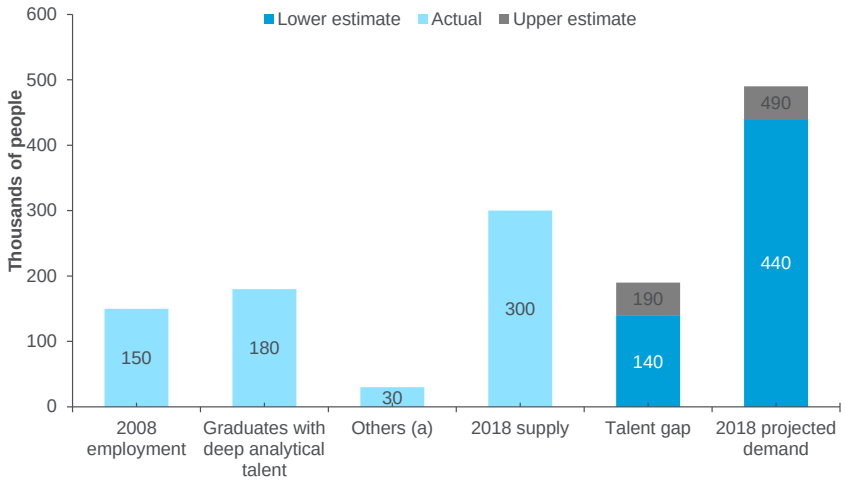
Figure 28. Big Data Architecture and Landscape



Source: Citi Research

The immaturity of these new technologies, as well as the inherent technology fragmentation, has been an inhibitor to broadly exploiting the data opportunity. We don’t expect there is a short-cut to the solution here, although we note building populations of “data scientists”, software engineers, systems administrators, and other technical personnel that are proficient in big data technologies will be a requisite competency for most data-centric companies.

Figure 29. Supply and Demand of Deep Analytical Talent by 2018



(a) Other supply drivers include attrition (-), immigration (+) and reemploying previously unemployed deep analytical talent (+).

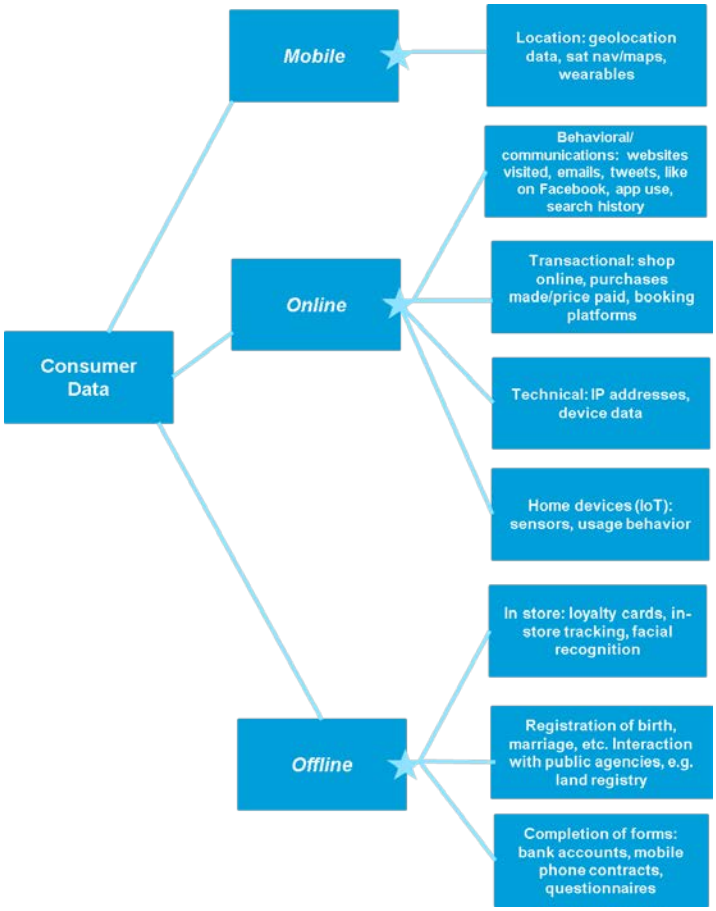
Source: McKinsey, Big Data: the next frontier for innovation, competition and productivity

Along with this improving picture around available skill-sets, we also see software and IT service vendors embedding the big data technologies discussed above (Hadoop, Spark, etc.) into their finished solutions, versus simply offering support for open source technology. As is typical as markets develop, initially, there is bottom-up demand for the open source technology from small engineering teams, particularly in industries like technology and Internet. These early customers only require commercial support for open source technology and typically don't pay license fees for proprietary software. We sense in the last year or so, there is incremental demand for proprietary software products where customers are paying a license for technology that includes open source. This has generated more revenue for solution-oriented providers and signals a maturing market.

Business Models and Age of Legacy Bring Opportunity and Challenge

As noted earlier, the size and age of a company brings significant "raw material" opportunities, in the form of data volumes that newer entrants in markets do not have. There is an old adage that "*more data beats better algorithms*", but when "more data" is tied up in a multiplicity of systems, it is difficult to gain value from data. The idea of "data gravity" encompasses this as data analysis is generally easier when it is close to the source of the data. When data sources were originally put into production in ways that were not meant for modern data analysis technologies, the challenge of data integration comes to the fore. We see a significant opportunity in data integration tools as legacy companies look to unlock data that is currently being generated or has been generated in the past. There are very tangible examples of this, such as bringing together all information around interaction with a given customer. This seemingly simple problem of having all information about interactions with a single customer has not only sparked significant data integration efforts, but has also lead to an investment cycle in many industries, whereby companies are replacing their customer-facing applications to deliver this "single view of customer".

Figure 30. Sources of Customer Data



Source: Citi Research

The Rise of "RegTech"

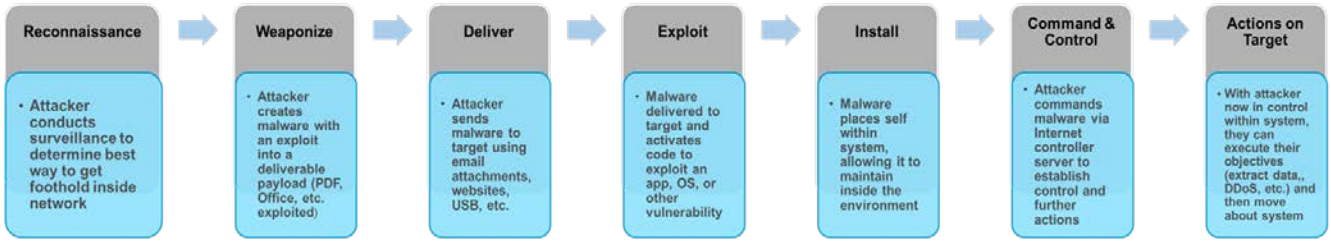
As defined by the Financial Conduct Authority (FCA), RegTech is a sub-set of FinTech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities. In April 2016, the FCA piloted a two-day event to help improve firms' understanding of regulatory reporting requirements and/or realize efficiency gains in the preparation and transmission of regulatory data. Traditionally, when a regulator conducts an investigation, it makes a request for data which the corporate entity then collates before "pushing" it to the regulator – at the event, the notion of a regulator tapping into a corporate's systems to pull the requisite data was considered.

Regardless of whether we move to an end-state where data is "pulled" rather than "pushed", the need for a quicker response that does not burden a corporate in view of burgeoning regulatory requirements leads to a need to: (1) possibly re-engineer underlying systems and processes to smooth data flow and ensure data uniformity across source systems; (2) implement a modern data governance and management system; (3) manage customer consent and data-sharing; (4) update data-retention and archiving needs; and (5) restructure existing "data processor" contracts to delineate specific responsibilities,

Data Security and the Fear of Breach Is a Clear Technical and Business Challenge

In 2013, the number of high-profile breaches of customer / consumer information in the U.S. began to skyrocket. This was years after the California Security Breach Notification Law, thus we know that the rise in "breaches" was most likely an actual rise in breach activity vs. simply more frequent notifications of these events.

Figure 31. Data Breach Flow Chart



Source: Citi Research

Data security often still involves a complex, inefficient patchwork of point products, which often overlap in terms of functionality, but do not actually operate as a cohesive solution to address the challenge. This is still largely where the market is today, although there are some signs this is changing.

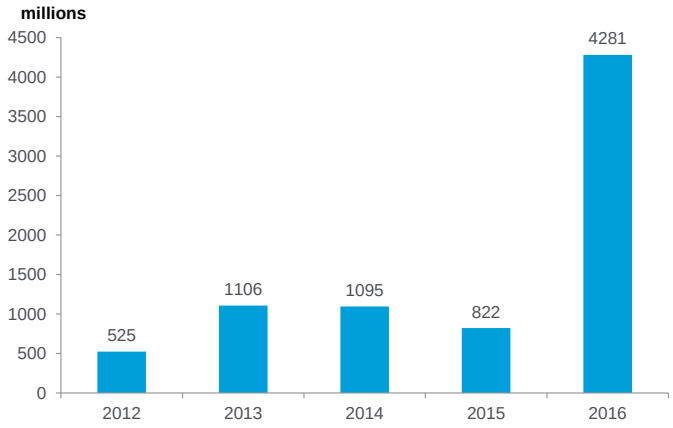
Securing data takes two basic approaches; in fact both are usually employed. The first approach is to secure the underlying infrastructure such as network, servers, PCs, and more recently mobile devices that operate on, store, transport, and otherwise interact with the data. This approach is easier, because these assets are very tangible (although are becoming less tangible with the shared public cloud). The second approach is to manage user identities and their access to the actual data. This approach should have more efficacy as it is applying security policies directly to the asset in question (the data) and those interacting with the data (versus a device, which is more of a proxy).

While the user / data approach is likely be where more incremental effort is applied, it has fundamental challenges.

- First, users are hard to identify and the authentication process has inherent flaws. For example, passwords are many times insecure and more sophisticated techniques are inconvenient.
- Second, securing data usually involves encryption. Encryption, or making information unreadable unless it is unlocked with a "key", is complex. In its simplest form, each data element must have a unique key. With the scale of more enterprise information stores, this presents a key management problem with high order of magnitude. Also, many applications are not written to be able to operate on encrypted data and simply "break". Workaround solutions are inherently limited in what they can do and may just work on an application-by-application basis. For example, companies employ solutions that encrypt information for use in email, but then when this information is stored, an enterprise application like inventory or supply chain cannot read the encrypted information the same way.

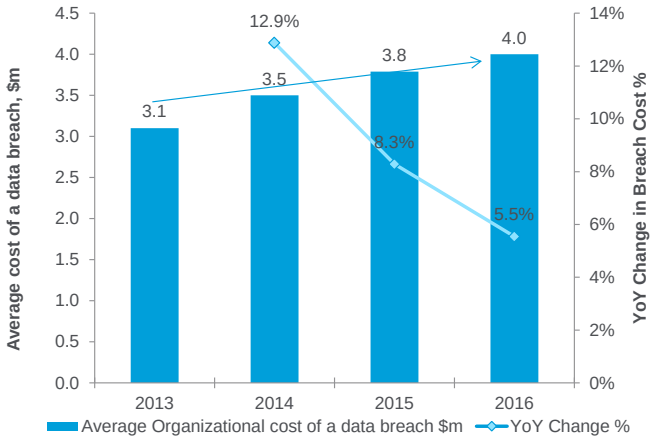
Historically in IT, technologies have evolved and have been implemented to derive business value with security as an afterthought. That has clearly been what is happening as companies have looked to capitalize on the data opportunity. At the same time, the increasing cost of "doing business" from security is high and likely to escalate.

Figure 32. Number of Records Exposed by Data Breaches



Source: Risk Based Security

Figure 33. Average Organizational Cost of a Data Breach ($m) & YoY Change %



Source: Ponemon Institute '2016 Cost of Data Breach Study: Global Analysis', June 2016. Sponsored by IBM.

Implications: Less Haste, More Speed

The opportunity from data is clear but exploiting this even for large companies is not always straightforward, either because of the challenges in making legacy systems work together or because of aggressive competition from newer, more flexible players.

In this context, in the rush to exploit the data opportunity, not all companies have paid enough attention to, or fully factored in, the necessary safeguards for either cybersecurity or privacy — something that may have consequences longer-term.

Before considering these, however, let's look at how consumers approach the topic of privacy and data protection as it is in the gap between what consumers want and how markets/companies actually work that regulation is often conceived.

Consumer Attitudes to Privacy

The main focus of this chapter is to look at consumer attitudes to privacy. We look at how consumers in different markets and of different types think about issues to do with privacy and data protection. We also look at how this affects their behavior both in terms of usage of different products and services but also their response in the event that their data security is compromised.

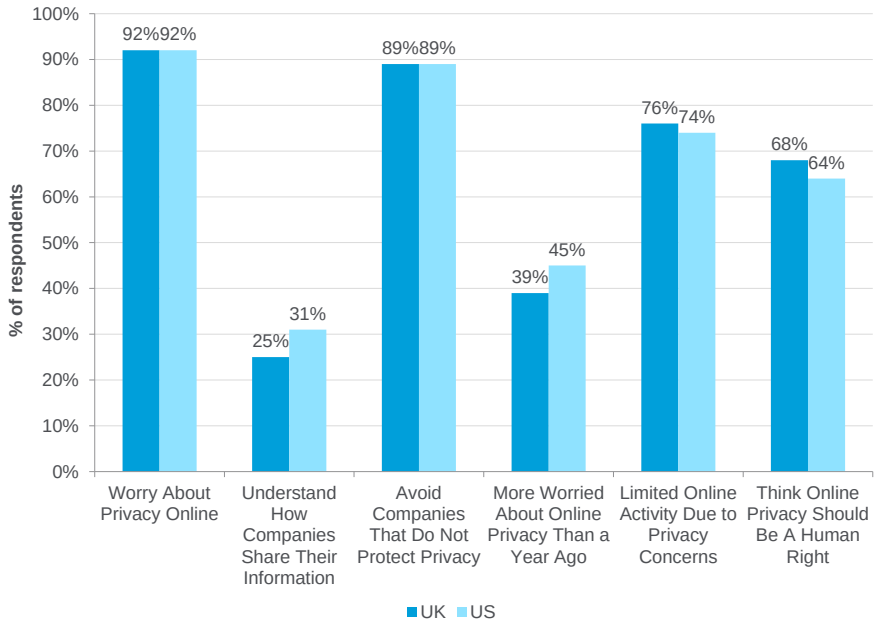
The picture this paints is a confusing one, not least because, as the U.K. Independent Commissioner's Office (ICO) argues, there is no 'one-size-fits-all' view on what the average consumer cares about. What is clear from a number of different sources, however, is that there is an inherent contradiction between what a lot of consumers say they think/want with respect to privacy/data protection and how they conduct themselves online.

It is perhaps because of this gulf that regulators worldwide have decided to act in the way they have. But before we get too caught up in how regulators are looking at addressing consumers' (supposed) concerns – we look at this in depth the next chapter – let's look at what consumers think and the juxtaposition with how they manage their own digital lives.

How Concerned Are Consumers About Privacy?

On one level this is a simple question to answer. In most surveys and in most markets, consumers tend to indicate that they are worried about privacy. In Figure 34 we show TrustE data from 2016 that simultaneously shows that general levels of concern about online privacy are high while the general understanding of how information used is low.

Figure 34. TrustE Snapshots of Consumer Attitudes Toward Privacy in the U.K. and the U.S.

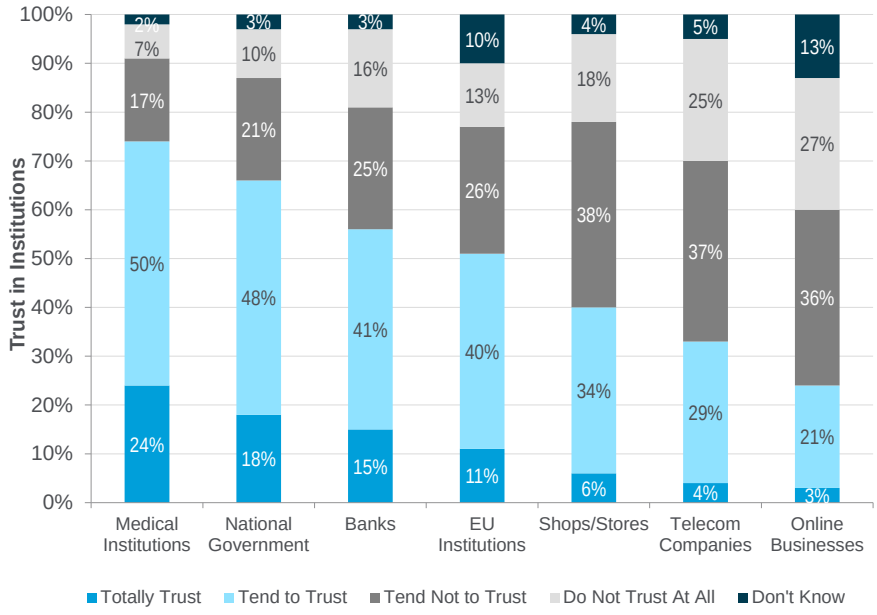


Source: TrustE

In practice, though, attitudes to privacy are more complex than the headline figures suggest. Consumers actually tend to hold different views depending on the type of information being shared and on who is collecting and using the data.

Survey work from Eurobarometer in 2015, for example, shows the tendency of consumers to trust organizations collecting information differs in different use cases. As per the chart below, 74% of EU citizens polled indicated they either totally trust or tend to trust medical institutions with data, while only 24% trust online businesses. A separate study done by the Scottish Government in 2013 found 'near universal acceptance of public bodies having access to data' as public sector organizations deliver public benefits and are seen to promote the 'public good'.

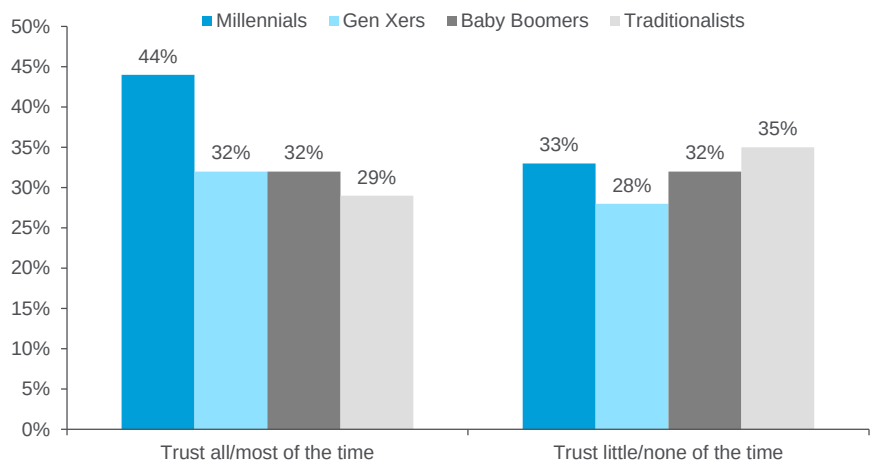
Figure 35. Tendency of Consumers to Trust Different Institutions With Personal Information, 2015



Source: Eurobarometer

Looking at differing attitudes to privacy and personal data by age group, you would naturally expect the more tech-savvy Millennials to be less concerned about online privacy vs. the older generations. This is indeed the case as 44% of Millennials trust companies to keep their personal data private compared to 29% of Traditionalists. However, this data still points to the majority of those in all age categories not having implicit trust in companies to keep data private. The difference in attitudes between the Millennials and Traditionalists (those aged over 61 years) is not as wide as one might expect.

Figure 36. Trust in Companies to Keep Personal Information Private (by age group) – Gallup, 2016



Source: Gallup

Digging in more detail to survey work around attitudes to privacy, the U.K. ICO sub-divides the questions about privacy and data protection into five key areas:

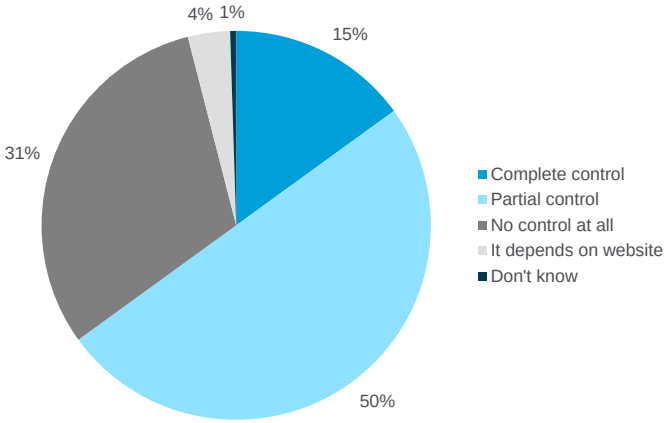
1. Control over personal data
2. Transparency on what data is being used for
3. Willingness to trade privacy
4. Security of data
5. Right of access and right to delete

Going through these topics in a bit more detail:

Control of Data

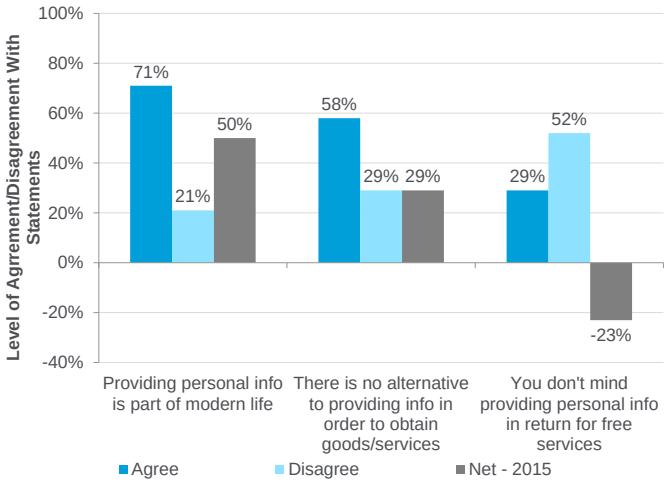
There are a number of themes that come out of the myriad of surveys that have been conducted on the topic of control of data. As we show in the charts below based on a Eurobarometer survey of EU citizens, in general consumers appear to accept that handing over data is part of life and that it is part of the bargain when it comes to obtaining goods and services online. This said, the amount of control that consumers feel they have over their data is comparatively low and while there is an acceptance that it is sometimes necessary, it is not exactly welcomed. The ICO in some of its focus groups found that many consumers perceive providing data as a 'necessary evil' and this feels about right.

Figure 37. How Much Control Do You Feel You Have Over the Information you Provide Online? – Eurobarometer 2015



Source: Eurobarometer

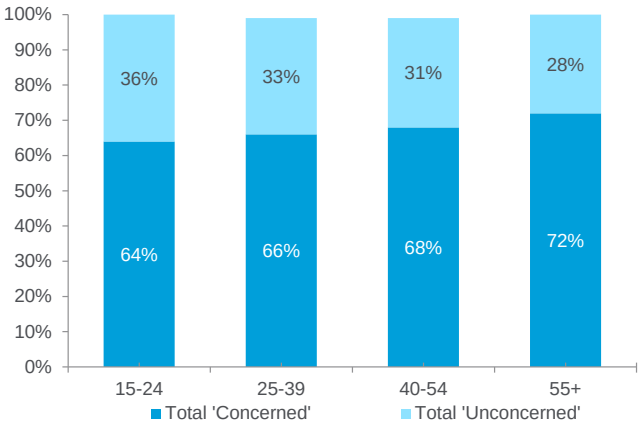
Figure 38. Attitudes to Sharing Data – Eurobarometer 2015



Source: Eurobarometer

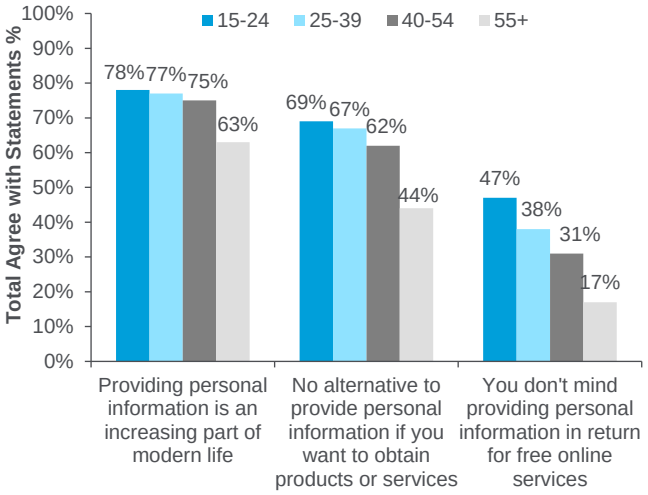
There is very little difference in viewpoint between the younger and older generations in relation to how much control they feel they have over information provided online. Across all the age groups at least 64% are concerned about not having complete control. However, the younger age groups appear to be more accepting of the idea that handing over data is part of modern life, and are much less likely to oppose providing personal data in exchange for free online services. The fact that the use of Internet-connected devices is much more engrained in everyday life for younger people is probably a key reason.

Figure 39. How Concerned Are You About Not Having Complete Control Over the Information You Provide Online? – Eurobarometer, 2015



Source: Eurobarometer

Figure 40. Attitudes to Sharing Data – Total in Agreement - Eurobarometer, 2015



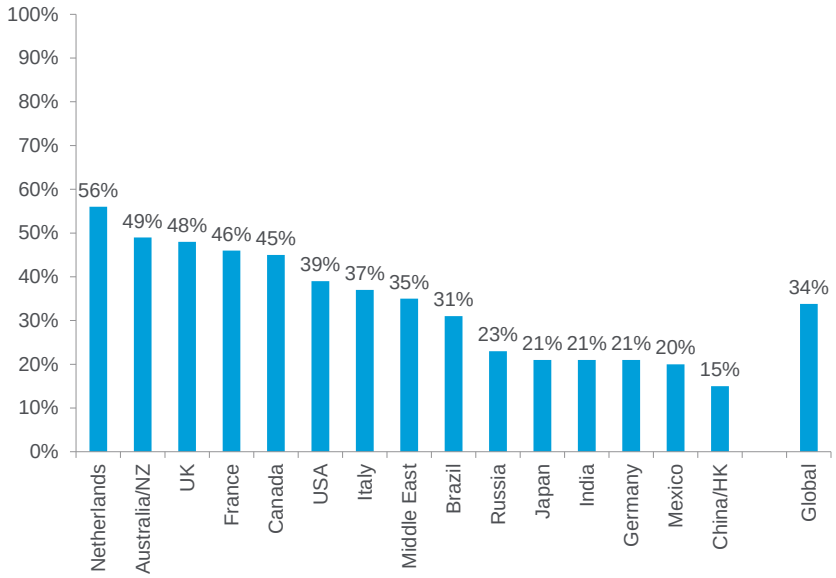
Source: Eurobarometer

Transparency in Data Usage

Historical survey work tends to show that overall levels of trust in organizations collecting data is comparatively low with many consumers (70% in a 2011 Eurobarometer survey) of the view that data is often used for reasons it was not originally collected for. As above, this does differ depending on the type of organization collecting the data and perceptions of its eventual use.

What is striking, though, is that consumers don't always help themselves. As Figure 41 below (which is based on an EMC survey) shows: a third of users worldwide actually don't even bother to read privacy statements when subscribing to an online service.

Figure 41. Propensity to Read Privacy Statements Globally, 2015 (% unlikely)

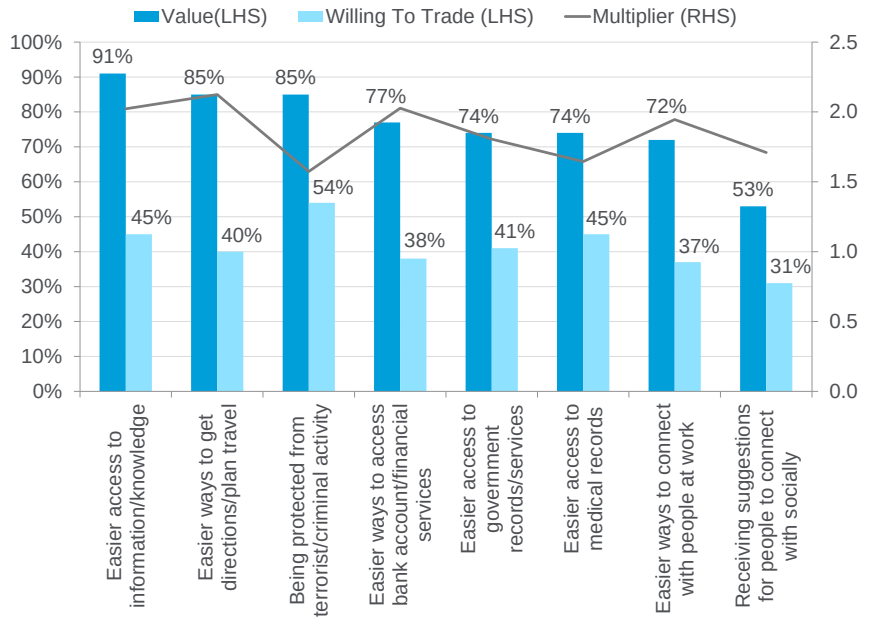


Source: EMC

Willingness to Trade Privacy

As the ICO points out there are a number of surveys (e.g. Sciencewise and Symantec) that suggest consumers fail to see the benefits of sharing data. We suspect this is probably too simplistic. As an EMC survey of global consumers in 2014 showed, the perceived 'value' of certain goods and services – e.g., easier access to information, being protected from terrorism etc. – is quite high. What is low is the willingness to trade privacy for these services. We show this in Figure 42. One aspect of this that is intriguing is the suggestion in EMC's work that levels of trust – or at least relative willingness to trade privacy – are higher for public bodies doing work for the public good than private companies exploiting data for commercial uses.

Figure 42. The Value of Convenience & The Willingness to Trade Privacy for Convenience (EMC Global Survey)



Source: EMC

Security of Data and Right of Access/Right to Delete

As the RAND Institute highlights, 17.6 million U.S. citizens were victims of identity fraud in 2014 according to Bureau of Justice statistics, up from 16.6 million in 2012 and with each large public data breach, awareness of data protection as an issue rises. A Symantec survey in 2015 indicated that 57% of consumers were worried that data is not being kept safe by organizations and 88% felt that keeping data safe was a factor of importance when choosing an organization with which to shop.

Perhaps reflecting this, the general consumer appetite to be able to access and even delete data held by organizations is high. A Eurobarometer survey in 2011 found that 75% of users would like to be able to delete personal data held on a website should they choose to do so.

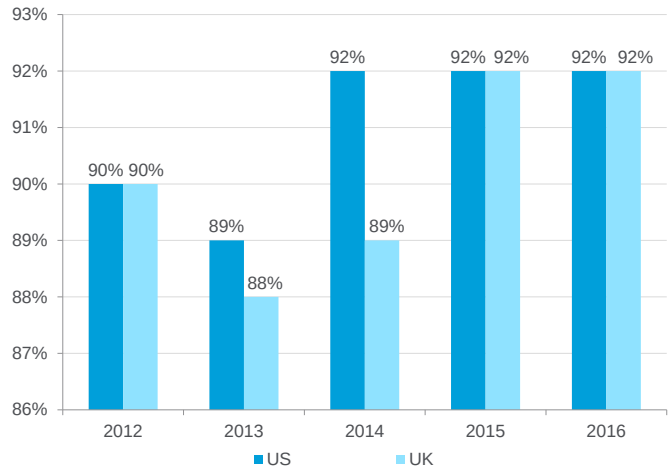
Attitudes Are Not Set In Stone; They Differ Region by Region and Change Over Time

While one can get a snapshot of consumers' attitudes toward privacy and data protection at a moment of time, in practice these attitudes are constantly evolving. Moreover, attitudes vary country by country.

In terms of how attitudes have evolved over time, unfortunately there are not many significant longitudinal studies on attitudes toward privacy. This said, both TrustE and Eurobarometer have done repeated studies over time with some continuity in terms of what was being asked. With TrustE we can get a sense of how worried U.K. and U.S. consumers are/have been about privacy over time and the implication is that they are mildly more concerned now than a few years ago, although we have to note that even then general levels of concern were comparatively high. The Eurobarometer surveys allow us to track trust in institutions and we can see that this, on average, has been steadily reducing.

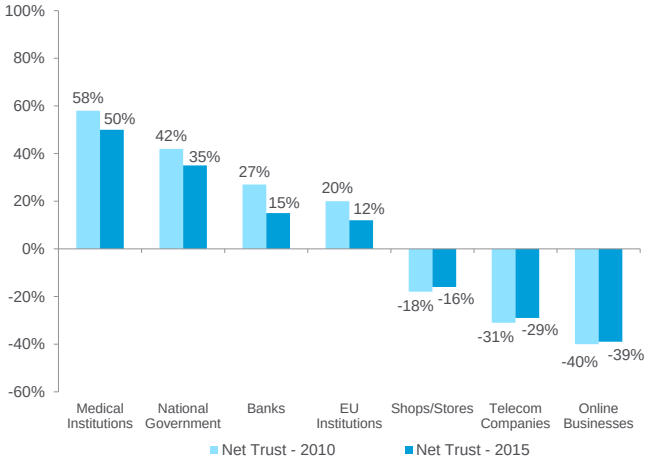
The implication is clear in our view: privacy is becoming more of an issue over time.

Figure 43. Proportion of U.S./U.K. Consumers 'Worried About Privacy', 2012-2016



Source: TrustE

Figure 44. Net Trust of EU Citizens in Institutions With Regard to Privacy, 2010 vs. 2015



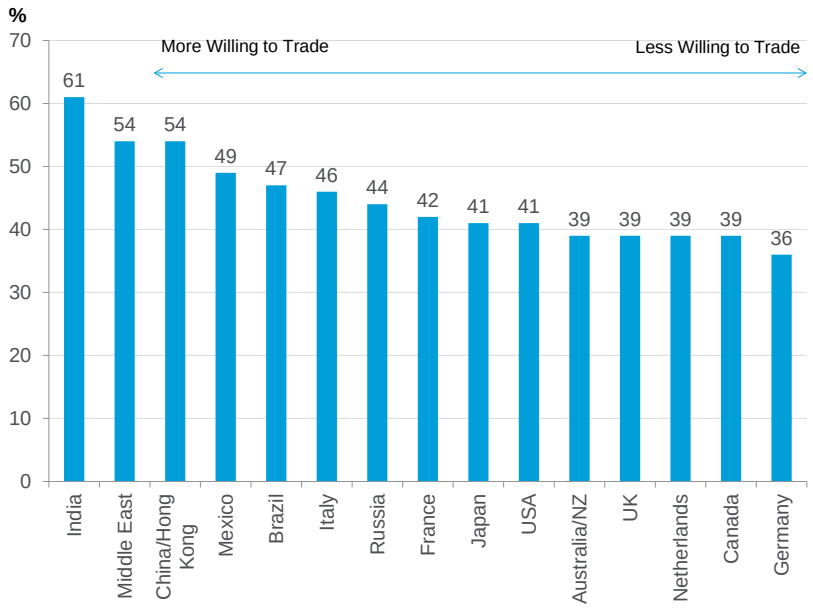
Source: Eurobarometer

But even here we are making a relatively blanket assessment based on just a handful of markets – the U.S. and U.K. in the case of TrustE and the EU in the case of Eurobarometer. We should consider whether attitudes differ across different countries and regions.

Here the survey work conducted by EMC is tremendously useful and allows to get just such a snapshot. In Figure 45 we show the results in terms of 'willingness to trade privacy for convenience' and the implications are quite striking.

The EMC study suggests that in general so-called emerging markets appear to be more willing to trade privacy for convenience while more developed markets appear to be less comfortable with the trade-off.

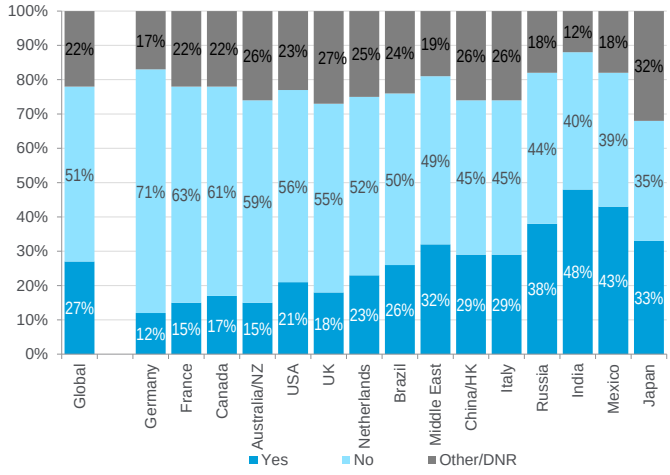
Figure 45. Willingness to Trade Privacy for Convenience – A Global Index



Source: EMC

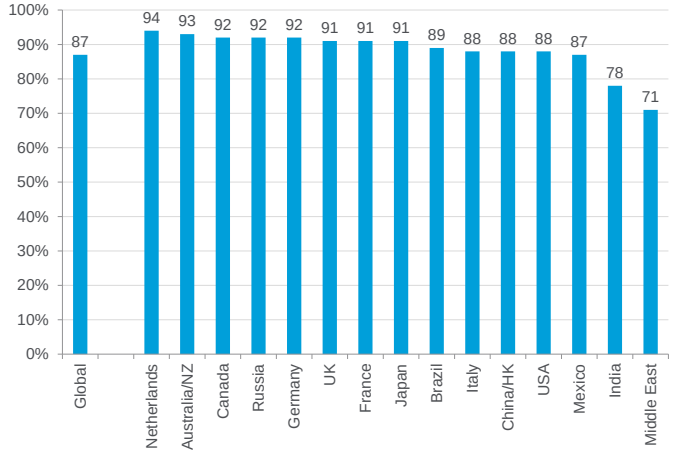
Digging into this in a bit more detail, we see that in some European markets, and in particular Germany and France, not only is there a relatively profound resistance to the concept of trading privacy for convenience (71% of German consumers and 63% of French consumers wouldn't vs. a global average of 51%), but this appears to be linked to a relatively high level of support for the idea of legislation to prevent business from trading in data (92% support in Germany and 91% support in France vs. global average of 87%).

Figure 46. Willingness to Trade Privacy for Convenience – Yes vs. No vs. Don't Know (Response by Geography)



Source: EMC

Figure 47. There Should Be Laws To Prohibit Businesses From Buying & Selling Data Without Consent (Response by Geography)



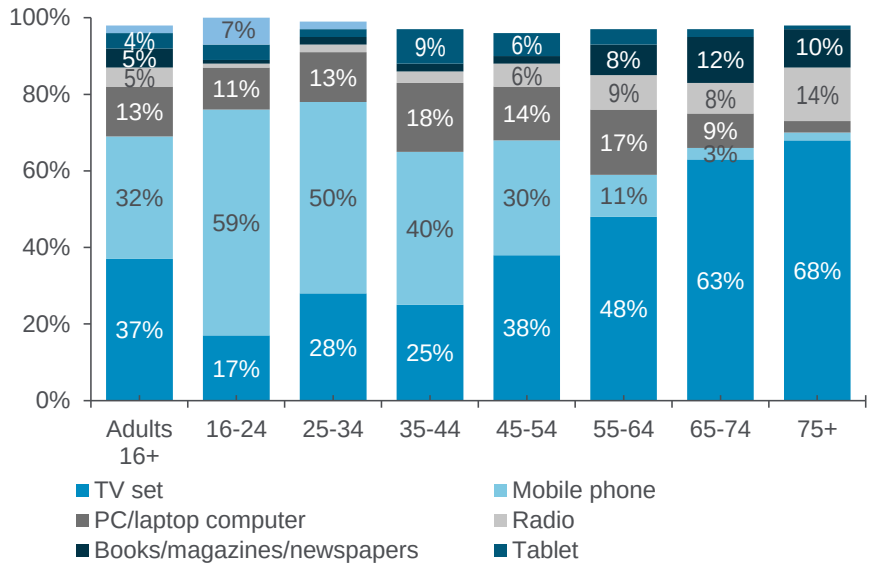
Source: EMC

Attitudes to Privacy Don't Appear to Impact Usage/Behavior

So what have we learned so far? At least based on many of the surveys available worldwide and over time, consumers appear to be deeply concerned about privacy and data protection and this should have an impact on the way that they interact with companies with respect to their personal information.

The problem is that it doesn't. A number of commentators talk in depth about this phenomenon but we can see it in usage statistics worldwide. The data below is based on the U.K., but it confirms that usage of devices connected to the Internet is increasingly embedded in behavior, especially for Millennials; the mobile phone would be the most missed device for >50% of Millennials.

Figure 48. Most-Missed Media Device by Age in the U.K.

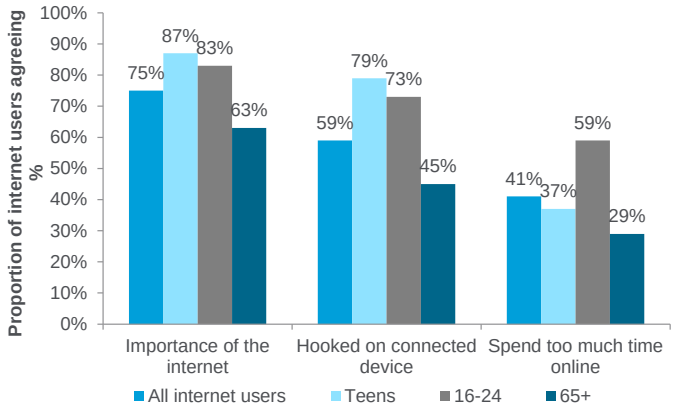


Source: Ofcom

We can see a similar disconnect when it comes to data breaches. The RAND Institute has done extensive work looking at the impact of data breaches on consumer behavior and some of the findings are quite striking.

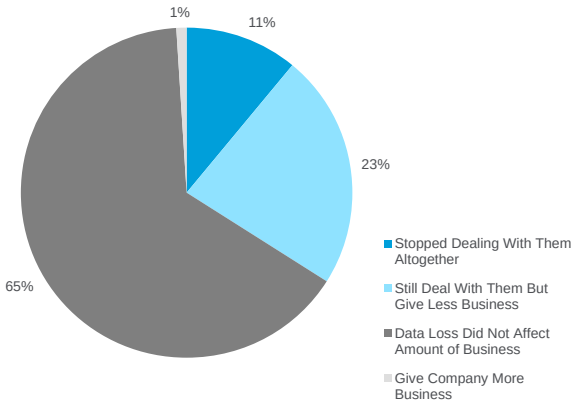
In a 2016 study, the RAND Institute estimates that up to 64 million U.S. citizens have, at some point, suffered from a data breach. Despite this, the willingness to take action is comparatively low. As per Figure 50, only 11% of respondents to a RAND survey indicated that a data breach led to them ceasing patronage of the organization involved. Meanwhile, 65% indicated the data loss did not affect at all the amount of business given to the offending company.

Figure 49. Attitudes Towards the Internet & Connected Devices in U.K.



Source: Ofcom

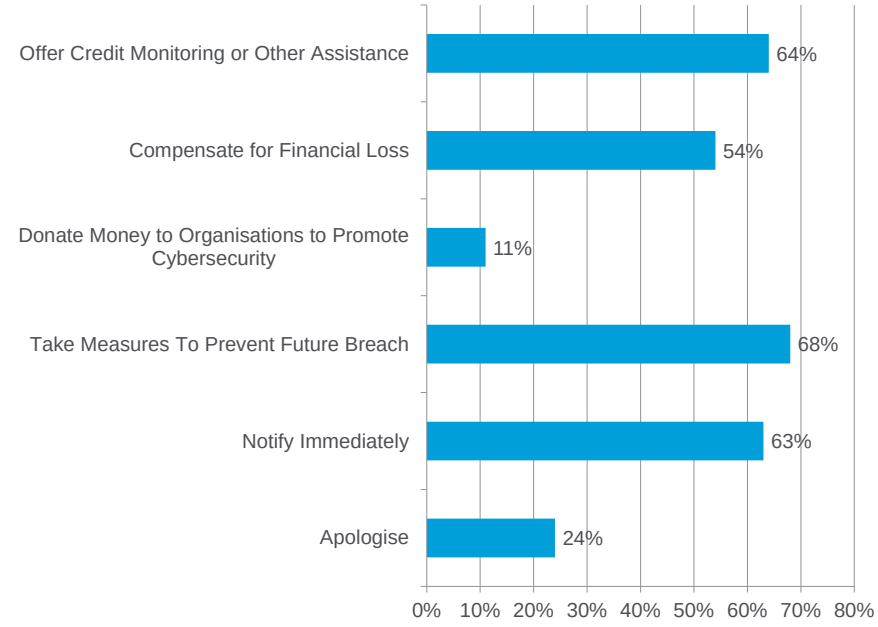
Figure 50. Consumer Patronage of Company After Most Recently Notified Breach



Source: RAND Institute

Similarly, when polled on what actions could be taken by companies in response to a data breach, more consumers suggested they would be satisfied with (1) measures taken to prevent a repeat (68%); (2) free credit monitoring or other service to monitor whether data is misused (64%); and (3) that companies notify consumers immediately (63%) than would be with direct compensation for any financial loss (54%).

Figure 51. Satisfaction with Following Breach Response (% Greatly Satisfied)



Source: RAND Institute

So, while we again have to be careful about extrapolating from a relatively small group of surveys, we are forced to reach the conclusion that while major breaches potentially raise awareness of the importance of privacy and data protection – and potentially even harden attitudes toward it – this doesn't appear to significantly alter behavior.

Implications: Do What I Say Not What I Do – Governments and Regulators Likely To Pick Up the Slack

EMC describe consumers as living in a 'world of paradoxes' and, in short, their conclusion seems apt. The ICO in the U.K. also reach a similar conclusion. The main planks of this are as follows:

- First, it is quite clear that while consumers typically value a lot of the goods and services enabled by the digital world, they are also nominally unwilling to forego personal privacy. EMC call this the 'We Want It All' paradox and, again, this seems apt.

- Second, although consumers are generally aware of privacy issues and profess themselves to be concerned about them, they also seem to take limited direct action to address these issues either ex ante or indeed post hoc.

What does this mean? We think there are a number of signals that these behaviors generate that have consequences for the broader ecosystem:

- For companies, the signal this kind of behavior potentially gives is that the consequences of poor performance are not as severe as they might have thought, as long as they are thorough with respect to prompt breach notification and have a clearly stated commitment to addressing the source of the breach (although the RAND Institute work also shows that 20% of data breaches are never resolved). Of course the danger is that the approach to privacy and data protection becomes (a) reactive and (b) largely cosmetic.

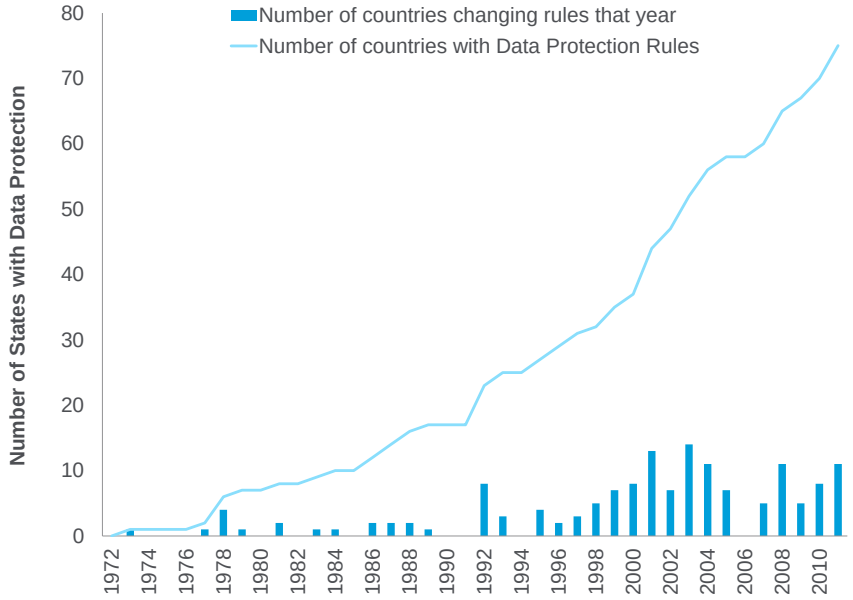
- For regulators, the clear signal from consumers is that they want – or, at least, need – an external agent to hold companies/organizations that use personal data accountable because consumers are unlikely to do it themselves. To the extent that businesses and organizations cannot be left to self-regulate, then the onus falls on the government to pick up the slack. Or put another way, if consumers won't look after themselves and companies won't proactively manage risk, then government/regulators will have to do it for them.

And this, we think, is the context within which we should consider government regulation of privacy and data protection, in general, and the EU's GDPR in particular. It is this we turn to in the next chapter.

ePrivacy and Data Protection Regulation: A History

Globally, the number of countries with some form of modern data protection standards has increased from 0 in 1970 to over 100 in 2016.

Figure 52. The Number of Countries With Domestic Data Protection Regulation



Source: Taylor Wessing. Greenleaf, Graham, Global Data Privacy Laws: Forty Years of Acceleration (October 10, 2011). Privacy Laws and Business International Report, NO. 112; UNSW Law Research Paper No.2011

This has been predominantly driven by a wish to regulate and protect citizens' data while exploiting the gains from transnational data flows. The cost has been an increase in regulatory heterogeneity.

Data Minimization: The organization should not collect or hold more data than is necessary to fulfil the purpose the data was initially collected for.

During the 1960s, privacy concerns grew. The post-industrial information revolution and the growing use of personal information by governments[13] generated new data processes and new bases for concern. As a result, in the late 1960s and early 1970s, governments began to consult on the issue. For example, in 1972 in the U.K., the Younger Committee first proposed the principle of Data Minimization; the idea that a data controller should not collect more data than is necessary for their purposes.

OECD: A 35 member intergovernmental economic organization that aims to stimulate economic development and world trade.

Since 1980, the development of data protection has been centered in the international sphere, as the Organisation for Economic Co-operation and Development (OECD) adopted guidelines governing the protection of privacy. These proposals were based on eight basic principles, which were aimed to protect individual rights, support transborder flows of personal data and provide a uniform minimum standard.

[13] Shimanek, Anna E. (2001). "Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles". Journal of Corporation Law. 26 (2): 455, 462–463

Summary of OECD Principles

Collection Limitation – There should be limits to personal data collection and it should be collected with the knowledge or consent of the data subject, where appropriate

Data Quality – Personal data should be relevant to the purposes for which they are to be used

Purpose Specification – Personal data should only be used for the purpose stated and not for any other purposes, unless specified

Use Limitation – Personal data should not be disclosed, made available or used for other purposes without the data subject's consent or by authority of the law

Security Safeguards – Collected personal data should be kept secure from any potential abuses

Openness – General openness about developments and practice in relation to personal data and data subjects should have means to establish main purpose of use and identity of who is collecting their data

Individual Participation – Data subjects should be allowed to access their data and make corrections or erase the data

Accountability - data collectors should be accountable for compliance with the above principles

Since their publication, these rules have been highly influential. They have set the standard and influenced the development of national data protection regimes in New Zealand,[14] Australia, Canada, and South Korea.

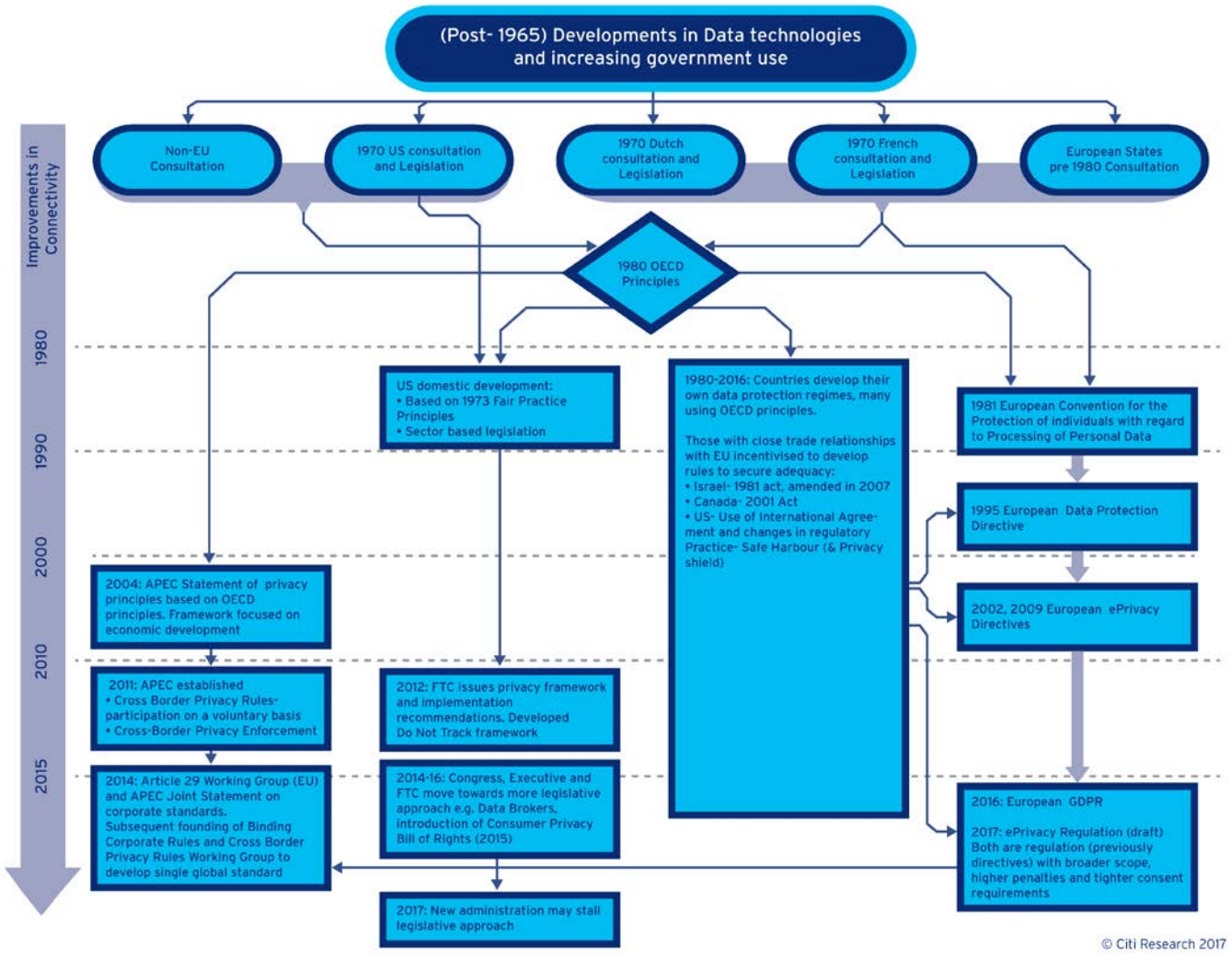
However, by time of their adoption, 24 OECD member countries, including Germany, France, and the United States, had already adopted some form of national data protection legislation. Since 1981, Europe has been attempting to implement a more uniform approach. In 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data required states to implement legislation providing for personal data protection. In 1995 the European Data Protection Directive set out more specific outcomes that must be achieved. The issue was that both use national legislation as their enacting instrument. Common aims were ultimately distorted by differing national approaches.

The varying approaches extend beyond Europe. Argentina, for example, has some of the strictest data protection rules in the world.[15] The United States has generally taken a more principles-based, collaborative, approach. The focus of the Asia-Pacific Economic Cooperation (APEC) countries is on economic outcomes and realizing the benefits of transnational e-commerce.

While Europe has taken the most prescriptive approach, it has also struggled the most with the lack of uniformity across its member states. The gap between data protection regimes globally remains as wide as ever. The increasing need to protect consumer privacy rights appears to be leading towards the development of a legalistic framework in Europe, while in the U.S. the election of Donald Trump (and an all-Republican House and Senate) indicates a possible shift towards deregulation. This presents a challenge for corporates and authorities.

[14] Adequacy decision: 'Heavily influenced' by OECD
[15] Forrester

Figure 53. ePrivacy and Data Protection Regulation Timeline

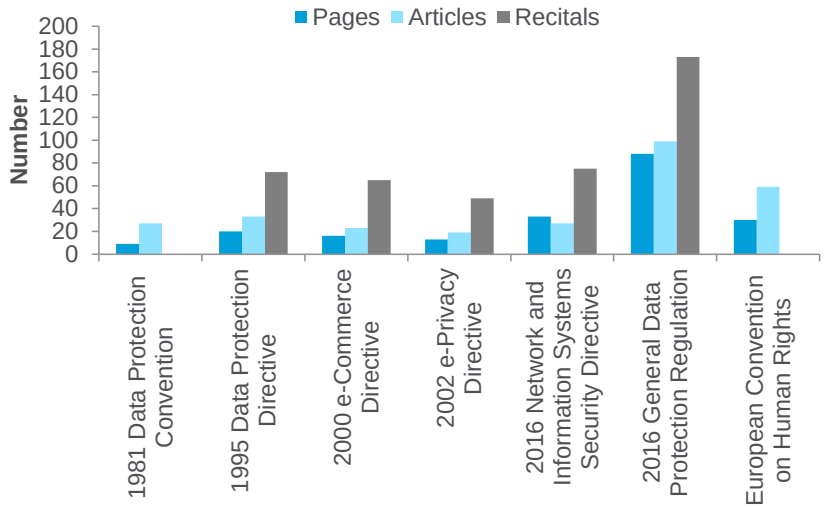


Source: Citi Research

Deep Dive into the General Data Protection Regulation (GDPR)

On April 27, 2016 the European Council, Commission, and Parliament jointly published the final version of the General Data Protection Regulation (GDPR), which will become legally binding in all EU member states on May 25, 2018. Until Edward Snowden's revelations about the level of government surveillance in some countries in 2013, the legislation was facing tough opposition. The Snowden event changed the course of events dramatically and after four years of consultation/negotiation, the final agreement was set. The GDPR is roughly four times the length of the 1995 Data Protection Directive (95/46/EC) (DPD) and it replaces and contains almost twice as many recitals (interpretative clarifications).

Figure 54. Comparison of the Length of European Data & Privacy Related Directives/Regulation



Source: Citi Research

The GDPR will apply to all companies based in the European Economic Area (EEA), and to an increasing number beyond. With potential fines ranging up to 4% of global annual turnover, this is no longer a risk corporates and investors can afford to ignore.

The GDPR *is not* a fundamental revision of the 'European approach' to data regulation but a tightening of existing themes. This is not to understate the degree of change, but rather to point out that the GDPR does not constitute a regulatory 'about turn.' The European Commission has attempted to highlight the economic benefits, claiming €2.3 billion of economic gain from implementation of the GDPR, stemming mainly from harmonization of data regulation. This has been contested by several critics, authorities and corporates e.g. the U.K. Ministry of Justice quantifies the net cost of the GDPR at £80m-£320m.

Directive: EU legislative instrument in which common goals are agreed at the European level and then realized by member states through national legislation.

The first major difference from the existing setup is that this is regulation rather than a directive (which it was in 1995), which means it will automatically become law in each of the EU member states. This affords member states less flexibility in implementing it and is another attempt to institute a uniform approach to data protection in Europe.

European Data Protection Supervisor, Recital 7: *The adoption of a Regulation should ensure consistent and homogenous application of data protection rules throughout the Union, thus eliminating divergences hampering the free movement of data within the internal market.*

Derogation: The relaxation of a law in a specific context. Under the GDPR, these are areas where the national authorities can define terms.

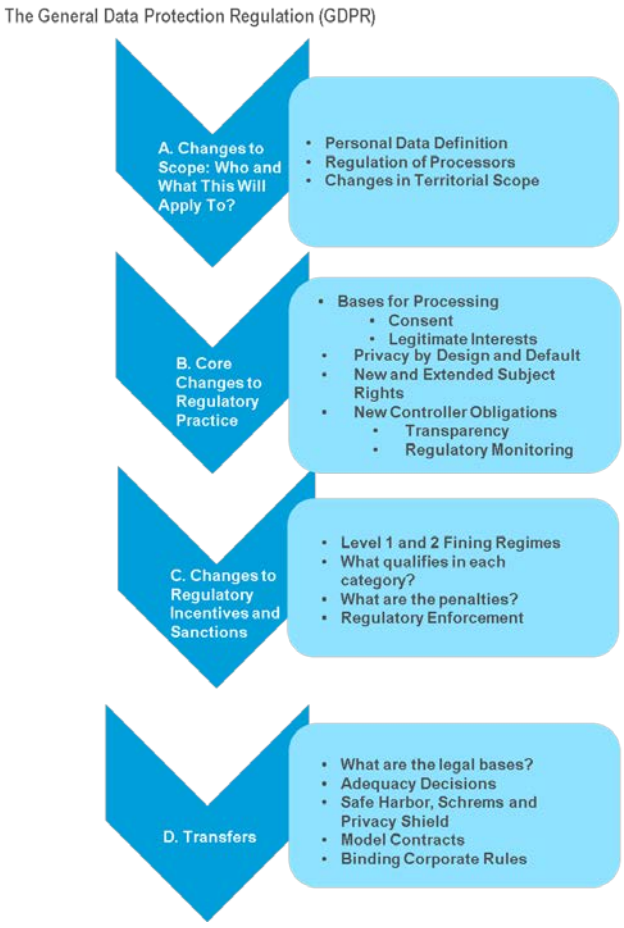
The GDPR places a greater emphasis on individual rights than the previous approach, which is really at the heart of the legislation.

In material terms, the GDPR clarifies a more expansive definition of personal data and directly regulates new actors for the first time. In territorial terms, the GDPR will regulate any entity established, or proactively offering goods and services within the European Economic Area (EEA). The previous requirement was only applicable to those companies established and/or processing data in the EEA.

There are roughly 51 so called 'derogations' in the regulation — these being cases where the regulation leaves it to national authorities to define the precise terms of the regulatory regime which means it will stop short of full uniformity. Large portions of the final regime remain undefined. While the Article 29 Working Party is publishing guidelines on 11 specific areas of the GDPR, this means that even upon implementation in 2018 there is scope for confusion.

We have broken the GDPR into 4 key areas and discuss each in turn.

Figure 55. Key Changes Arising from the GDPR



Source: Citi Research

A. Changes in Scope - Who and What Will This Apply to?

Data Considered Personal

Data subject: A living individual to whom personal data pertains.

Under Data Protection Directive Article 2 (a), personal data was defined as '*… any information relating to an identified or identifiable natural person ('data subject')*' where an identifiable person was defined as:

'… one who can be identified , directly or indirectly , … by reference to an identification number or to one or more factors specific to his physical, physiological, mental , economic, cultural, or social identity.'

The GDPR largely maintains the above definition of personal data but it expands on the type of data used in the context of identifying individuals (additions in bold):

'*…an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,* ***location data, an online identifier,*** *or to one or more factors specific to the physical, physiological,* ***genetic****, mental, economic, cultural, or social identity of that natural person.'*

What also has changed is that no longer does it have to be shown that data itself is *specific* to an individual's identity (e.g. a personal ID number), but rather that it could be used in conjunction with other resources to derive it.[16] The implication is that data that might not qualify as personal data for one controller but might for another when one is in possession of complementary data and such resources as to allow an individual's identity to be derived. Regulators will now have to consider the context into which data is transferred and used.

Greater Number of Organizations Falling Under the Regulation

The GDPR, for the first time, will regulate data processors directly. Previously the data controllers were the only ones directly subject to the Data Protection Directive. Article 3 of the GDPR states that the regulation will apply '*…to the processing of personal data in the context of the activities of an establishment of* ***a controller or a processor*** *in the Union…*'

Data Controllers - These are '*…bodies which, alone or jointly with others, determine the purposes and means of the processing of personal data.*'

Data Processors These are '*…bodies which, alone or jointly with others, process personal data on behalf of the controller.*'

An example of how this could have ramifications is in cloud computing where software services, platform services, and infrastructure services are provided by different organizations. In this case, owners of the data infrastructure, e.g., Amazon's AWS, are often considered to be sub-processors to the data activities of companies using their hardware. The GDPR would see them both directly regulated, and hence might see the owners of the infrastructure penalized if users utilize their infrastructure for illegitimate means. For large global corporates which may outsource to thousands of different vendors, many of which could fall under the category of data processor, it increases the burden on both parties. According to a report by Netskope, 90% of its customers use 'infrastructure as a service' (IaaS), with an average of four services used.

[16] More guidance is given in the Council of Minister's Recital 23: … *account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual directly or indirectly. To ascertain whether means are reasonable… account should be taken of all objective factors, such as the costs of and the amount of time required for identification…*

Territorial Scope; Focus Is on Origin of Citizen Not Corporate

Lastly, the GDPR dramatically expands the territorial scope of European data regulation. The 1995 Directive applied to data controllers established in the EEA and those using processing facilities in the EEA. Article 3 of the GDPR expands this scope significantly. Data collection and processing activities will be subject to European regulation if such activities involve European Nationals' data and the 'monitoring' of European Nationals and/or involve European Nationals' data and the 'offering' of goods and services in the EEA. Any company tracking European consumers or proactively offering goods/services in the EEA (factors such as a change of language and the choice of currency for payment processing being relevant.[17]) will have to comply with the requirements of the GDPR.

The critical point is that the location of the controller and processor is no longer relevant.

Figure 56. Change of Emphasis on Location of Data Processors

1995 Directive	2016 GDPR
Article 4(1)(a): *Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where the processing is carried out in the context of an establishment of the controller on the territory of the Member State…*	Article 3(1): *This Regulation applies to the processing of personal data in the context of the archives of an establishment of a controller or a processor in the Union,* ***regardless of whether the processing takes place in the Union or not****.*

Source: Citi Research

[17] Recital 20

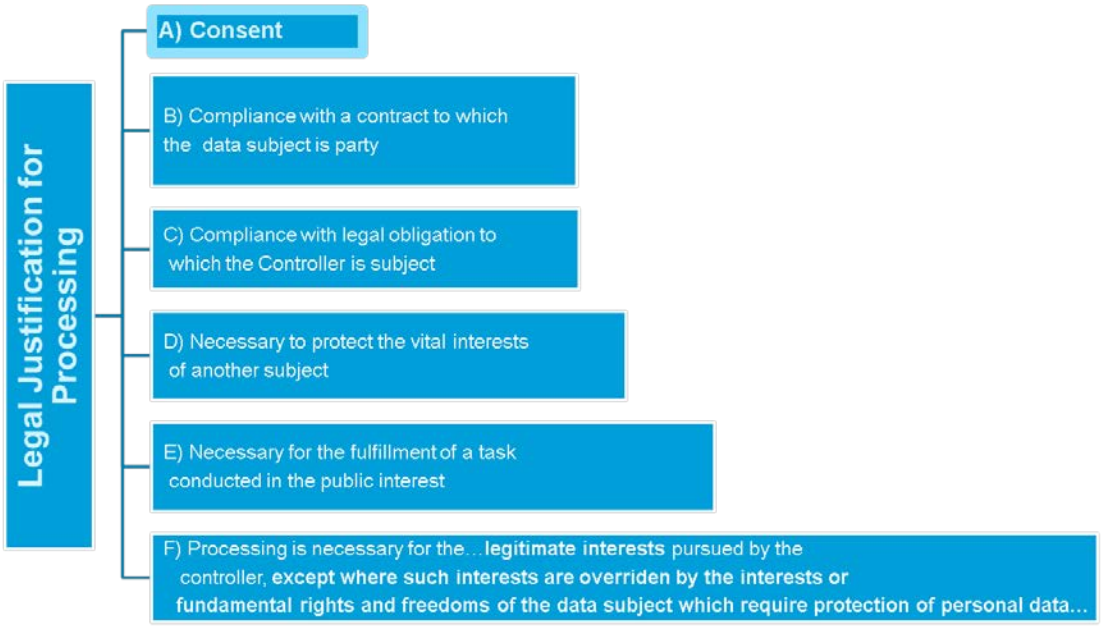
B. Changes to Regulatory Practice

Given the GDPR's emphasis on individual rights, the legislation also requires a demonstration of compliance to the data subjects and regulators.

Justifications for Data Collection and Processing

According to the GDPR, there are six bases for legal processing of personal data.

Figure 57. Justifications for Data Collection and Processing



Source: Citi Research

These are the same as the bases specified under Article 7 of the Data Protection Directive. However there are changes to the precise specification of many of these justifications. The most common justifications, and those that can be used at the effective discretion of private organizations, are **Consent** and **Legitimate Interests**. These are also areas of great change and hence we look at these in more detail.

Consent Requirements Tightened Up

The GDPR characterizes consent as the following:

Article 4(11)…*freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.*

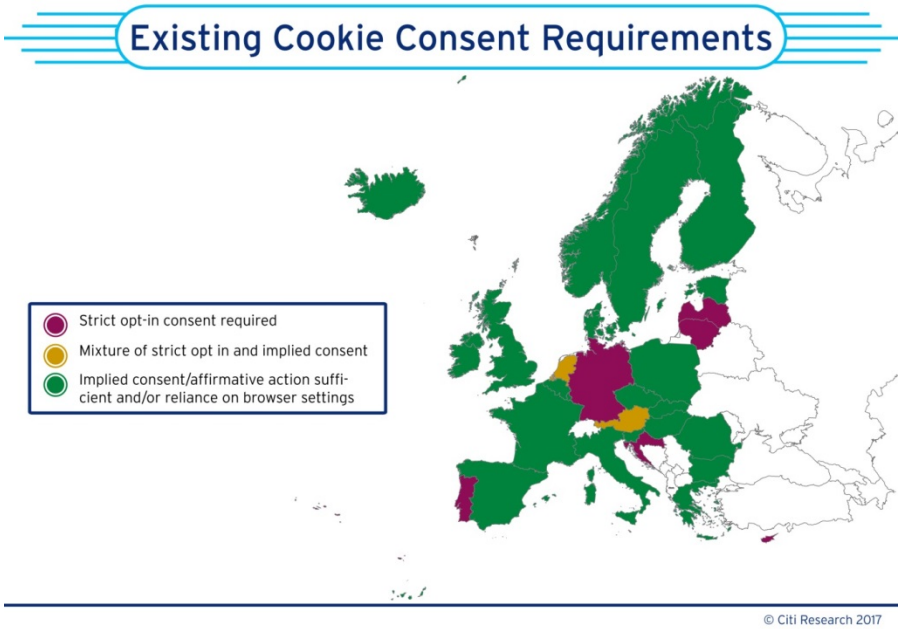
The GDPR attempts to further specify the conditions necessary for consent in order to increase consumer control over what, and how, personal data is used. The GDPR makes two main changes:

1. Standards for consent bolstered under the GDPR

ePrivacy Directive – A European directive first passed in 2002 and subsequently amended in both 2009 and 2016. Its aim is to ensure privacy in online communications. It deals with regulation in a range of areas including the confidentiality of data traffic and the use of spam. Crucially, since 2009, it has regulated the use of cookies.

Consent was one of the most contentious elements of the regulation negotiations, with agreement only being reached in the final rounds. Under the Directive regime, standards of consent varied across Europe. The Data Protection Directive specified that consent had to be 'unambiguous'. Subsequently, the 2009 ePrivacy Directive (09/136/EC), which governs electronic communications, introduced the requirement that clear and comprehensive information be provided to the data subject before consent can be acquired. Explicit consent has only been adopted by a handful of European countries. For most, such as in the U.K., users have become used to the appearance of cookie banners popping up when landing on a webpage and specifying that, on the basis of continued use of the website, consent for dropping cookies will be assumed.

Figure 58. Existing Cookie Consent Requirements in the European Union



Source: FieldFisher (April 2015), Citi Research

The GDPR stops short of uniform 'explicit consent' for all personal data, but does tighten up consent requirements. Under Article 6, it requires *proactive expression of consent* and consent must be unambiguous and demonstrable. Recital 32 states that '*… the use of default options which the data subject is required to modify to object to the processing, such as pre-ticked boxes, does not express free consent…*' but consent can be given through "*another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data*".

What does this mean practically? In the case of cookie banners, for example, the proactive use of a tick box/ acceptance button could be used as a basis for consent. Whereas today, simply having a page open could be used as a basis for consent, under the GDPR, demonstrability requires proactive action. The possibility of managing consent through browser settings remains (and has been suggested as the key mechanism in the latest draft of the ePrivacy Regulation), though the same 'proactive' standard will be required. Combined, these will constitute a meaningful tightening of consent requirements.

Secondly, consent will also have to be given to each form of tracking independently. Currently, many permissions are 'bundled' within a single consent option, sometimes with scope even beyond data processing. The GDPR changes this, rendering such consent decisions illegitimate. Article 7(2) of the GDPR specifies that '*consent shall be presented in a manner which is clearly distinguishable from the other matters.*' In the recitals, the meaning of this is further specified, '*…Consent is presumed not to be freely given if it does not allow separate consent to be given to different data processing operations…*' As a result, consent tools will increasingly have to allow consumers to opt out of individual tracking operations.

Sensitive Personal Data is defined as those categories of data that run a particularly high risk of harming an individual's rights or interests if the data was to be misused or leaked. This includes data such as an individual's political views, sexual orientation etc. Newly added to this category, under the GDPR, is medical and biometric data e.g. facial recognition.

Under Article 9 of the Regulation, explicit consent will apply to any collection and processing of sensitive personal data. Generally, this standard is already observed under the DPD.

There are new provisions in relation to children's personal data. Consent has to be provided from a parent or guardian for access to online services, and reasonable efforts have to be made to verify consent is from a parent/guardian. The contentious element of the regulation is that the age of a child has been raised to 16 years and under (from 13 years and under), and this was done late in the process, which makes it inconsistent with the U.S. at 13 years and under. Member states can bring down the age to no lower than 13, but this would have to be legislated for and given the GDPR will automatically come into law from May 2018, it is not clear whether this is going to be a priority for any of the member states.

As we discuss later, the proposed new ePrivacy Regulation provides a clearer (and more stringent) stance on consent requirements, and it will sit alongside the GDPR as a new piece of regulation.

2. The GDPR will increase regulation on the framing and context of the consent decision for consumers

Firstly, the current provision of data by consumers as a requirement for a service/good that we are used to today may no longer be straightforward. The regulation appears to render access to services conditional on consent to data collection illegal in many contexts. The regulation itself, under Article 7(4), says:

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

This is further fleshed out in the recitals. Here, when considering whether consent is legitimate, the European Data Protection Supervisor (EDPS) say that '*Consent is presumed not to be freely given… if the performance of a contract is made dependent on consent… and the data subject cannot reasonably obtain equivalent services without consent.*'[18] The implication, then, is not a blanket ban on the practice. Crucially, the GDPR emphasizes whether equivalent services can be reasonably obtained without consenting to tracking.

The implication is that firms providing goods and services that are seen as more integral will see this requirement policed more rigorously as it is more costly to substitute one form of provision for another. In addition, the more concentrated the market, the more difficult providers will find it to operate such practices.

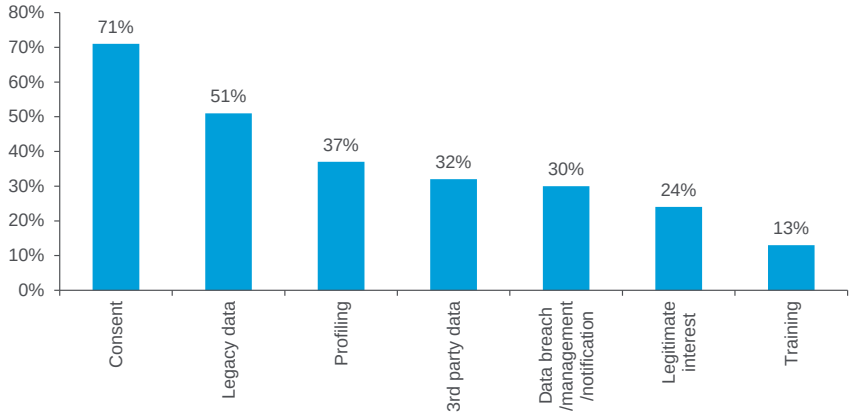
[18] Recital 34 EDPS

The overall aim here is to ensure consumers are not held at ransom and consent is not 'forced' by ulterior incentives irrelevant to the actual purpose of the data processing. Business models based on offering free services in exchange for subsequently monetized data tracking will become more difficult. One option may be offering a paid-for equivalent if they wish to ensure that they sustain a data for service revenue model.

Finally, the GDPR will also require consent to be withdrawn at any time with equivalent ease as giving consent.

Consent is the biggest concern for companies in relation to the GDPR, according to a survey conducted by the Data & Marketing Institute (DMA).

Figure 59. What Are the Biggest Concerns for You and/or Your Organisation (in Relation to the GDPR)?



Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2' Survey conducted Sept-Dec 2016

Legitimate Interest Basis for Processing Tightened Up

Legitimate interest: This is the basis for processing data under the GDPR. It allows processing without consent when it is deemed to be in the legitimate interests of the data controller. The expectations of data subjects are a consideration.

Beyond consent, the other basis on which processing is commonly undertaken is for so called 'Legitimate Interest' purposes. Legitimate interests are commonly understood to include things such as ensuring the integrity of IT networks. Another example, used by the ICO, where legitimate interests could be applicable is:

'*A finance company is unable to locate a customer who has stopped making payments under a hire purchase agreement. The customer has moved house without notifying the finance company of his new address. The finance company engages a debt collection agency to find the customer and seek repayment of the debt. It discloses the customer's personal data to the agency for this purpose. Although the customer has not consented to this disclosure, it is made for the purposes of the finance company's legitimate interests – i.e. to recover the debt.*'[19]

A legitimate interest justification for processing depends on the proposed action being proportionate to need. It must also not undermine the rights and interests of the individual whose data is being processed to an 'unwarranted' degree.[20]

[19] https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/
[20] ICO

'Legitimate interests' was a basis for processing in the 1995 Directive. While the GDPR is broadly similar in this regard, the regulation does insert a '*reasonable expectation*' condition in the considerations of whether legitimate interests justify processing. This condition specifies that a legitimate interest basis for processing should be considered more legitimate if subjects would reasonably expect, at the time of data collection, that their data would be used in this way. This small wording change could have wide-reaching implications as it may make the use of the legitimate interest basis, overall, more difficult to justify.

Privacy by Design and Default Should Be at the Heart of How Businesses Operate

Privacy by Design: Takes privacy into account from design through to execution.

Privacy by Default: The privacy settings for a new product or service are set at an appropriate level to minimise risk associated with processing and storing personal data.

This is about minimizing the use of personal data and reducing data risk where it is not disproportionately costly, essentially embedding the protection of personal data into the DNA of companies. The regulation lays out that all actions to reduce risk must be taken where no additional cost is incurred, and any additional costs incurred are proportionate to the associated risk. For example, companies will have to employ techniques such as pseudonymization of the data, which means that the identifier, e.g., name, is removed from the data so that data cannot be attributed to a specific data subject without the use of additional information, which must be kept separately (or can be deleted).

This is a feature which is central to data protection by design, and the GDPR incentivizes pseudonymization by allowing greater scope for processing beyond the initial purpose (as long as it is "compatible") if data is pseudonymized. Consequently, notifications in the instance of any security incidents will be less extensive, and where the identifying data is deleted, this limits the rights of data subjects to access, rectification, erasure, or data portability.

As we noted earlier there are ways to identify data subjects even when data appears to be pseudonymized or anonymized. The GDPR has addressed this in its Recitals (75 and 26) in which it states controllers need appropriate safeguards to mitigate the risk of reversal, e.g., encryption, privacy by design, as well as assessing the risk of re-identification taking into account cost and available technology.

Figure 60. Privacy by Design vs. Privacy by Default

Source: Citi Research

Both Privacy by Design and Privacy by Default will restrict data controllers and processors as they must, in operational and design terms, demonstrate that they have minimized data risks, maintain an internal documentation of this, and conduct a data protection impact assessment.

Giving More Rights to the Consumers

The GDPR strengthens data subjects' rights to object to processing of personal data, including an extension of some rights already present under the Directive as well as the inclusion of new ones (rights to erasure and to data portability):

- **The Right to Object** (Article 21): Data subjects now have an absolute right to object to processing of personal data, unless the controller can demonstrate the need for the processing of the data. A subject objection can only be overruled in cases where '*the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedom of the data subject.*' The onus is on controllers and processors, rather than individuals, to demonstrate their case in the event of conflict. This has the potential to be seriously disruptive, especially as processing has to be restricted immediately in the case of a complaint. More generally, the right to object is strengthened in several other areas when processing is not based on consent, in particular when data is used for direct marketing purposes. If the data subject objects to the processing for that purpose then the processing has to be stopped (no questions asked).

There are several other areas in which rights have been extended by the GDPR:

- **The Right to Exception from Automated Decision Making:** Under the GDPR, automated decision making on the basis of so called 'sensitive personal data' is only permitted if done on the basis of explicit consent and/or public interest.

- **The Right to Access your Data** (Article 15): Under the directive the data subject could access: Confirmation of processing, data used and purposes. The GDPR extends this to include additional information. The Recitals imply that companies will be required to make it relatively easy for subjects to access their data and, in some cases, controllers will have to provide remote access portals that will provide secure direct access for subjects to their data. Some of the larger corporates already have a mechanism for this, e.g., Facebook users can download a copy of the data Facebook holds about them; Acxiom has launched 'Aboutthedata.com' in the U.S. so individuals can see the information which is held about them and amend it; www.stopdatamining.me is a site in the U.S. that informs consumers how to access the information data brokers holds about them, and opt out. These are likely to be exceptions rather than the norm at this point.

Additionally, the GDPR also creates two new rights for consumers:

- **The Right to Erasure** (Article 17): 'Right to be Forgotten,' was initially brought to prominence in the 2014 case of *Google Spain v AEPD and Mario Costeja González*. The GDPR cements this right as a data subject can request all the data is deleted by a controller when personal data is no longer useful to the purpose it was initially collected and there is no longer a legal ground for processing and so forth. This is a particularly draconian restriction on controllers as they are forced to both delete data on their own servers and take '*all reasonable steps'* to notify third parties of the erasure requirement, including those to whom they may have transferred/ sold the data.

- **The Right to Data Portability:** Data subjects must be able to transfer personal data from one controller to another, e.g., consumers with a music playlist on one platform should be able to retrieve it if they want to move platforms. The different technology platforms could make this complicated in practice. Given it has taken years to be able to smoothly port a mobile phone number from one provider to another, the prospect of porting large swathes of data between providers/systems could be practically impossible by 2018.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González: This was a crucial case in the history of European Data Protection. Here, the Court of Justice of the European Union (CJEU, see above), ruled that individuals had a 'right to be forgotten' (see below). This ruling was based, predominantly, on individuals having control over their own data, and subsequent ability to largely determine what data about them was publically available.

Obligations of Those Handling Data

More Information & Transparency to Consumers

In general, the GDPR requires controllers to supply more information to subjects at every stage of data processing. In the table below we detail the information provision requirements of the DPD vs. the GDPR:

Figure 61. Transparency For Consumers – 1995 Data Protection Directive (DPD) vs. GDPR

1995 Data Protection Directive, Article 10	GDPR Article 13
Data Subject must be provided with: 1. The identity of the controller and of his representative, if any; 2. The purposes of the processing for which the data are intended ; 3. Any further information such as: • the recipients or categories of recipients of the data, • whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, • the existence of the right of access to and the right to rectify the data concerning the subject.	Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: 1. The contact details of the data protection officer, where applicable; 2. The legal basis for the processing; 3. The legitimate interests pursued by the controller or by a third party, if applicable; 4. Where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation (and adequacy status). In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: 1. The period for which the personal data will be stored; 2. The existence of the subjects rights (erasure, data portability, to object); 3. The right to withdraw consent at any time; 4. The right to lodge a complaint with a supervisory authority; 5. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

Source: Citi Research

Additionally, outside of initial collection, the GDPR also imposes more extensive informational requirements on data controllers and processors:

- When data is acquired on a third-party basis the GDPR specifies that such information must be provided within a month or when the new controller first communicates with the subject or first discloses the data to another controller.[21]
- In the event of additional processing beyond the purposes the data was initially collected, the controller has to notify the subject before such processing takes place. The logic here is to provide an opportunity for data subjects to exercise their right to object before such processing is carried out, which of course can cause delays.

Breach Notification Within 72 Hours

The GDPR specifies that a breach must be reported to the Data Protection Authority (and in some cases the individuals impacted) within 72 hours of becoming aware of the breach when '*… the controller becomes aware of a breach, which is likely to result in a risk for the rights and freedoms of individuals has occurred.*' For processors this means they will need to notify the controllers well within the 72-hour window, which could have a huge impact on the supplier relationships.

What is notable about the GDPR is risk is ultimately measured in terms of the likelihood and severity of damage to individual rights resulting from unauthorized access to personal data, or 'data breach.'

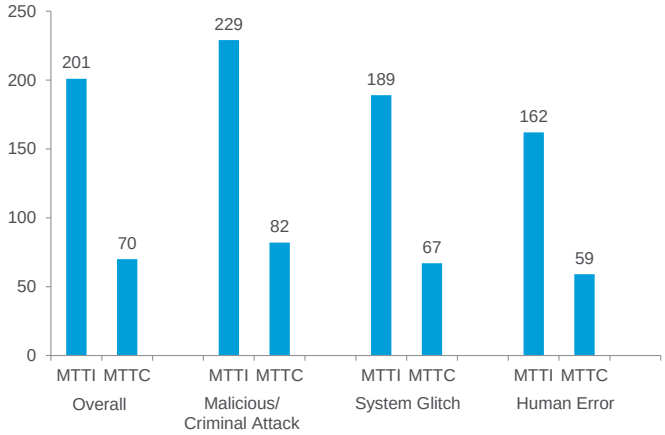
[21] Article 14(3)

Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

This requirement does mean that companies will need to adopt internal procedures to identify breaches and assess the risk in a timely manner, in order to determine if a breach is reportable.

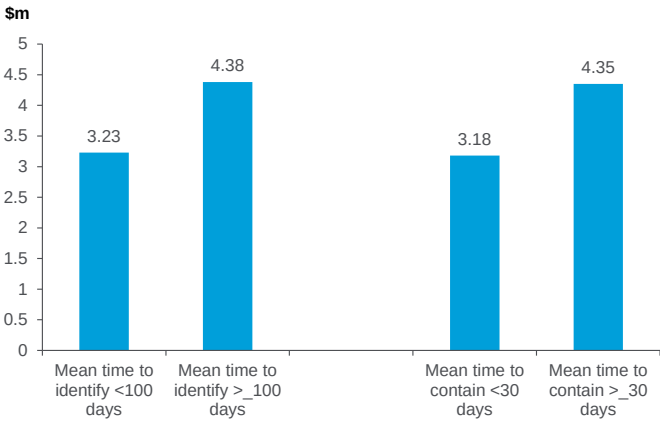
Research by the Ponemon Institute found that the mean time to identify a data breach is 201 days, and the mean time to contain a data breach is 70 days. The number of days is higher for criminal attacks, and lower for human error-related breaches. The cost of the breach (before taking into account related fines) rises the longer it takes to identify and contain a data breach.

Figure 62. Number of Days to Identify and Contain Data Breaches



Source: Ponemon Institute '2016 Cost of Data Breach Study: Global Analysis', June 2016. Sponsored by IBM.

Figure 63. Total Average Cost to Identify and Contain Data Breaches in Relation to Mean Time



Source: Ponemon Institute '2016 Cost of Data Breach Study: Global Analysis', June 2016. Sponsored by IBM.

Demonstration of Compliance

The final set of procedural requirements relates to the obligation on controllers and processors to demonstrate their adherence to other elements of the GDPR to the National Supervisory authority.

Data Controllers must keep a comprehensive internal record of all of their processing activities. This will have to include, inter-alia:

- A demonstration of necessary security (Article 21 (of the GDPR))
- A demonstration of Privacy by Design and Privacy by Default (Article 25)
- The legal basis of all processing (Article 6)
- It should also note the results of privacy impact assessments (Article 33) and privacy breaches (Articles 31 and 32)

Privacy Impact Assessments (PIA): A tool or process that organisations can use to identify and minimise privacy risks in the collection, use and disclosure of personal information.

This bookkeeping requirement includes an exception for controllers with less than 250 employees who are not processing any 'sensitive' personal data. Whether this is sufficient to protect small business from such an onerous requirement has yet to be seen.

A national supervisory authority can request access to these records at any time, and hence these records must be effectively maintained. Two new requirements stand out.

Data Protection Officer (DPO): A new position specified by the GDPR and required of companies managing higher volume or processing personal data. The DPO is responsible for ensuring compliance with regulation and is to report to the highest level of management in a company.

- Companies subject to the bookkeeping requirement must employ a Data Protection Officer (DPO), with legal expertise on issues of data protection, direct access to the highest strata of management, and can be shared between employers.
- The Requirement, under Article 35, to conduct a Privacy Impact Assessment in all cases in which so called 'high risk' processing is taking place. Processing may be deemed 'high risk' when novel processes are being used, sensitive data is being processed or the purpose of processing is particularly risky.

Areas of Clarification

While the GDPR is a very extensive piece of regulation there are several areas of ambiguity. The Article 29 Working Party has already provided guidelines on the areas of data portability, data protection officers and identifying a controller or processor's lead supervisory authority.

Throughout 2017 it will publish guidance on the following areas:

- Administrative fines
- High risk processing and Data Protection Impact Assessments
- Certification
- Profiling
- Consent
- Transparency
- Notification of personal data breaches
- Tools for international transfers

C. Regulatory Sanctions Structure; Raises Risk Profile

Fines Could Reach 4% of Global Annual Turnover

All of these more onerous and complex regulations are accompanied by an enormous increase in the scale of fines. Combined, this significantly increases the risk posed by regulation to EU data operators. Under the GDPR, Article 58 sets out the range of authority powers. Supervisory authorities have the power to:

- Issue warnings
- Impose bans
- Suspend transfers
- Order the correction of an infringement

The GDPR sets out a very prescriptive fines regime, leaving supervisory authorities with little discretion over the scale of fines. A fine should only be issued if it is **appropriate, proportionate and dissuasive**. However, in reality, the level of autonomy here is also limited. Any ruling by domestic regulatory authorities can now be challenged by other European regulators.

There are two levels of fines, with the larger being reserved for violations of consumer data rights.

Figure 64. Sanctions Regime Under GDPR

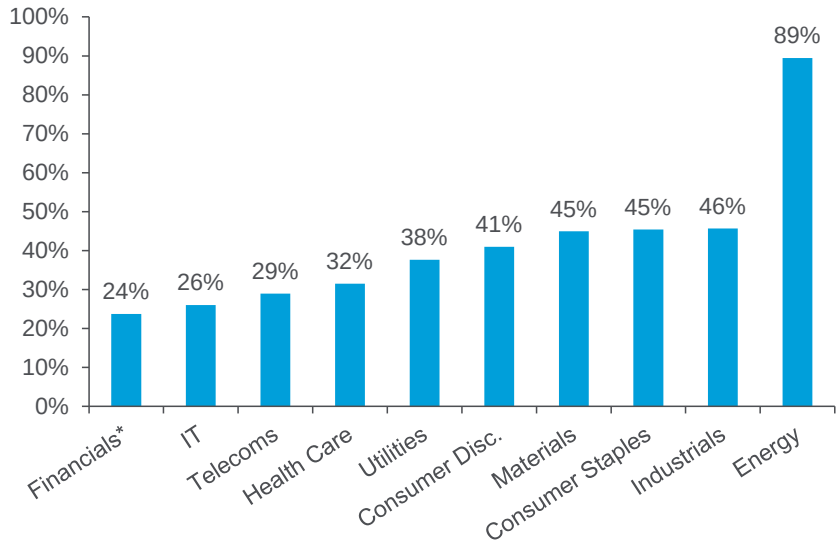
Level 1: Maximum 2% of global annual turnover or €10 million: Applicable to the violation of 19 Articles		Level 2: Maximum 4% of global annual turnover or €20 million: Applicable to the violation of 23 Articles	
Consent of a child	Identifying a data subject	The principles for processing	Conditions for lawful processing
Data protection by design/default	Joint controllers	Conditions for obtaining consent	Processing of special categories of data
Designating a representative	Processing by a processor	Provision of information to data subject	Provision of information at point of collection
Third-party processing	Record of the processing	Data not obtained from the data subject	Right to access data
Co-operation with supervisory authority	Security measures	Right to obtain rectification	Right to erasure
Notification of data breach	Communication of data breach	Right to obtain restriction	Communication to recipients of data
Data protection impact assessment	Consultation with supervisory authority	Right to data portability	Right to object
Data protection officer ("DPO")	Role of DPO	Adoption of specific rules by Member States	Automated decision making
Tasks of DPO	Certification mechanisms	Failure to comply with an order, limitation or suspension	Transfers to a third country or international organization
Obligations of certification bodies	Obligations of monitoring bodies	Failure to provide access to supervisory authority	

Source: FieldFisher

What is notable here is the scale of the fines. The GDPR increases the potential scale of fines to as much as 4% of global annual turnover. This compares to the largest fine in the U.K. issued so far for a data breach of £400,000 in October 2016, which was issued by the ICO to TalkTalk following a cyberattack which accessed customer data. The highest fine enforced by a data protection authority in Europe was €900,000 when Google was fined in Spain in 2013 as the Agencia Española de Protección de Datos (AEPD) claimed that the combination of data collected through different Google services exceeded reasonable expectations of the majority of users, and Google did not make it easy for users to access their data.

Even if little else about the GDPR was different from the Directive Regime, this fundamentally transforms the risk profile of data protection. With the potential to pay out 4% of global annual turnover, companies can no longer risk continuously falling foul of the regulator. Based on MSCI's 10 global sectors, fines of this magnitude could wipe out upwards of 25% of operating profit.

Figure 65. Impact on Operating Profit From Maximum Fine (MSCI Global Sectors)



*Financials is based on a percentage of profit before tax (PBT)

Source: DataStream, Citi Research Estimates

Regulatory Enforcement Falls Under Data Protection Authorities

Data Protection Authority: A national regulator responsible for the protection of personal data as required by EU legislation.

The GDPR specifies a greater number of tasks to data protection authorities, while simultaneously empowering them with a great range of capabilities. This new, more expansive, regime will bind national Data Protection Authorities in a more tightly knit network. The Directive had been administered by Data Protection Authorities (DPAs), National Telecoms Regulatory Authorities (NRAs) and, in many cases, split between the two.

In conjunction with expanding the competencies of national regulatory authorities, the GDPR also specifies a greater degree of cooperation between authorities. This takes two forms, both of which aim to improve the degree of regulatory consistency. The first is a framework for cooperation between regulatory authorities on specific transnational regulatory issues. Articles 61 and 62 specify that regulatory authorities must mutually aid one another when requested, and when a regulatory issue concerns data subjects in multiple different countries. It also states that regulatory authorities should work collaboratively to reach a decision.[22] One of the key elements of the GDPR is to create a one-stop shop for transnational regulation. What this will mean is that when cross-border issues come to the fore, the national supervisory authority in which the accused has their 'main establishment' will take the lead in the investigation. The lead regulatory authority will then cooperate with other regulatory authorities in so far as is necessary.

European Data Protection Board (EDPB): A new body that will replace the Article 29 Working Party. It will be comprised of representatives from the national data protection authorities in Europe, as well as non-voting representative from the European Commission.

The GDPR, finally, regulates for the creation of a new European Data Protection Board (EDPB) to replace the Article 29 Working Party. The New European Data Protection Board will stand at the center of a much more complex regulatory regime and will play a more involved role. As well as issuing guidelines and recommendations, it will provide a dispute resolution mechanism between national authorities.

Challenges to regulatory decisions can now be raised by any regulatory authority, and ruled on by a 2/3 vote of the new Data Protection Board. This will be transformative as it should reduce the number of cases going to the Court of Justice of the European Union (CJEU).

[22] Joint decision making clause

D. International Data Transfers

Data transfer: Under the GDPR, data transfer refers to transferring personal data to countries outside of the EEA.

The GDPR does not constitute a significant change to the regulation of data transfers. Both the DPD and GDPR require that protection of personal data should not be undermined when transferred to third countries, and should be carried out in compliance with the regulation. There remain four bases on which personal data can be transferred out of the EEA; these remain substantially the same as those under the Directive.

Figure 66. Mechanisms to Address International Data Transfers Under the GDPR

Mechanism & GDPR Article	Description	Data Protection Directive Article
EC Adequacy Decision (Article 45)	Here, the European Commission decides another countries domestic data protection regime is sufficient. Only 11 countries are whitelisted, including Canada, Argentina, Israel, New Zealand and Switzerland.	Directive Article 25
Binding Corporate Rules (Article 46)	These are binding sets of intra-corporate global privacy rules that allow corporates to transfer data within their group companies on the basis that they commit all to European Standards of Data Protection. Applies to multinationals.	Directive Article 26 (4)
Model Contract Clauses (Article 46)	These are written by the EC and can be attached to contracts. These commit both parties to certain enforcement mechanisms, as well as committing them to certain practices	Directive Article 26(4)
Contractual clauses between the parties (Article 46)	These are now, under the GDPR, subject to pre-approval by the National Supervisory Authority. Here transfer is allowed when the data importers liability to the European controller is deemed to offer sufficient protection	Directive Article 26(4)

Source: Citi Research

Adequacy: A standard used by the European Commission to assess countries outside the EEA and whether personal data can move freely between an EEA economy and another third economy. If protections in the third economy are deemed 'adequate', then data can be transferred freely.

If no other transfer mechanism is in place (such as contractually based agreements), controllers have to obtain explicit consent to transfer data to countries that do not have adequacy status.

Given the GDPR applies to all EU citizens, and not just to data processed in the EU, the rules around international transfers will become more relevant. The increasing use of cloud services blurs the picture further as it breaks down geographical barriers, but the EU regulation retains very strong geographical boundaries. In the past year we have seen announcements from large tech companies such as Amazon, Google, Apple, and Microsoft that all are opening up data centers within the EU. This is partly to ensure compliance with the European regulation.

Data Transfer Agreement with the U.S. on Shaky Ground

Max Schrems: Austrian lawyer and privacy activist. He played a key role in the ECJ ruling that the Safe Harbor agreement between Europe and the U.S., allowing data transference, did not provide adequate levels of protection.

While the GDPR did not address it directly, the single largest shake-up in relation to transfer agreements has occurred in the wake of the Edward Snowden revelations about the surveillance approach taken by the U.S. intelligence services and the practices of institutions such as the Foreign Intelligence Surveillance Court (FISA court). The subsequent ruling, in *Schrems v Data Protection Commissioner (2015)*, stated that the Safe Harbor agreement, which allowed (~4,600) U.S. companies to receive data from Europe if they committed to set principles, no longer constituted an *adequate* level of data protection led to the U.S. losing its adequacy status.

Safe Harbor: Agreement between the US and EU that allowed the free transfer of data from the EEA to the US. This agreement was deemed invalid by the ECJ in 2015.

Privacy Shield: Replaced the Safe Harbor agreement, with a more robust program of enforcement under US law. American companies can volunteer to participate, with membership allowing companies to freely transfer data between European and American operations.

After intense negotiations, a Draft Adequacy ruling was published on July 12, 2016 to form the basis of the Privacy Shield, a new agreement between the U.S. and EU on data transfer which increases company obligations, requires explicit guarantees on government access (disallowing mass surveillance), personal redress options and increased monitoring of how the Privacy Shield is functioning, especially in relation to data for national security and law enforcement.

Despite this new agreement the debate remains ongoing, and privacy group Digital Rights Ireland has brought a challenge against the Privacy Shield. The change of regime in the U.S. also raises questions as to whether the Privacy Shield can remain in place. The European Commission is seeking assurance from the U.S. government over the future of the agreement, and EU Justice Commissioner Vera Jourova has said "*I need to be reassured that Privacy Shield can remain. I need to have reconfirmation that there is continuity and we will be very strict assessors of the current decisions because Privacy Shield is not a one off decision, it is the mechanism where we have several American national authorities involved.*"

Banks, insurers and telecoms companies are precluded from signing up to the Privacy Shield (it applies to companies under the jurisdiction of the FTC or Department of Transportation (DoT) in the U.S.) and so will need to rely on binding corporate rules (which only cover transfers within an entity across borders) and model contract clauses for data transference to the U.S. The Binding Corporate Rules (BCR) have only been adopted by a small number of companies due to the complexity. The outlook for these mechanisms is also unclear as Max Schrems has brought a case against Facebook's use of model clauses as a legal basis for transfer of data from its Irish office to the U.S. It is currently sitting with the High Court in Ireland which is considering whether to refer it to the CJEU.

Brexit Implications

Since the GDPR was published the U.K. has voted to leave the EU. The U.K. Culture Minister has confirmed that the Britain will adopt the GDPR as it will still be a member of the EU in 2018 when the GDPR comes into force; it will be reviewed post Brexit. The immediate impact post Brexit will be that the ICO (the U.K.'s data protection authority) is unlikely to have a position on the EDPB, and will therefore lose the ability to influence data protection policy within the EU.

Even if the U.K. implements the GDPR and continues to apply the regulation post Brexit, the U.K. could still face issues in seeking adequacy status from the EU. This is key in ensuring data can be transferred by businesses freely across the EEA. There are two reasons the U.K. could face a stumbling block in seeking adequacy:

GCHQ: British intelligence and security organization

- 1) The Snowden revelations highlighted that the U.K.'s Government Communications Headquarters (GCHQ) was involved in surveillance (like the U.S., which has since seen the Safe Harbor agreement announced as illegal);
- 2) The U.K. passed the controversial Investigatory Powers law in November 2016 which extends state surveillance, and requires web and phone companies to store consumers' web browsing histories for 12 months and give the police, security services, and official agencies access to the data. It also provides the police and security services with new hacking powers.

Neither sits comfortably with the GDPR's approach.

Implications: GDPR Represents Major Shift in Landscape

Although the GDPR is presented as a 'tightening of existing themes' rather than a fundamental revision, it is hard to believe that it won't have a significant impact on both consumers and corporates alike.

For consumers, the GDPR will potentially lead to a significant increase in transparency in relation to personal data – what data companies have and how it will be used – as well as the opportunity to exercise new rights, in particular with regard to data portability and the right to erasure. What is more, this approach will be uniformly applied across Europe.

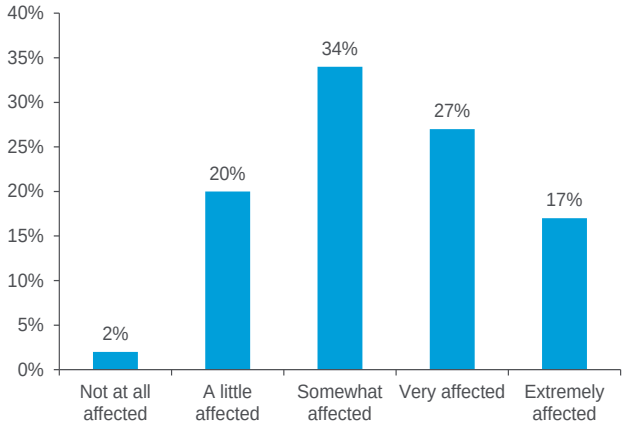
For corporates, the changes will be no less seismic but are so complex that compliance has to be a concern. Most companies outsource functions across their business, e.g., payroll, expenses and travel, data storage, and all of these will now have to be compliant with the new regulations. According to analysis by Skyhigh in September 2016, of more than 20,000 cloud services, only 6% can claim to be fully compliant with the GDPR, and 84% of cloud services do not immediately delete customer data on termination of contract.[23] Coupled with the significantly enhanced breach notification requirement and a sanctions regime with real teeth, we think privacy and data protection will be moving up the agenda of management teams. And if it isn't, then it should be.

A survey on the GDPR by the U.K. DMA (Direct Marketing Association) highlights the reach the GDPR will have: 98% of companies expect to be affected by the GDPR to some degree, and 44% expect to be very/extremely affected. It also shows what companies are prioritizing in order to be compliant.

Figure 67. Biggest Priorities for Your Organisation (in Preparing for the GDPR)?

Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2' Survey conducted Sept-Dec 2016

Figure 68. To What Extent Do You Think Your Organisation Will Be Affected by the GDPR?



Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2' Survey conducted Sept-Dec 2016

[23] http://www.securityweek.com/94-cloud-services-not-gdpr-compliant-report

In terms of who is particularly impacted, there is a central paradox, in our view. We believe that the EU had the large technology corporates in mind when setting out the GDPR agenda. Ironically however, these companies – and larger corporates in general – will most likely be able to navigate its strictures given they are more likely to have the resources and infrastructure in place to be able to deal with it. By contrast smaller enterprises, which potentially don't have the resources to deal with the implementation of the GDPR but are nevertheless bound by its rules, face the biggest challenges in terms of compliance.

Another key challenge is in navigating any contradictions between the GDPR and industry specific regulation, especially industries which already deal with stringent regulation, e.g., financial services. The industry regulator tends to require data maximization whereas the GDPR aims for data minimization. Which wins out? We suspect the GDPR but this remains to be seen.

ePrivacy Directive 2.0: Potentially as Game Changing as the GDPR

The GDPR will not operate in isolation. The ultimate regulatory framework facing citizens will be the product of the GDPR meshed with a range of other regulation/legislation.

Amongst others, there are two important pieces of European legislation that will directly overlap with the GDPR:

Digital Single Market Strategy: European Commission strategy that aims to ensure uniformity in digital industry standards. The aim is to create an integrated market in digital industries in Europe.

- **ePrivacy Directive (2009/136/EC) -** This Directive was initially drafted in 2002 to replace the 1997 Directive providing specific rules on the regulation of the telecommunications sector and applies to providers of *electronic communications networks and services to end-users.*[24] The core aim of this directive is to ensure the privacy of consumers in the use of such services, specifically covering the use of cookies and the opt-in/opt-out requirements related to direct marketing. The ePrivacy Directive is currently being reviewed for the third time in 14 years (under the Digital Single Market) and appears likely to change materially (not least because it will become regulation), which will have important implications for the actual operation of the GDPR.

- **2016 Network and Information Security Directive (2016/1148) -** This regulates so called' providers of essential services' and 'Digital Service Providers.' Essential Service Providers are providers of goods used by large numbers of people, where the failure to provide the services results in significant damage to the interests of others. Examples, listed in Annex Two of the directive, include providers of air travel, water supplies, and financial services. Digital Service Providers are those that provide a digital service, often at arm's length and for remuneration. The overall aim of the directive is to ensure a '*high common level of security of network and information systems*.'[25]

There are two reasons why all of this is significant.

- Firstly, while the GDPR may occupy a fundamental position, other directives may provide additional details/requirements for specific industries or areas.

- Secondly, this inserts a third level of uncertainty for stakeholders. Already, there is ambiguity in the manner in which the GDPR will be interpreted by the CJEU and the derogations formalized by member states.

Many operations will be simultaneously bound by the requirements of several of these regulations. Just as with the GDPR, this broader regulatory system is mired in uncertainty.

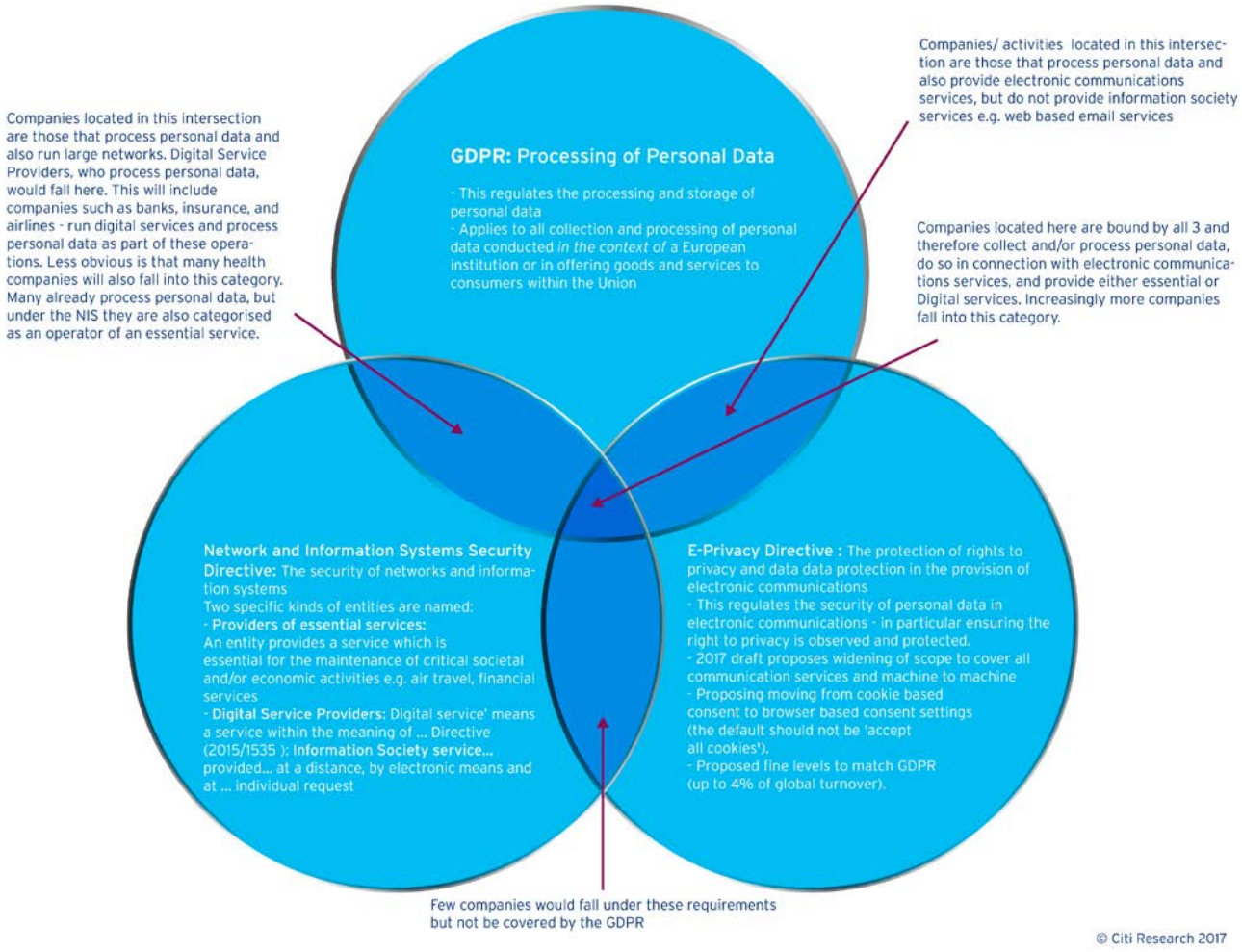
---

[24] This phraseology is used in the 2009 Amended ePrivacy Directive (Directive 2009/136/EC) Article 1 (1). The definition of Electronic Communications Networks subsequently used in the Directive is itself taken from the 2002 Framework Directive (2002/21/EC). Article 2(c) defines Electronic Communications Networks as "service(s) normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks."

[25] Article 1(1) 2016.

Below is a diagram detailing the respective material scope of each of these regulations, and their respective overlaps:

Figure 69. Areas of Overlap Between the GDPR and the NISS and ePrivacy Directives



Source: Citi Research

Review of the ePrivacy Directive 2.0

The 2015 Regulatory Fitness and Performance Programme, introduced under President Junker, aims to improve the general effectiveness of European regulation. Key is that all pieces of European regulation must add value, and therefore must not be duplications of provisions made elsewhere. This recognizes the inherent cost of regulatory duplication, resulting from additional complexity and risks associated with double jeopardy.

The adoption of the Digital Single Market strategy, which aims to increase trust in and security of digital services, triggered a review of the ePrivacy Directive (which was only reviewed last in 2009) in order to align it with the GDPR. The ePrivacy Directive is in place to ensure the protection of fundamental rights and freedoms in respect to privacy and personal data. A draft of the newly updated ePrivacy directive was published on January 10, 2017.

The EC adopted a 'compare and contrast' analysis in relation to the existing ePD and the GDPR, and some alignment has been proposed, e.g., in relation to reporting of data breaches, the ePD had specified a 24-hour timeframe to report a breach while GDPR specifies 72 hours, and the Commission proposes to remove the overlapping breach reporting requirement set out by the ePD as redundant.

What is clear from the draft proposal is that the EC believes that "*the protection of fundamental rights cannot be left to self-regulation by industry.*"[26] This is reflected in the tightening up of other areas of the ePD. The main proposals are:

Shift to Regulation

The EDPS is proposing the ePrivacy Directive be implemented as a Regulation across all member states. The sanctions will be enforced by the national data protection authorities and aligned with the GDPR: maximum of up to €20 million or 4% of global annual turnover.

Widening Scope of Companies Which Have to Comply

Over the Top (OTT): Delivery of content over the internet.

Machine-to-machine communications: Direct communication between devices through a network. Integral to the Internet of Things.

The definition of an electronic communication service according to the 2009 ePrivacy Directive does not currently include over-the-top (OTT) services, e.g. WhatsApp, iMessage. Based on the EC's public consultation (April to July 2016) 76% of citizens agree that the scope should be extended to new communications services (OTTs) and so the EC has extended the regulation to apply to any company processing data in connection with electronic communication services, regardless of where the processing takes place, which means that OTT providers will be included. Even where communications is not the core business, but there is an element of electronic communication, then the regulation may be applied e.g. review sites, ecommerce sites, web-based email services. It will also apply to machine-to-machine communications, which the EC sees as needed to promote a secure Internet of Things.

[26] Com2017 10 final, 2.3

Consent; Clamping Down on Tracking

The previous 2009 ePrivacy Directive introduced the focus on consent for cookie use, which led to the pop-up banners requesting approval for cookie use. The Commission appears to acknowledge that the cookie consent rule has led to "consent fatigue" and has not met its objectives as it lacks transparency on how to withdraw or manage consent, does not distinguish between the cookie types i.e. included those essential to a site operating as intended, does not encompass a wide range of tracking techniques e.g. device fingerprinting, and consumers did not necessarily understand the meaning of accepting tracking cookies:

"*The consent rule is over-inclusive, as it also covers non-privacy intrusive practices and under-inclusive, as it does not clearly cover some tracking techniques (e.g. device fingerprinting) which may not entail access/storage in the device.*"[27]

The proposal makes a distinction between tracking cookies and some first-party cookies. Consent will not be needed for cookies used to improve the Internet experience, e.g., shopping cart history or for a site to measure web traffic.

Consent requirements for tracking users online with cookies or other tracking tools face more stringent consent requirements. Browser settings will become the key tool for consent, which will eliminate the need for cookie banners and notices, and reflects the findings from the Eurobarometer survey conducted in 2016 in which 89% of respondents supported privacy by default in the browser setting.[28] Web browsers are seen as potential 'gatekeepers' to help information being unknowingly accessed/stored.

The proposal notes that the default setting for web browsers is currently 'accept all cookies'. The draft Regulation proposes that the software is reconfigured to offer a range of privacy setting options: 'never accept cookies', 'always accept cookies', 'reject third-party cookies, or 'only accept first-party cookies'. In the case of third-party tracking cookies the web browser should "*require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies.*" This means that at the point of software installation consumers should be informed about the privacy settings choices, and asked to make a choice. The information should not be biased in a way that dissuades users from selecting the higher privacy settings, and users should also be provided with information on the risks of allowing third-party cookies. Users should be able to easily change privacy settings at any time, and should be able to whitelist certain sites or specify which websites' third-party cookies are always or never allowed.

The EC believes that this approach to consent will save €948.8 million in terms of compliance costs overall, although this is mainly due to a decrease in the number of businesses implementing the consent settings, i.e., removes the need for cookie acceptance banners.

Direct marketing is also an area where requirements have been tightened up. Consent of the end user is required before direct marketing related electronic communications are sent to individuals, although email contact within the context of an existing relationship for offering similar products and services is allowed. If consent is given, then individuals should be able to withdraw consent at any time; the means by which to withdraw consent should be provided each time contact is made.

[27] ePrivacy proposed regulation – COM (2017) 10 final, 2017/0003 (COD)
[28] 2016 Eurobarometer survey (EB) 443 on ePrivacy (SMART 2016/079)

Internet access and voice communications are seen as essential services and the draft Regulation states that consent for processing data from Internet or voice communication usage will not be valid if the data subject has no genuine or free choice, or is unable to refuse or withdraw consent without ramifications.

Restrictions on Use of Metadata

Metadata: Data that provides information about other data. It describes how, when, where and by whom a set of data was collected.

The proposal has specified certain metadata, e.g., time of call and location, from electronic communications are deemed to have a high privacy component and will need to be anonymized or deleted if users have not provided consent, unless required for billing. If consent is provided then telecoms operators have greater scope to use the data to provide additional services or use the data to help public authorities, e.g., heat maps of individuals' presence.

NIS Requirements

It is important to remember that the GDPR specifies the right to an individual's data protection, not broader rights of data use and so is lacking in the area of cyber security. The Network and Information Systems (NIS) Security Directive, here, is complementary. This requires both operators of essential services and Digital Service Providers to:

Take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems used in the context of offering services.[29]

This NIS Directive, unlike the GDPR or ePrivacy directive, provides a definition for the 'Security of network and information systems:'

'*…the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.'*

Rather than requiring proportional action be taken to minimize the risk of data breach, here proportional action is necessary to *manage risks posed to the security of the network*.

One of the main differences is that the GDPR requires breach notification in 72 hours. The NIS Security Directive specifies notification should be given with undue delay and covers more general cases of so-called 'incidents'.[30] An incident is defined, under Article 4(7) as any event having an actual adverse effect on the security of network and information systems.

For notification to be necessary at all, the incident must meet certain requirements taking into account the number of users impacted, duration of incident, geographical spread and economic and societal impact. Rather than the controller or processor being obligated to notify unless it can demonstrate no harm, here the network operator only has to notify when the incident meets certain thresholds.

[29] Article 16(1) for Digital services, and 14(1) for essential services.
[30] Article 14 NIS

Implications: ePrivacy Directive 2.0 Makes Strict Consent Requirements Very Clear

Looking at complementary regulation, the one that appears more controversial is the draft ePrivacy Regulation. The EC has gone from considering whether this Directive would be needed with the advent of the GDPR, to now taking the stance that not only should it become Regulation (i.e. law in each member state) with the same level of fines as the GDPR, but that the scope should be broader in terms of operators that it impacts and that it should be implemented on the same time frame as the GDPR itself.

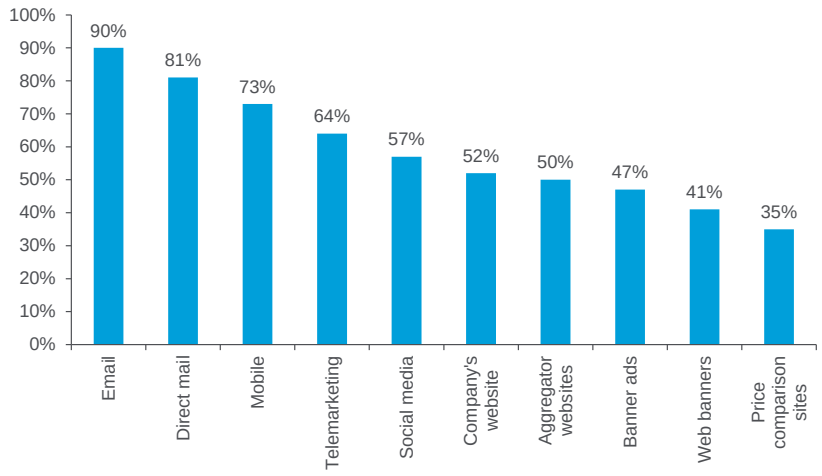
As we noted earlier, the use of cookies could potentially diminish as technology has enabled new means to track consumers. The EC has acknowledged that the 2009 ePD was far too narrow in its approach, focusing solely on cookies, and also too blunt, as it didn't distinguish between different types of cookies i.e. ones needed for the service to work vs. third-party tracking cookies.

What is clear from the first draft of the proposed regulation is that the EC has attempted to deal with technological changes by widening it to any form of tracking between any form of user, including machine to machine.

On the positive side for consumers and companies, the consent requirements for any form of tracking that is not for the purpose of the Internet experience have been clarified, and the move to a default 'opt-out' setting at a browser level is likely to be welcomed by consumers.

This said there will clearly be costs. Take for example the ad-funded online media ecosystem. A survey by the DMA of companies already identified channels like email, direct mail, and mobile as those that will be affected by the GDPR. In its current form, the revised ePrivacy Regulation will be extremely restrictive given some form of tracking is required for consumer profiling and ad targeting and, unlike the original ePD, there is limited scope for the industry to circumnavigate requirements.

Figure 70. What Channels Do You Think Will Be Affected by the GDPR?



Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2' Survey conducted Sept-Dec 2016

Likewise, subjecting OTT communications platforms to the same regulatory requirements as telecoms operators, while laudable in terms of levelling the playing field, could also be viewed as 'overkill' given many of these platforms have already got encryption in place.

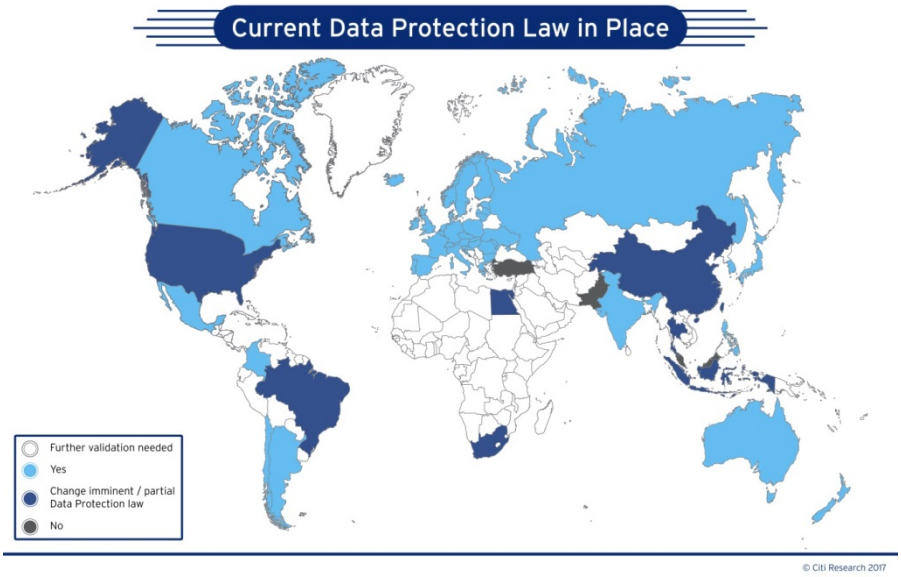
The only caveat is that, while the ePrivacy proposal potentially adds to the risks presented by the GDPR, it should be noted that what we have seen so far is just a draft. This is to say, it could yet be watered down.

At the same time, we should also note that its final form may well be influenced by external political factors. There was a time when the GDPR was seen as an 'ambitious first draft' but the NSA revelations firmed up the EU's resolve. An external event – a privacy-related political scandal and/or a large-scale commercial data breach – could be a wildcard.

International Data Protection Regimes

Data protection is not only a dynamic space in Europe. Common technological trends are driving changes on a global scale. The implication has been growth, and increasing heterogeneity, in the global data protection landscape.

Figure 71. Status of Current Data Protection Laws Worldwide



Source: https://united-kingdom.taylorwessing.com/globaldatahub/risk_map.html, Citi Research

The United States: Principles and Sector Based Approach

The United States has generally taken a more principle and sector-specific based approach than the EU. U.S. regulators have been willing to work collaboratively with industry operators, encouraging self-regulation. Legislation has been used to address specific risks (in the eyes of U.S. policy makers). Hence U.S. regulation has historically been comprised of a patchwork of different, industry-specific, regulations, rather than uniform data protection standards.

Fair Practice Principles

Modern Data Protection in the United States remains based on traditions stemming from 'fair practice' principles first enunciated in 1973.

Figure 72. Summary of 1973 Fair Information Practice Principles

Notice/ Awareness	There must be no personal-data record-keeping systems whose very existence is secret.
Access/ Participation	There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to correct or amend a record of identifiable information about him.
Integrity/ Security	Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
Enforcement/ Redress	There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.

Source: Citi Research

As the executive office of the President wrote in 2014, these principles form the bedrock of modern U.S. Data Protection. However, unlike in Europe, these aims have not been legislated for but rather pursued via a range of different means and by a range of different bodies e.g. legislation along industry lines. This also results in the diffusion of responsibilities among different regulatory authorities.

California Has Been the Pioneer at a State Level

Some states have led the way in privacy regulation, pushing ahead of the Federal Government. In this regard, states such as California are particularly noteworthy. For example:

Figure 73. Examples of Privacy Legislation in California

2003 California Online Privacy Protection Act	This requires commercial websites to post their privacy policies in a conspicuous manner, among other things
2002 The California Security Breach Notification Law	This requires holders of non-public personal information to notify users in the case of a breach.
2003 The California Shine the Light Law	This requires companies to disclose who they are likely to pass information on to and state their privacy policies

Source: Citi Research

None of these requirements exist in a general form at a Federal level, despite recent attempts. California's state law has been the basis of some recent, notable, prosecutions. In 2012, the Attorney General brought a case against Delta Airlines on the basis that its mobile app did not give sufficient prominence to its privacy policy. Additionally, there are important differences in sanction severity. Although this case was ultimately dismissed on the basis that state law could not regulate airlines in this way, Delta faced a fine potentially ranging up to $2.54 billion.[31] This is far in excess of federal fines.

[31] The regulations require financial institutions to provide particular notices and to comply with certain limitations on disclosure of non-public personal information. A financial institution must provide a notice of its privacy policies and practices with respect to both affiliated and non-affiliated third parties, and allow the consumer to opt out of the disclosure of the consumer's non-public personal information to a non-affiliated third party if the disclosure is outside of the exceptions.

In some cases, state provisions can converge to a considerable degree. For example, a notification requirement exists in 47 U.S. States as well as the District of Columbia and Puerto Rico. Despite this there are significant divergences in areas where states have specific concentrations in terms of industry exposure, such as New York for financial services.

Industry-Specific Approaches; From Self-Regulation to Legislation

There is sector-specific legislation that includes requirements around data protection, e.g., the 1996 Health Insurance Portability and Accountability Act, the 1999 Financial Services Modernization Act, as well as legislation driven by specific consumer groups, e.g., the 1998 Children's Online Privacy Protection Act, and covering narrow areas within industries, e.g., the 1988 Video Privacy Protection Act (preventing the sale of movie rental data).

The Federal Trade Commission (FTC) has been at the center of efforts to develop binding industry codes of conduct that can be used as a voluntary basis for self-regulation. The FTC has also tended to be central to the regulatory rule making.

In March 2012, the FTC issued a report that laid out a privacy framework and implementation recommendations ("Protecting Consumer Privacy in an Era of Rapid Change"). This was a follow-up to a preliminary report that was issued in December 2010.

The framework applies to all businesses that use consumer data that can be reasonably linked to a specific consumer or device. To avoid placing undue burdens on small businesses, companies that collect data from fewer than 5,000k consumers per year and do not share the data with third parties are exempt.

The framework has three key components:

1. Privacy by Design

The framework calls on companies to make privacy a central focus of their organizations and it should be built in to every stage of the development of products and services.

In practice, companies are expected to incorporate privacy protections – including data security, reasonable collection limits, sound retention and disposal practices, and data accuracy – throughout the life-cycle of their products and services.

2. Simplified Consumer Choice

The framework calls for companies to provide consumers with the ability to choose whether or not their private data is collected and used for targeted advertising. It also defines circumstances under which consumers should be given choices.

Companies should simplify consumer choice about collection and usage of personal data at the time the decision is being made. Companies should obtain affirmative consent before using the data in a different manner than was initially claimed and if sensitive data is being collected.

Companies are not required to provide choice if the practices are consistent with the context of the transaction or the company's relationship with the consumer (i.e., first-party collection) or are required by law.

3. Transparency

The framework lays out three principles to increase the transparency of data practices:

- Privacy notices should be clearer, shorter, and more standardized;
- Companies should provide consumers with access to their data;
- Companies should make efforts to educate consumers about commercial data privacy practices.

World Wide Web Consortium (W3C): A group of international tech companies working to develop common web standards.

Do Not Track: Individuals use of browser settings to block tracking by websites.

The FTC has been very proactive in the development of more collaborative initiatives to promote good data protection practices and self-regulation. A good example of this was the attempt to develop a common Do Not Track Framework in 2012. Here, the FTC worked alongside the World Wide Web (W3C) Consortium (including large tech corporates) to develop a universal web protocol for Do Not Track to allows users to control, through their browsers, how and when they were tracked. This initiative has since collapsed (see below).

Digital Advertising Alliance: An independent, non-profit body that develops common practices and standards for digital advertising. It has developed a set of principles that apply to data gathering and use in advertising.

Additionally, The Digital Advertising Alliance (a coalition of U.S. media and marketing trade associations) developed a targeted advertising icon, used in online behavioral ad campaigns in the U.S. The ad option icon is clickable on display ads. By clicking on the icon, consumers are able to view the companies that are collecting data, what the data is being used for, and can opt out of receiving targeted ads.

Movement Towards Legislation; FTC Enforcement Stepped Up

While there were few specific legislative changes during the Obama administration in Data Protection, there does appear to have been significant movement in institutional thinking. This applies in Congress, in the Executive and at the FTC.

There has been an increasing willingness to adopt a more legalistic approach. The collapse of the Do Not Track initiative seems to have shaken confidence in self-regulation. This initiative ultimately failed for a range of reasons. Most notable was the inability to get cooperation between different browsers, and advertisers. With an absence of broad buy-in browsers quickly abandoned the cooperation and tried to launch their own standard in an attempt to seize a first-mover advantage.

In July 2016 the White House released its first U.S. 'National Privacy Research Strategy', which identified priorities for privacy research funded by the Federal government. Congress has become more proactive in the area of privacy legislation. During the First Session of the 114th Congress alone, the following bills were introduced (although have not been passed yet):

- **S. 547 (Commercial Privacy Bill of Rights Act of 2015)** establishes a more specific framework for personal data protection which would fall under the responsibility of the FTC. It includes providing an opt-in mechanism for third-party data use, emphasis on data minimization and rules on data retention. It also aims to tighten up requirements around the use of children's data.

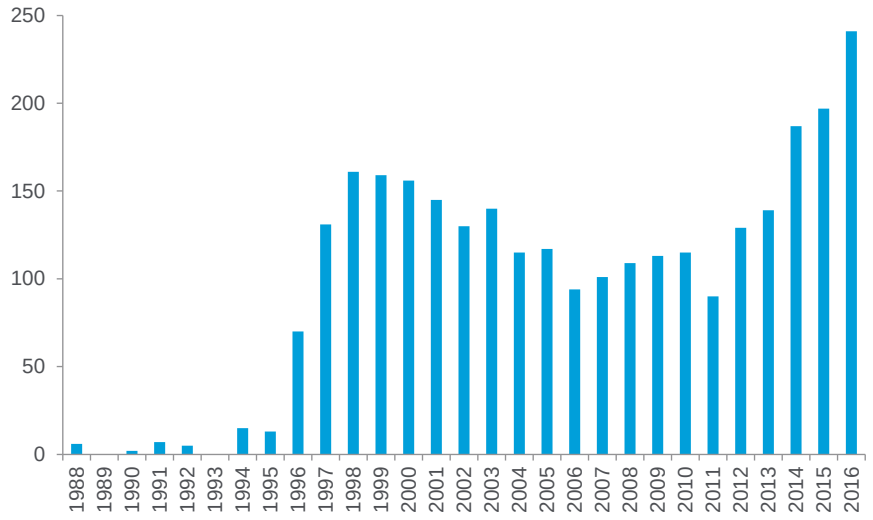
- **S. 1158 (Consumer Privacy Protection Act of 2015)** focused on businesses safeguarding personally identifiable information, and a framework for implementing a consumer privacy and data security program that complies with standards identified by the FTC. Provides explicit guidelines in treatment of data breaches, and makes concealing a data breach (which impacts any individual by $1,000 or more) a criminal offense.

A notable issue has been the regulation of Data Brokers. The FTC has had persistent concerns about Data Brokers, stemming from a perceived absence of transparency as these actors acquire data from many sources on a third-party basis. The FTC estimated in 2014 that these bodies had roughly 3,000 data points on every U.S. consumer. As a result, consumers do not know who their data is going to, what it is being combined with, and what is being derived using it.

In 2012, the FTC proposed a part legislative, part collaborative approach to Data Brokers. By 2014, a much more extensive set of data protection legislation was being suggested by Congress, cannibalizing many of the self-regulation initiatives. Legislation was introduced in 2015 to force Data Brokers to disclose the inferences made about individuals, and their sources, and, where risk mitigation products are used to block transactions, the company must notify the consumer, explain which broker provided the product and highlight the consumer's right to access and correct.

There also seems to have been a growing tendency, on the part of regulators like the FTC, to step up their enforcement operations. The FTC has brought high-profile data processors to task, including Google and Facebook. For example, in 2012, Google paid $22.5 million to settle an FTC probe resulting from their apparent misrepresentation of data tracking practices.[32] Crucially, however, enforcement is largely focused around companies violating their own policies, rather than specific legislation.

Figure 74. Number of Enforcement Actions Taken by the FTC



Source: FTC

[32] https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

The FTC settled with Nomi Technologies in 2015 alleging it misled people by saying they could opt out from its tracking technology in stores when no opt-out tool was available. In 2016 there was a $950,000 settlement with InMobi as the FTC said it had followed device locations even when people, sometimes children, had disabled tracking or never consented in the first place. Mr Polonetsky, CEO of the Future of Privacy Forum, believes it "should be a real wake-up call to the industry" and "the FTC now has a pretty detailed tech lab that has dozens of forensic tools."

The FTC has already been active in the area of data protection and privacy in 2017:

- It released a report in January 2017 offering recommendations to consumers on how to navigate cross device privacy. This followed the release of its OTech study examining data practices and privacy policies on 100 most popular websites, in which it found only three sites linked to a privacy policy that acknowledges it enables third-party cross device tracking, and many of the third parties don't belong to self-regulatory programs run by the Digital Advertising Alliance.

- The FTC agreed to settle with Vizio on February 6, 2017 (for $2.2 million) over its collection, and sale, of TV viewing data. The settlement requires that Vizio delete its old data and obtain affirmative opt-in to gather any future data. FTC attorney Kevin Moriarty said "*we have alleged that TV viewing information is sensitive data that requires an opt-in for collection and sharing*", according to AdExchanger. The incoming FTC chairwoman said she will launch a review to examine the issue further.

The Federal Communications Commission (FCC) had also stepped up its approach to privacy when it included specific privacy-related requirements into its regulation of network service providers in October 2016. These originally required ISPs to get opt-in consent from consumers before sharing sensitive web-based browsing data, e.g. geolocation, web browsing history, app usage history, and health and financial information. The regulation also required opt-out to be offered on other private information being shared with third parties, e.g., email addresses, service tier information.

These proposals were actively lobbied against by ISPs as they would have introduced a two-tier system whereby ISPs would operate under stricter rules than service providers (companies like Google and Facebook) which remain under the purview of the FTC and in March 2017 Ajit Pai, the incoming FCC Chairman, announced a stay on the implementation of the new rules precisely on these grounds. In their announcement, Mr. Pai, and Maureen Ohlhausen, acting FTC Chair, specifically confirmed their view that: *'the best way to [protect privacy] is through a comprehensive and consistent framework. After all, Americans care about the overall privacy of their information when they use the Internet, and they shouldn't have to be lawyers or engineers to figure out if their information is protected differently depending on which part of the Internet holds it'.*

Change of President Could Mark Change to Approach to Privacy

During the latter years of the Obama administration, a new privacy narrative was building momentum that would constitute an important change in the approach toward ePrivacy and data protection in the U.S. A 2014 report by the United States President's Council of Advisors on Science and Technology advised a change in regulatory focus from ensuring effective 'notice and consent' to active regulation of the uses of data. Prior to leaving office, the Obama administration also published a report on the White House website on the efforts it had made to improve consumer privacy and move the Consumer Privacy Bill of Rights into law.

It is not clear, as of today, how the new administration in the U.S. will approach online privacy. The commentary from both the FTC and the FCC suggests that the administration is still very focused on the topic and that any change in approach is purely to allow time for rules to be properly harmonized. Again speaking about the stay, the FCC and FTC Chairs argued that this is principally a question of jurisdiction: '*All actors in the online space should be subject to the same rules, enforced by the same agency'.* The question, however, is whether the move to the more legislative approach initiated by the Obama administration — which brings with it more specificity on what is/isn't allowed as well as tougher sanctions for non-compliance — will stall. We will have to continue to watch this space.

Asia-Pacific Economic Cooperation (APEC) Privacy Approach Economically Driven

APEC's aims in the area of data protection are exclusively economic. The framework has been developed in order to *build public confidence in the safety and security of data flows… to realize the potential of electronic commerce*. This is in stark contrast to Europe where the key aims of data protection revolve around the protection of fundamental rights and freedoms.

In 2004, the APEC countries (a forum of 21 Pacific Rim member economies that promotes free trade throughout the region) agreed their own set of privacy principles. These were based closely on the OECD principles of 1980, but notably the purpose specification and openness requirements were removed from the APEC framework (although some have adopted these anyway, e.g., Singapore). This is consistent with the narrower focus of APEC on economic development.

APEC Privacy Principles

Notice: Notice must be given of the collection/ acquisition of data

Access and Correction: Considering the burdens faced by controllers, subjects should be able to reasonably access and correct their data

Use of personal information: Use of data limited to the purpose initially stated and those compatible with it

Collection Limitation: Must only collect data relevant to the purpose for which it will be used

The means of implementation were not specified. This was left deliberately vague in order to permit the greatest flexibility in compliance. The Privacy Agreement formally stated that there were several options for giving effect to the framework including legislative, administrative, industry self-regulatory or a combination of these methods.

Out of the 21 member economies, 14 have successfully implemented the Privacy Agreement and are verified as having done so via the publication of an Individual Action Plan. In addition to this, Peru, the Philippines, Chinese Taipei, and the United States have also all submitted Individual Action Plans.

None of the APEC members that failed to submit an Independent Action Plan (IAP) have joined the OECD Global Privacy Enforcement Network (GPEN). This network provides a means of coordination between those data protection authorities that have implemented the OECD principles (the basis for the APEC Principles). GPEN requires states have a domestic enforcement authority with the investigatory and enforcement powers APEC specify. Membership of this network can be used as a proxy for the domestic regulatory organization.

APEC Privacy Principles (cont.)

Choice: Subjects are provided a choice with regard to whether to subject themselves to collection or not. Though this regulation does allow consent to be implied

Integrity of Personal Information: Personal information should be accurate

Preventing Harm: Proportionate protections be designed to minimize risks to the interests of whose data is being used

Security Safeguards: Safeguards stated in principle one should be implemented to a degree proportionate to the risk being faced

Accountability: Controllers should be held to account for compliance with these standards. When transferring personal information, controllers should take reasonable steps to ensure that they should be protected

Global Privacy Enforcement Network (GPEN): An organization founded by the OECD that facilitates coordination between privacy enforcement authorities.

APEC Cross Border Regime

In 2007 APEC launched a pathfinder to further reduce the difficulty in transferring data between APEC nations which culminated in the launch of three initiatives in 2011:

- **Cross Border Privacy Rules (CBPR):** a system of rules governing transnational data transfers.
- **Cross-Border Privacy Enforcement Arrangement (CPEA):** a system ensuring that consumer rights are enforceable, even when data is transferred internationally. This provides for cooperation between enforcement agencies.
- **Privacy Recognition for Processors System (PRP):** provides formal recognition for processors that meet certain privacy standards.

The overall aim of this framework was to foster the development of international data flows by ensuring enforcement of data protection standards on a transnational basis.

The scheme works by allowing corporates operating in multiple APEC nations to adopt certain 'Binding Corporate Rules' that, in turn, can be used as a basis for burden free data transfer. This framework is based on the adoption of rules sufficient to ensure transfer standards are maintained.

Both companies and APEC countries choose to join the CBPR system but must first secure the membership of domestic data protection enforcement authorities in the Cross-Border Privacy Enforcement Arrangement (CPEA) to do so.

Those states that have implemented the 2004 principles with IAP verification, and are members of the GPEN, are also all members of the CPEA. There are several countries that have implemented the 2004 principles but are not yet members of the CPEA.

Figure 75. APEC Regime Implementation

Country	IAP Verification	GPEN Member	CPEA Member
Australia	Yes	Yes:	Yes
Brunei	No	No	No
Canada	Yes	Yes	Yes
Chile	No	No	No
China	No	No	No
Hong Kong	Yes	Yes	Yes
Indonesia	No	No	No
Japan	Yes	Yes	Yes
Korea	Yes	Yes	Yes
Malaysia	Yes	No	No
Mexico	Yes	Yes	Yes
New Zealand	Yes	Yes	Yes
Papua New Guinea	No	No	No
Peru	Yes	No	No
Philippines	Yes	No	No
Russia	No	No	No
Singapore	Yes	Yes	Yes
Taiwan	Yes	No	No
Thailand	Yes	No	No
US	Yes	Yes	Yes
Vietnam	No	No	No

Source: Citi Research

In addition, countries wishing to actively participate in the CBPR must also ensure that there is at least one so-called 'Accountability Agent' in the country once they have joined the framework. Accountability agents independently review and verify the rules proposed by companies to meet the standards of the CBPR. For an accountability agent to be approved, the country must first formally join the CBPR. Currently, four economies are formally signed up — the U.S., Mexico, Canada, and Japan.[33]

Implications: A More Laissez-Faire Mindset Internationally Contrasts with the EU's More Dirigiste Approach

The irony is that for a challenge that is so global in nature, the approach taken by different regulators is so regional/local.

We draw three inferences from this compare-and-contrast between the approaches taken by the EU vs. other regions:

- First, we note that while the approach toward privacy is hardening in the U.S., it nevertheless appears more collaborative in nature than the approach taken in Europe. Both have similar aims in protecting the rights of consumers but the U.S. has no overarching legislation in place versus the EU's GDPR, which will be forced into law across the member states.

- The open question, especially post the change in administration in the U.S., is whether the direction of travel continues to be toward tighter controls. In this context, whether the Privacy Shield survives in its current form will be an interesting and important litmus test.

- Second, it is clear that APEC's approach is (a) much more economically driven and (b) much more practical in nature with the broad and consistent application of 'privacy principles'. Clearly APEC believes this will encourage data protection and in turn build the trust of consumers, while also avoiding a significant chilling of economic activity.

- Third, it is worth re-highlighting at this stage the relatively limited number of countries to which the EU has given 'adequacy' status as well as the commitment to enforce the requirements of the GDPR on any company that aims to operate in the EU and/or sell into EU consumers.

Put simply, we have the beginnings of an impasse. There appears to be a global consensus that privacy and data protection are important issues that need to be addressed by regulation, but the asymmetry in approach is likely to make compliance a challenge.

Of course this could be addressed by simply adhering to the rules of the toughest regime – i.e. those of the EU – but for some companies/corporations this may not be worth the work/investment relative to the size of the opportunity. In this context, there is a very real prospect that consumers, especially those in the EU, could potentially miss out on products/services that they might otherwise value.

This said, to get a better sense of how corporates will approach the broader issues around privacy and data protection and the specific challenges associated with implementation of GDPR, it is important to talk directly to companies affected by the issues we raise. In this next section we do just this.

[33] http://www.cbprs.org/Agents/CBPRsRequirements.aspx

Expert Views

A Conversation with Vivienne Artz

Managing Director and Head of International Privacy, IP and O&T Law, Citi

Vivienne Artz is a Managing Director and General Counsel for Intellectual Property, Technology and Privacy Legal for the EMEA and APAC regions in the General Counsel's Office at Citi, in London.

Prior to joining Citi in 2000, Vivienne worked in private practice in London.

Vivienne chairs the AFME Data Protection Working Group, the International Regulatory Strategy Group Data Working Group and is an active participant of the Data Working Group at the BBA, as well as a Steering Committee member for the Technology Discussion Group. Vivienne has recently been appointed to the IAPP European Advisory Board having also served as a co-chair of the IAPP Knowledge Net for the U.K., a co-chair of the U.K. Citi Women Network, chair of the Legal Diversity Council for EMEA, and is currently a Citi Women Community Ambassador. Vivienne was awarded the Women in Banking and Finance "Champion for Women" Award in 2016.

Privacy and Data Protection: How big a topic is this for consumers?

Given its hugely multi-faceted and pervasive nature, most people don't really understand how the Internet works and how their Internet usage can be tracked. Ignorance, in this context, and in relation to big businesses, can generate a lot of concern as many consumers immediately assume all forms of data collection is for nefarious purposes.

If we look back at the past, I don't think companies have particularly helped themselves in this regard as data has, more often than not, and particularly in some jurisdictions, been used for targeted marketing and sending unsolicited emails, i.e., services that consumers don't necessarily immediately value.

Prior to GDPR, how did you approach privacy as an issue?

It has been a topic of growing interest and importance over the years but it has been a progression. It started off life as primarily an EU issue, and in the last 8-10 years we have seen a sudden and exponential growth in the number of privacy laws and regulations all across the world.

What is interesting to see is which model the new privacy laws are following — in general, the EU model, which is fairly restrictive, is prevailing.

The advent of social media has been a game changer because suddenly privacy has moved from being primarily a relatively obscure legal and data security topic to something that actually means something to consumers on a personal level more generally. Another important issue is the introduction of penalties, because for all that you ask entities to adhere to best practice, and for all that you might have requirements vis-à-vis privacy and data protection, if there are no real consequences for non-adherence, then compliance with those requirements tends to be relatively minimal, especially if there are conflicting obligations.

The regulators historically have been under-resourced and lacking in the tools to help organizations to comply and to address non-compliance. As such they have often looked to business, such as large banks, to undertake significant compliance obligations. Moving forward, a response to data protection has to be proportionate and done in partnership with regulators – the danger nowadays may now arise from a small FinTech start-up, who in all fairness may not be fully aware of the data protection requirements and who will need regulatory support and guidance. The response therefore needs to be proportionate to the circumstances especially if simple human error or illegal behavior plays a part.

How does the GDPR impact your approach to privacy and data protection in general terms?

I think it is a huge game changer in terms of how companies process data and how they think about data. I think many organizations need to fundamentally rethink their current models of storing, using, and accessing data because there is a potential clash between how businesses operating in the global economy approach some of these challenges, and the increasingly geographical/localized approach being taken by the EU.

It is a question of finding all those intersections of data and ensuring an awareness and decision-making process that encourages and supports the right behaviors. So, for example, when data is collected – is it being collected, used, and disposed of in the right way?

For many organizations , it may require revisiting the core business model and making sure privacy considerations are considered afresh: yes, we would *like* to do this or that with data but *can* we do it, and even more importantly, *should* we do it? In many cases these are issues that have not been thought about in depth before, but now we have to consciously engage with all of the issues.

Should data be stored centrally, and if so where? Should data be anonymized or pseudonymized? How do I know that my proposed data uses are compliant?

These kinds of questions have to be considered across the life-cycle of data, up to and including deletion. In the past, it may have been interesting and useful to keep the data, but actually the rules no longer allow this, at least for personal data.

In summary, the GDPR is going to impact every step of the life-cycle of data within our organization and we are going to have to start making some difficult decisions about where we store it, where we access it and how we use it.

On a practical level how should we think about compliance with GDPR?

The starting point is a data mapping exercise. It is important to understand what the landscape looks like within your organization: what data you are collecting and where it is stored and accessed. There are then broader data themes that have to be considered at each stage and within each business line, such as information security, profiling, supervisory authority etc. Organizations need to establish their own methodology for tackling this issue to avoid trying to boil the ocean.

This said, certain sectors such as financial services, are at an advantage because client confidentiality has always been at the heart of what we do. We also have compliance and audit processes already in place. In this context, the GDPR is an incremental change, albeit a sizeable one.

In short, we can do it. It is not easy, it is costly, it is unwieldy and it will be hard work, but we will get it done. This will be a lot more complex for small & medium enterprises (SMEs) as well as companies in other industries without these structures already in place.

What are the obvious implementation challenges from your perspective?

For financial services firms, our biggest challenge is in balancing our regulatory obligations against our GDPR obligations and where the two find themselves in conflict or inconsistent – for example Anti-Money Laundering (AML) – we have a challenge.

For AML, we are currently obliged to process information and profile personal data. The GDPR, however, aims to restrict profiling and prohibits firms from processing information about criminal convictions. In practical terms this means that each member state in the EU will need to implement legislation to permit financial services firms to process information about criminal convictions as part of background screening or as required by AML rules (as is current practice today), to enable firms to continue this processing once GDPR comes into effect.

This is an important point: the GDPR, as an EU law, takes precedence over any regulatory guidance, standard, best practice, or internationally agreed protocols unless those other rules are articulated in Member State law. This means there is a big 'catch-up' that needs to take place to make sure all the pieces fit together.

Another important challenge is how GDPR-related requirements are implemented in firms with a global footprint. For companies with branches, subsidiaries, and affiliates in non-EU jurisdictions with their own regulatory obligations, compliance can become incredibly challenging to enable the sharing of information with regulators or authorities outside of the EU, for example the U.S. Federal Reserve, the Office of the Comptroller of the Currency (OCC) or the Hong Kong regulator as these countries are not regarded as 'adequate'.

Is there anything that you think is incrementally positive for the financial services industry that is associated with the implementation of the GDPR?

It is difficult to find absolute positives, this said, it has taken the issue of data protection and ePrivacy from somewhere in the bottom 20 of issues that corporates worry about and spend time on to somewhere in the top 10. For consumers, too, the EU has achieved a significant amount of awareness-raising of privacy and data protection issues, arguably more so than any other jurisdiction, and for that they truly deserve credit.

It is also fair to say that the regulators have tried hard to be creative in some areas to streamline processes, although this is in danger of being outweighed by inflexibility in other areas.

As examples of an area where streamlining has been introduced, I would highlight the explicit statement that Member States can no longer add additional requirements around model contracts. This is good as it reduces the potential for unnecessary bureaucracy in this area.

They have also expanded binding corporate rules to include processors. This, too, is good. Some of the tidying up around lead supervisory authorities is also helpful. There are also some positive statements about concepts like codes of conducts and certification which show that they clearly want to embrace more sensible ways of doing things.

The problem across the board, though, is that more often than not either the key details are left out or the articulation gets lost in the wording of the GDPR itself. So while it is clear that the authority's heart is in the right place, the end product is not as clear and distinct as it could or should be.

You mentioned Binding Contract Rules and Model Contracts. Can you expand on these concepts in the context of international data transfers which will be a key issue for any large, complex business?

Binding Contract Rules (BCR) are a brilliant concept and absolutely work for large organizations. However, it has become so wrapped up in conditions and requirements that it are somewhat unwieldy. If we take Citi as an example, when we implemented our BCR, we had to cross the cultural divide and articulate the requirements in EU-style language. This has the effect of making it user unfriendly. For example, terms like 'data controllers' and 'data processors', although consistent with the EU terminology, are not part of a natural language suite.

With this in mind, their success – or rather relative lack of success – is demonstrated in the fact that only about 40 companies have ever embraced BCRs. This suggests that while it is a brilliant idea, the fact that so few companies feel they are able to do it is testament to the fact that it is an incredibly onerous process and one that very few have the time, the budget or indeed the stomach to undertake.

From a Citi perspective, however, despite this we think it was the right approach. It was hard work, but it embedded privacy in our organization in a proactive and positive way, rather than as simply a 'legalistic' thing.

Model Contracts, again, represent a clever legal solution to a legal problem, but they don't necessarily change the culture or change behavior, and this is a shortcoming. One of the big inferences of the GDPR is that you need to take it to the next level in terms of transparency, culture and behavior and simply putting in documents and signing things doesn't necessarily achieve this.

I would say that one of the biggest challenges with respect to privacy-related issues is that, because it has been so complicated in the past and so often sat with the lawyers (and I say this as a lawyer myself), that it has become somewhat unintuitive and excessively legalistic. And this is one of the issues with international data transfers: we have ended up with legalistic solutions to practical problems and this is not always that helpful.

How does the fact that data processors are now also impacted by regulation impact the broader landscape in your view?

The responsibilities of data processors have been significantly enhanced so rather than simply following instructions and putting in place technical and organizational security measures and responding when asked to, they now have liability and responsibility for data processing.

But this goes both ways: it puts more onus on processors to make sure they are compliant, but it also opens up the potential for them to push back on data controllers and challenge the validity of the processing that they are engaged to do.

The negotiation of these provisions is daunting. Indeed, in our own negotiations with suppliers, privacy and data protection are among the most significant clauses in any agreement.

And negotiating around provisions is only one aspect. One cannot insert a clause in the contract saying that each side agrees to comply with their obligations – there must be accountability. In practice this may require audits of third parties' processes to ensure compliance.

One example of things that users of data will have to check is whether processors are using cloud-based providers themselves. This means there are three distinct parties that are using/processing data, all three of whom have to be compliant.

One analogy I have used which is apt, is that data protection obligations are like a virus: they follow the data wherever it goes. And the approach of the EU regulatory authorities has been that, unless the 'virus' can follow the data, the data will not be allowed to flow.

The end result of this is that there is going to be significant change in the balance of the relationship between vendors and customers, and, ultimately, I think there is a danger that the cost of contracting could go up significantly, which may price smaller businesses out of the market as well as negatively affect the functioning of a competitive, efficient financial ecosystem.

Is the right to erasure a pain point for Citi or financial services firms in general?

Initially, we were very concerned about the right to erasure, but through a lot of effort and awareness-raising, it appears that we have reached the right place in terms of how this is framed within the GDPR. There is still a challenge, however, in terms of managing expectations of consumers around what it means.

Originally, the concept started off as the 'right to be forgotten' but the reality is that this is very challenging. Yes we can make sure that data is not held for longer than is necessary, but this is more akin to a policy of 'data minimization' rather than complete 'amnesia'. Fortunately the regulation acknowledges this and the challenge is to make sure we are absolutely clear about which data is retained and the justification for doing so.

This is a good outcome relative to how the right to erasure was originally framed.

How could data protection regulation be improved further?

It's about moving beyond a legalistic framework that focuses narrowly on the 'geographic' location of data. This is where, perhaps, we could become more innovative. In practical terms this is about setting open standards in areas like encryption, and agreeing standards at a global level, rather than bluntly imposing EU standards.

In this context, Asia has a very different approach to privacy and Asian governments (and citizens) are seemingly comfortably with this. That said, creating a system whereby different regimes achieve what is called 'adequacy' is likely to prove extremely challenging.

How does the ePrivacy Regulation impact the implementation of GDPR?

The impact of the ePR is not as significant for financial services firms as for the telecom industry, but the changes to how cookies are treated and direct marketing is regulated, will have an impact.

Taking a broader perspective, as drafted, it looks incredibly ambitious as it is designed to be implemented at the same time as the GDPR; it carries similar sanctions in the form of fines, and is going to be monitored by the same regulator. The EU has literally 'GDPR-ed' the 2009 ePrivacy Directive which is a significant statement of intent.

That said, it is important to take a 'wait and see' approach to the ePR because this is a first draft, not the finished article. As breath-taking as it is in terms of its scope and ambition, it is an opening gambit. As we saw with the GDPR, it can be complex to develop legislation like this — the GDPR is a real example of legislation in a global world and all the tensions that that it gives rise to with respect to standard conflict of law issues.

How do politics impact how regulation is framed?

To understand data protection, you have to appreciate that it has become a 'political football'. Personal data has become politicized, and this has driven the agenda within the EU and internationally, and it will continue to drive this topic for the foreseeable future, because data is such an essential part of the world in which we live today. And in some cases, the politics are ruling over common sense and the legalities. The way in which the GDPR is written is specifically aimed at particular companies in particular sectors in particular jurisdictions. It's political.

As evidence of this, take for example, the passage of the GDPR itself. It is important to remember that the GDPR was on its knees in 2013 when the NSA scandal broke, and it was this that breathed new life into it.

While this gave a lot of impetus to how the GDPR was framed and eventually enacted, we have to acknowledge that there is a mountain of difference between wholesale surveillance and monitoring that might be carried out by institutions like the NSA, and sector-specific regulated activity with the purpose of safeguarding the international financial services sector and system. With the GDPR, this distinction is somewhat lost.

The profound irony here is that national security sits outside of data protection in the EU as well. This means that while personal data may not be handed over to government authorities outside of the EU, it can be handed over to governmental authorities within the EU.

How do changes in the administration in the U.S. and the process of Brexit impact the privacy/data protection debate?

As we discussed, a lot of the debate around privacy and data protection is political and to understand it, you need to put it into its geopolitical context. Given the level of uncertainty in the world today I fear it may get worse before it gets better.

As a specific example of this, take the Privacy Shield agreement between the EU and the U.S. For now, it is not clear whether it will be directly impacted by the change of administration in the U.S. but the statements by the administration so far indicate that there has been a change of mindset.

Brexit, on the other hand, is less of an issue, quite simply because on the current timetable, GDPR will be implemented before Brexit actually happens. The real challenge for the U.K. will be maintaining adequacy status after it leaves the EU and, although having already implemented GDPR will be helpful, it is not necessarily a guarantee that adequacy will be granted.

A Conversation with Mikko Niva

Group Privacy Officer, Vodafone

Mikko Niva is the Global Privacy Officer of Vodafone. He is responsible for Vodafone's privacy program globally. A lawyer by training, Mikko has spent most of his career at the intersection of policy, law and technology. He has extensive experience of managing privacy in complex global technology environment. Before joining Vodafone, he worked as the Group Privacy Officer for Nokia.

How is big data impacting Vodafone's business?

Vodafone is taking a balanced approach when it comes to big data. We clearly see the opportunity and benefits that big data can deliver, but also take the privacy dimension very seriously.

A lot of the discussion is focusing on big data as a separate revenue stream. At Vodafone, we take a different view where we see the opportunity in generating big data insights to serve our own customers better and to drive social good.

If we use data driven insights across our business well, it will not only improve the overall customer experience but will also drive lower churn, enable novel services, and make us more efficient. For example, it can help us detect areas of poor network coverage (e.g., high call drop-out) to improve our network infrastructure and, where necessary, compensate our customers if they have suffered poor connectivity.

Similarly, we should not ignore the potential for big data to be a force for social good. We're already looking at use cases in which it could be used to inform anything from the design of public transport infrastructure – for example the data driven insights we provided to the Welsh government to inform its motorway design (https://www.youtube.com/watch?v=fj353Sj8zdI) – to resource allocation when addressing pandemics or natural disasters, decisions which impact thousands if not millions of people.

How do Vodafone and the telecom industry approach privacy?

At Vodafone privacy is more than something we simply 'comply with'. Customers trust us with their data and we have to meet their expectations above and beyond what the law says. We approach privacy at a global level; all Vodafone companies are required to abide by certain privacy standards.

In practice this means several things, it means that senior management is actively involved in scrutinizing our global policy toward privacy and we have a privacy compliance program to make sure that policy is implemented in our local markets internationally. The program itself is delivered by our local market privacy officers or privacy teams who work with our group privacy team. Finally, we run group-wide audits to assess our compliance, the results of which are reported to senior management.

In the area of big data we have paid attention in particular to ensuring that with any proposed use case for data analytics we identify the potential risks and benefits to individuals or society upfront so that these risks can be managed at the outset.

How differentiated is the Vodafone approach to privacy within the industry?

We have done a lot of research on our customers' attitudes to privacy. Via the Vodafone Institute we have also done a lot of work on ethics and customer views, much of which is available publicly. A lot of this work shows that our customers not only care about privacy; they care about it in a nuanced way. For example in the area of big data they might be more willing to share their data for health, traffic, and

the environment but disapprove of the sharing of their data with third parties for commercial purposes.[34]

Our customers want to be informed on how their data is used and they want to exercise choice on how it is used. For us, there is a big aspiration to do more, to make our customers' life better, but to make sure that they understand what we are doing and are happy with what we are doing.

What specific actions do you plan to take in order to make sure you are compliant with the new GDPR requirements?

Protecting our customers' privacy has always been critical to us so the GDPR for us is more of an evolution of what we do already. The difference is that before the GDPR it was principally a question of reputation and company values; post-GDPR there are obviously more acute financial penalties associated with non-compliance.

We already have a group-wide GDPR implementation program which covers a number of changes that need to be implemented and a number of different workflows both at the local market and at group level. For example, there are technology implications in the sense that we need to make sure we have the right technology infrastructure to manage the data in a compliant manner. This is a really significant effort as it involves addressing our legacy systems as well as future technological development. For any company, especially those in technology, built up via years of acquisitions with a number of legacy systems, this is a sizeable challenge.

Are you looking at being GDPR compliant just in Europe or will it become a global standard?

We approach privacy at a global level; all Vodafone companies are expected to abide by certain privacy standards. When it comes to our customers we don't want to apply a mind-set of privacy 'haves' and privacy 'have-nots'. This said, there are some requirements under GDPR that are specific to the EU.

Which aspects of GDPR do you think represent the greatest implementation challenge for Vodafone/the industry?

The right to data portability (Article 20 GDPR) will present several implementation challenges to the telecoms industry as a whole unless it is properly scoped out. The Article 29 Working Party published draft guidelines (December 13, 2016 WP 242) late last year. However, these guidelines present a very broad interpretation of the wording of Article 20 – in particular the guidelines suggest that the data portability right should extend to data *generated by* a business about a customer; whereas the wording of Article 20 limits itself to data *provided by* the customer.

The data portability right has the potential to really benefit customers by allowing them to move their data between services and by encouraging a more competitive market as a whole. At the same time, we need to be aware of the practical impact it will have on issues such as protecting third-party personal data, sensitive data and vulnerable individuals; its impact on trade secrets; the security of data portability arrangements; and the technology and cost implications. Thought also needs to be given to its relationship with other legal obligations. Getting the correct scope is key.

[34] http://www.vodafone-institut.de/researcharticle/transparency-and-user-control-critical-to-success-of-big-data/)

Do you see any challenges from the revised ePrivacy directive?

The telecoms industry position has been that the current ePrivacy directive is not technology neutral in the sense that other forms of communications services – in particular internet-based communication services – are excluded from the ePrivacy's scope. Our view is that all communications services should be subject to the same obligations; a consumer should benefit from the same legal protections, regardless of how their communications are delivered. This issue seems to have been recognized in the Commission's legislative proposal for a new ePrivacy regulation.

In the area of big data it is important that the new regulation strikes the right balance between allowing technological and commercial innovation and protecting the privacy of EU citizens and the confidentiality of their communications. The real advantages to consumers and society at large that big data can bring should not be ignored. In our view the legal framework in the GDPR strikes this balance because it allows data analytics, provided that appropriate privacy safeguards are adopted, such as pseudonymization or anonymization.

Could privacy-related regulation reduce the opportunity from data?

Not necessarily, but our aim has been to make sure that regulators are aware of the issues that arise from greater regulation. We need to make sure that everyone works to the same rules. There are strong views on all sides and we think it is very important that the appropriate protections are in place. We need to make sure the policy is workable in practice.

Which aspects of the GDPR do you see as potentially being helpful longer term?

We were happy to see that pseudonymization of data has made its way into the GDPR in a way that protects privacy but enables data to be used in an analytics setting. That said it is important that we ensure that when we anonymize or pseudonymize data we do it properly. Therefore, we put a lot of focus on ensuring that we have the right technology, security and organizational measures in place to complete the task.

A Conversation with Andrew Brem

Chief Digital Officer, Aviva

Andrew Brem is Chief Digital Officer of Aviva. Andrew joined Aviva in December 2014 as chief digital officer. Andrew is accountable for driving Aviva's group-wide digital transformation which is having a significant impact on every aspect of interactions with customers, including product innovation, distribution, communication, claims handling, marketing and branding. Andrew is also a board member of Founders Factory, a leading multi-sector digital accelerator and incubator. Andrew's previous roles include launching Hive, the Connected Homes division of British Gas and leading the multichannel ecommerce and services businesses at Carphone Warehouse. His early career was in strategy consulting at McKinsey, where he worked on a broad range of assignments in retail and consumer businesses across the globe.

Andrew holds a first class degree in philosophy, politics and economics and an MSc in the economics of developing countries from Oxford University. Andrew also has an MBA from INSEAD, France.

How is big data impacting Aviva's business?

Data is the lifeblood of our industry. This is the most existential question in our industry currently. If we believe that public data and third-party data – in larger volumes and variety – can better price risk than traditional sources of data, then there are two big questions that arise:

The first is whether the spread of risk changes with better access to data. For example, do two people who previously looked identical in terms of risk, based on traditional questions, suddenly no longer look remotely identical from a risk and pricing perspective? The whole basis of insurance is to create pools of individuals or assets that face similar levels of risk; where the difference in risk between those people or assets is essentially random. And the bigger the pool, the better. If big data means we can better gauge risk and therefore split risks into ever smaller pools, price differentials might vary significantly. Conceivably this might even make some people/segments uninsurable, as greater visibility on risk means there will be higher costs to price that risk. Our view is that we are a long way from that. In general insurance, our sense is that 'perfect' information would somewhat increase the variance in risk and price, but a large part will remain essentially random. In life and health insurance, however, we might be facing a major problem. The likes of DNA sequencing, for example, mean that in a relatively short period of time we will have much better information about susceptibility to disease, and therefore the risk of a life or health claim, and this could be a substantial problem for our industry and for society.

To the extent that big data drives a much finer measure of the risks facing individual people or assets, it potentially undermines the notion of pooling similar risks, because it would reveal that actually there is cross-subsidy within the pool: for every person who gets a better price because the data reveals them to be lower risk, someone else in the pool is getting a higher price. There is a tension here as it feels ethically and commercially right to give a lower price to those revealing themselves as having lower risk – but obviously this has an impact on people carrying a higher risk, which may not be a risk that they control. This has much bigger ramifications for society and we want to work with government and regulators to address this.

The second question is whether the insurance companies are the very best people to access, aggregate, and analyze the data. The insurance industry's position is not a right, so we have to work very hard to make sure that we can build the technological capacity to do this and earn consumers' trust. Insurance companies need to be the best at risk analytics, as this is our crown jewel. There are start-ups and big data companies out there crunching through data to work out risk. One key advantage we have is that we do have the claims data which is proprietary and which is very important in terms of determining whether our hypotheses about risk relationships are correct.

What data, if any, are you missing when it comes to public data?

Public data is going to become more and more important in pricing risk, and if public data can be as effective as private data then this represents a potential threat to the model of the incumbents. The barriers to fully exploiting this opportunity are in the first instance broader privacy issues and in the second instance correlating that with the traditional proprietary data sets, in particular claims data.

The reason we are looking at non-traditional sources of data isn't just about pricing risk but also about ultra-convenience for consumers. The way consumers purchase insurance is still very much like it was in the 1980s. They contact insurance companies and get a quote on the basis of a lengthy questionnaire. Using public data allows us to offer a better customer experience as it will enable Aviva to pre-populate information and even pre-price risk. This will be more convenient for customers as each interaction will be easier but also more personalized. For example, via the My Aviva digital platform, if we have a customer that takes a pension product, we will be able give customers a snapshot of what other services might be available and at what price without having to go through a drawn out quotation process. This means we can present personalized products while being transparent with customers about what Aviva knows.

We have also found interesting risk relationships between products that generally haven't previously been used in pricing. For example, we might hypothesize that people who diligently lock their doors and windows at home are also more careful when they go out driving…but it might also be the case that people who display particular behaviors when saving for retirement have distinct risk profiles in general insurance. Existing customers with a deeper relationship with Aviva have better risk all around. This is something that should benefit both us as an insurance company but also, critically, the customer.

As a user of big data analytics, what are the major challenges that you struggle with to exploit the opportunity?

Technology and talent. Data scientists do see the attraction of the insurance industry; it is a treasure trove for data. When you talk about data and insurance you naturally think about pricing and fraud analytics – but customer analytics is just as important, e.g., for segmentation, programmatic marketing, and deep customer insight to design products. In our industry big data has not sufficiently been applied to the customer analytics side, but it needs to be.

How does Aviva approach data protection and privacy?

There is an issue for the entire digital industry which is that consumers, in general, are not highly engaged and not very well informed on data protection and privacy; most consumers have limited appetite to get into the detail of privacy policies. But it is critical that consumers do understand and consent to the use of their data, and the digital industry needs to make this easier for them. We want to work with regulators and policy makers to address this.

Take for example the cookie consents mandated by the 2009 ePrivacy directive. Individual consumers may or may not accept cookies as a blanket approach, but it is not clear that consumers actively engage with the detail of individual companies' privacy policies. The same applies to 'Terms and Conditions' in insurance contracts. So the challenge, for us, is to make sure that we get proper 'informed' consent. We want people to think about what they are doing. We are looking internally to experiment with different ways to present what we are asking customers in order to maximize the level of knowledge.

When we talk to customers about data privacy, what they particularly react against is selling data to third parties. Aviva does not sell customer data. Security of data systems is also of paramount importance to customers.

One interesting aspect of the privacy debate is that different generations have very different approaches. Millennials, as a generalization, tend to be more relaxed about some of the issues around data but, in return, also tend to have higher expectations of what this more relaxed approach should mean for them in terms of access to products or indeed price. Other customer segments are not supportive of that.

Data debates are somewhat reminiscent of the debates on what constitutes 'advice'. The danger is that you throw the baby out with the bath water by being too constrained, e.g., a consumer really wants help with savings or investments but the industry is so worried about staying the right side of the regulations that it gives none. At a senior level, regulators in the U.K. understand these challenges and want to fix them.

What specific actions do you plan to take in order to make sure you are compliant with the new GDPR requirements?

We have a lot of people working on the challenges associated with implementation of GDPR. The challenge for us is that there are elements of the GDPR where there is still ambiguity.

Which aspects of GDPR do you think represent the greatest implementation challenge for Aviva/the industry?

Implementing a 'right to erasure' will be a challenge for the industry for a couple of reasons. First, the variety and age of much of the database technology used across the industry means that any technical change can be time-consuming and costly. Secondly, from a consumer perspective it's likely to prove challenging to explain exactly what rights the GDPR offers – the legislation is quite specific, rather than the blanket 'right to be forgotten' that's in the public mind.

Are there any aspects of the GDPR that are helpful to the insurance industry longer term?

An interesting area is the right to data portability. If consumers are able to transfer their data between companies seamlessly, they can be more demanding with all financial services providers. We see this leading to more effective competition and better incentives for the industry to create great products – this is something we always welcome.

A Conversation with Andrew McClelland

Head of Industry Insight, Interactive Media in Retail Group (IMRG)

Andrew McClelland has been involved in digital commerce for over 14 years and having held senior roles at e-Retail trade body IMRG, has a unique insight into the development of digital enabled commerce, changing consumer trends and the challenges that incorporating a digital offering into a more traditional proposition presents. He now runs his own consultancy, Mirador Digital, to work with clients to develop and deliver strategic planning and review for digital channels, provide digital insight to private and public sector organizations.

Note: These comments are the personal views of Andrew McClelland and do not represent the view of either the industry or IMRG.

Would you say that data protection and privacy was something that retailers have been quite on top of? What is the current approach?

Data protection is taken very seriously by all businesses, in general, due to the combination of potential for bad press, customer relations, financial impact, and brand damage if things go wrong. This is especially the case for retail where the customer is very fickle, not locked into long-term contracts, and there is a limited grace period to rebuild fences, and every customer interaction could involve payment. So, data protection, at most retailers, is fairly engrained into corporate policy.

It is hard to make a sweeping generalization across the industry in terms of approach. There are some businesses which have gone about data protection the wrong way. For example, they engaged certain technologies for data processing and signing contracts with a third-party supplier before they have got legal input on how it may impact exposure on data protection.

Around 10 years ago our data protection requirements were fairly straightforward. In the last five years you have seen that change with the advent of retargeting, behavioral advertising, personalized services to consumers – that has probably forced the pace of adoption of a lot of practices. You could call into doubt some of the ways we have tried to achieve the objectives. There has always been this conflict between commercial and legal. What we are seeing, increasingly, is legal teams becoming more focused on their interpretation of legislation in commercial terms, and getting more involved to help the business be a retailer – not just a compliance check box any more. There is probably more of an understanding from the commercial side that you have to be sensitive to it also. There is some benefit from consumer trust if we do this in the right way.

What are retailers putting in place in response to GDPR?

I have not seen evidence of a common way of doing things at the moment. A lot of them are still working out how it will work. Some of the new regulation has been fairly woolly – the guidance from the data protection authorities is still coming. There are still a lot of areas of uncertainty, such as whether I need a data protection officer. It is fairly safe to say the big multichannel high street brands will need a data protection officer. It is less clear for mid-tier retailers because what does ‘large scale’ mean, and that’s a requirement for having a data protection officer (DPO) is if you are a large scale data processor. Some of the terms are vague. If you read the rules there is a grey area around large scale processing - a small business could argue it isn’t a large scale data processer. The minute you have a DPO, then you fall under the jurisdiction of all the rules.

Is there a difference in approach between large and small retailers? And between offline and online retailers?

The bigger retailers will be aware of the scope of work required in response to the GDPR. The smaller retailers – I wonder how many are aware what data protection really means. For example, if they start to use a voucher website and they hand over their customer database to do some marketing, have they thought about what the implications are for them as a business, have they got consent from customers to do it, and is the voucher website checking? There is probably a lack of understanding in the first place.

We are also moving to an environment where you won't have to register with the ICO to be able to handle personal data. How many small retailers are even aware they must be registered at the moment? From May next year this requirement is lifted which means the regulator may be a step further away from the coalface, so will the new and smaller businesses know about these requirements? They will need to be advised.

I think that some of the smaller pure plays are less likely to have a full awareness as they have been technology driven. Whereas the multichannel retailer physically sees their customers daily and so it is a real person, rather than just a dataset. Larger pure plays are much more aware of the requirements and probably have a better feel for the intricacies of the changing rules than some of their multi-channel peers.

Retailers have used relationships to drive other services e.g. insurance, banking – do you think this could have an impact on that?

If you look at the basic tenets of GDPR, they are not so far removed from what we are doing currently. Yes, there are some headline grabbing areas but the underlying idea around data protection by design isn't a new concept, it's just been raised up the agenda. That's a reflection of how technology is enabling us to do more with information and data than we have ever been able to in the past. It's a natural progression.

In terms of implementation of the GDPR, is there anything that stands out as particularly challenging for the retail sector?

The challenge for a lot of businesses is going to be that the current status around what constitutes personal data is changing from the current regulation to the GDPR. Some clarity is coming through case law anyway. There is a better understanding that IP addresses, for example, can constitute personal data.

There are some new areas where there may be room for concern. One of those is 'right to be forgotten'. When you look at the circumstances in which a customer can ask to be forgotten I don't think it will impact retail that heavily. Certain elements around loyalty programs could present a risk but a more interesting debate is what data has to be disposed of - just because we think it may not impact retail, it doesn't mean retail shouldn't have a plan. The ICO will expect us to have that plan in place. It is understanding the different types of data and what uses they have. For example, data provided by the customer would need to be forgotten, and some observed data about behavior on the website, e.g., what a customer has looked at, would also need to be forgotten. When a number of different data sets have been used to come up with our own conclusion about what you are like as a customer, the customer may have no right to ask for that to be forgotten.

The increasing use of cloud services is a challenge under the GDPR – where does the data reside and who has access to it? If a retailer is using a cloud service and the database is sat in a European city but the 24/7 support centers are based around the world, and they have access to that information, then technically the processor is outside of the EU. Contractually how does the retailer sit with those companies – some of them will be so big that the retailer can't push its own terms. Are there additional things the retailer can put in place to protect itself and its customers? Increasingly, a lot of those cloud providers understand this challenge and are starting to put contracts in place to become compliant as well. In general, retailers will be asking 'are my suppliers aware of the requirements', e.g., if marketing is handled by a third party.

These concerns are probably more of a legal pondering at the moment as the commercial guys won't have looked at it. They will see them as marketing tools. For a non-legal person the concept is quite abstract.

I think consent models, in terms of how we move forward from here to get consent, and how we review the customer database, is a challenge. Don't underestimate the scale of the challenge the businesses face, particularly if they are early on in the process and the concern around how to deal with it. If a retailer has a large database of several million, they are asking if they will have to contact each individual to get consent. We don't know.

If I am CEO, all of a sudden the penalties have gone up to 4% of global annual turnover. That's a huge hit by any stretch. Compliance is one issue, and you may tick all the boxes in terms of private Internet Access (PIAs), but what if a contractor comes in and leaves a port open on a server, enabling someone to come in and take that data. That's the bit which is scary.

The majority of the change needs to be cultural, rather than box ticking. Everyone needs to understand that this is important. For example, a marketing manager may be incentivized based purely on the number of email addresses in the database, and that does not sit comfortably with the GDPR. Currently the understanding has not seeped through culturally.

The journey getting from here to there could well be bumpy.

What do you think could be the longer term benefits of the GDPR for the industry?

I think there is always a tension between compliance and commercial, particularly around the marketing element, and more often around how obvious consent is gained. The GDPR is moving us towards a regime of active consent, and from a marketing perspective, over time that means our databases will be more valuable to us. There is possibly a challenge within industry where some marketing functions have been incentivized by developing a massive database of prospects. There is also a counter argument – if the customer doesn't know they have given consent, is that data worthwhile in the first place?

In a lot of ways the GDPR brings a level of finesse to the industry which means, through compliance, we can actually improve the level of performance of the data we hold. There is a big drive towards collecting data on all sorts of things, and there's a school of thought that the more data we have, the more efficient we can be, and more active we can be in the marketplace. That works to a point. I am a big advocate of only collecting data that you can use, and having tangible outputs from collecting that information, and when the outputs change you need to reassess what data you are collecting.

Even if the cost of collecting that data is cheap, in financial terms, there's still a cost of maintaining that data, especially customer data. Where we are moving to is a very exciting world of being able to measure customer behavior, target customers, and increase engagement, the ability to have a lot more analytical tools leading to personalization, and most customers like that as well. There is so much choice online now that the ability for retailers to co-ordinate, create discovery paths, curate the customer experience – when you go to a retailer's website for the first time it's a fairly blank sheet of paper, so how can you build on that.

Technology is helping curate the product selection to customers, especially in the digital world where the costs of customer acquisition and retention are rising. It makes a lot of sense to maximize the use of the existing database around insight and understanding the customer, and all of that can provide great service to the customer. The problem is the industry isn't as open as it could be with the customer about what it is trying to do — we are often scared of telling our customers of what those benefits might be, such as 'we might share data for promotional purposes etc.', as that involves highlighting that data is shared with third parties. Retailers should be telling them – if it's around personalization, we do that by telling customers we want to share their information with third parties so we can ensure we provide the right product offer and so retailers won't have to contact customers as often, but when we do contact customers it will be more relevant. Retailers need to get into the situation of taking the customer on the journey with them, and not delude and coerce them. Customers will appreciate that level of service but it is a journey, we don't want to spook customers who don't understand the technology and benefits as well as we do.

There are some really bad examples of retargeting. Having the technology is one thing, but understanding what the boundaries are is just as important. Knowing a little bit about your customer and making sweeping generalizations in the name of personalization is worse than not knowing anything.

If the industry can curate the product selection to help guide the customers, it is important – a retailer spends a lot of money to get customers to shop with them. Looking for more than one relationship with a customer is when the retailer can start looking for the return.

Retailers are asking about how to have a conversation with the customer in the first place, and when to have it. With data protection there is a benefit, perceived and actual, to the customers to collect their choices clearly so more benefit can be provided in the long term. It is knowing when to ask those questions and when to deliver the service. It is about getting a balance. This isn't necessarily about the GDPR per se. For example, if you want to talk to a customer via their mobile phone then make sure the customer has a clear understanding of what you are going to do – there will be nothing worse than walking into a shopping center and the customer's phone pinging saying 'we know you are near our shop, come and see us' if they are not expecting that level of service. Having access to rich data enables retailers to make those judgment calls and enables them to serve those services at the appropriate time.

Retailers have a face to face relationship but with near field communication (NFC) payments retailers worry they are getting disintermediated between them and the customer at the point of checkout. That is the remaining contact point where you stand in front of a member of staff – that is an opportunity to talk to the customer. A quick swipe of the phone means the customer has paid and gone. How can you extend the opportunity to have a conversation? Loyalty cards are one way, and the other is getting more staff onto the shop floor to engage and speak to customers earlier in the store.

I think the benefit, for most retailers operating on a European level is the GDPR harmonizes a lot of regulation. It is not 100% but it is getting fairly close. It makes it easier.

What are the implications of the proposed ePrivacy regulation?

We still need to see what it will look like and how it will sit alongside GDPR.

There is a welcome reconsideration around the cookies element of it and how we gain consent. More broadly, there is an ongoing debate around what is personal data.

A Conversation with Simon McDougall (MD) & John Bowman (Senior Principal)

Promontory Financial Group, an IBM Company

Simon McDougall leads Promontory's global privacy and data protection practice, advising firms on governance, risk, and regulatory issues related to their data and records. Simon helps organizations obtain greater value from the data they own, providing practical and proactive solutions that follow the latest legal and regulatory requirement and enable businesses to use personal information properly in the interests of their organization.

Simon is a U.K. chartered accountant and worked in Deloitte's audit and technology risk unit before joining Promontory's regulatory consulting practice. He has particular experience in building data protection programs in large organizations, advising on integrating privacy into large projects, and undertaking data protection compliance reviews. Simon has direct experience as a data protection officer through a six-month secondment to a large U.K.-based bank.

John Bowman advises clients on all aspects of compliance with data-protection laws and regulations. He is a specialist on the European Union's General Data Protection Regulation.

Prior to joining Promontory, John worked at the U.K. Ministry of Justice, where he was the head of EU and international data-protection policy and lead negotiator on the GDPR at the EU Council's DAPIX working group in Brussels. John also represented the U.K. at the European Commission's Article 31 Committee, which is responsible for determining the adequacy of non-EU data-protection regimes.

By sector, how is privacy and data protection currently approached pre GDPR?

If you are going to consider which industries have been most engaged with data protection to date, simply look at the volume of personal data being handled and how sensitive that processing is. If it's something like healthcare, it's very sensitive data and important things are being done with it; it's a matter of life and death. If you are looking at something like retail banking, you have a huge volume of data, some of it quite mundane and some of it quite personal to people.

We usually work with firms that have some kind of retail footprint or some kind of live data being handled at scale. How these firms handle the data is very important to their customers. The main sectors we see that are engaged today are financial services, life sciences and healthcare, retail, tech, and social media. You also have public sector entities such as the National Health Service and the Department for Work and Pensions, which hold enormous amounts of data.

What priority does privacy and data protection have within organizations?

It varies significantly by sector and by companies within the sector.

Some companies have aligned the management of their brand and building customer trust with how privacy is handled. This makes sense because privacy regulation already covers the full information life-cycle – what you are going to be saying to people about how you use their data, how you keep those promises, making sure data is kept secure along the way – all these things matter to people.

There are other organizations that have taken quite legalistic and reductive approaches and said, 'OK, here are the rules, and how do we comply with them?'

We have seen quite a lot of disparity between peer organizations where one has really invested and another hasn't. It is not always the case that higher-profile brands and those with heavier retail presence have invested more heavily in privacy and data protection.

This partly reflects that we are in a market that, in some respects, is immature. If you compare where privacy is relative to information security, it is probably about 5-10 years behind, but privacy is absolutely on a curve. The privacy functions within organizations are getting more responsibility and more funding.

What specific actions are you advising companies to take to ensure compliance with the GDPR and ePrivacy Directive?

The GDPR represents change for everyone, even if they have a good framework in place. If they don't have anything in place, then there's considerably more effort required. The GDPR is an enhancement of the existing directive, so none of it should really come as a surprise, apart from a few brand new requirements like data portability.

We advise companies to take stock of the current situation and to what extent they have a mature framework in terms of compliance with the current directive and member state laws in Europe. In other words, we advise them to do an assessment or gap analysis.

They can then decide whether they will handle it internally with change program management teams or contract external services. We do things like readiness assessments and scoping, and the readiness assessment will contain recommendations on working toward compliance (as 100% compliance may be difficult to achieve, if not impossible) through to 2018, and then beyond.

Also, the development of artificial intelligence could help companies prepare for regulation.

Does the GDPR widen the net in terms of sectors/companies which need to take it into account?

Yes. There are some sectors that are reasonably good at this, such as financial services, as they are used to operating in a heavily regulated environment. The institutions often have compliance and EU teams that look at every single regulation and think about what it means to them. The industry associations in banking circles have been active in trying to set out what it means within financial services.

There might be a lot of companies out there that start off as small businesses and are data driven, and then suddenly they have growth. With growth, they have to take on the burden of regulatory compliance as well. They may not realize that in developing apps for phones, for example, that they need to give data protection rights and obligations greater thought. It might be more difficult for them to scale and acquire the expertise to be able to do that. You see it in payments, FinTech, media, games, and anything that uses an online platform.

Which areas of the GDPR present the greatest challenges for corporates?

One of the challenges is the consent requirement, the idea that consent has to be unambiguous. You can't infer consent on the basis that someone hasn't opted out of an agreement. Individuals have to effectively opt in and demonstrate that they have freely given their consent to processing.

The cookie consent, which was as a result of when the ePrivacy Directive was last amended, brought the concept of consent into everyone's lives. Are people going to read all the terms and conditions, and is the cookie consent popping up distracting to the web-surfing experience? It does raise questions about how informed people are when they provide consent. Are they just ticking a box to get rid of it, or are they reading the information? The data protection notices say individuals have to be given information about processing in a clear, concise, and easily digestible manner. This can be quite difficult when you consider the concept of data being pseudonymized, for example, or how to manage the logic behind an automated decision. Automated decision making is allowed if you have explicit consent, a higher level of consent, but that level is yet to be defined.

Another key challenge is the 72-hour breach notification, which is considered to be particularly challenging for large organizations where it might take time to investigate the breach, including what the source was and who is impacted. Providing all the information in the required timeframe to the Data Protection Authority (DPA) can be very challenging as the company may not have a complete or even a minimal picture of what is going on that early on in the investigation. If the

management first learns about the breach when picking up a newspaper in the morning, then it may be in the public domain before the company is aware. Yet the clock already has started ticking.

Companies pay a lot of attention to things like cyber-attacks and internal information security, as it is clearly a threat. There may be a disproportionate emphasis on that, however, vs. standard controls, such as clear desk policies, showing passes, etc. Information security should be considered along with the protection of data. It ties into a broader debate about internal controls, compliance, and culture.

The other challenge is data retention. It is difficult for large, complex organizations to curate their data. It might have been collected over many years or many decades. It might be structured in terms of database, and it might be unstructured in terms of spreadsheets and lots of paper files. When a business says, 'By the way, we've got a warehouse of paper files, and no one knows what's in there,' this raises concern about records management. What the GDPR says on retention is you don't retain data for longer than is necessary for the purposes of the processing. There is a data minimization principle and a purpose limitation principle; you can't carry on processing data without re-obtaining consent or having other legitimate grounds for processing. GDPR also states that data minimization can contribute to data protection by design and by default, so active management of the data life-cycle is considered important.

Data that has not been deleted becomes inaccurate over time. The more you have of it, the more exposed you may be in terms of a breach. A lot of companies are saying, 'We have lots of data, and we don't really know where it all is.' Some organizations have systems that don't seem to allow you to delete data categorically. The individuals have to be informed about how long the data will be retained for and the criteria that will be applied to the retention of the data.

If you are using the cloud, then the cloud provider is often a data processor, and it should be acting under your instruction. If you opt to delete the data, it should follow your instruction. Data controllers have to be assured that the data processor is doing these things, and they can go in and audit and demand evidence that the contract is being adhered to. The other issue with cloud is whether data is being transferred outside of the EU and whether there is an appropriate safeguard in place to protect that data, including when there is further onward transmission of the data.

This leads on to the area of international data transfers, which is controversial. Obviously, the Privacy Shield has replaced Safe Harbor (a data transfer agreement between the U.S. and Europe). There are only 11 countries or territories with the adequacy status currently, which allows free flow of data between the EU and those countries. Some of these adequate countries may be processing data for national security purposes, which is effectively the issue which brought down Safe Harbor. This may be a consideration once all adequate regimes are subject to a regular review under the GDPR.

Data portability is an interesting question as it doesn't really reflect a data protection right as such; it is more of a consumer empowerment measure. It allows people to extract their data; and they may be able to gain some kind of value – for example, market comparison for better deals.

The challenge of data portability is around the format of the data file and security; you don't want people to be socially engineered to divulge their data and then it be acquired by a dubious party. Companies may set up systems and then get only 10 requests a year; at the same time, they might get millions of requests. How is that addressed – do you put a self-service portal on the website? How do you inform people of their right to portability? You might get organizations encouraging campaigns on it, as well. It is a step into the unknown.

Companies will have to consider the requirement for a Data Protection Officer (DPO) and how that fits into the organization. It isn't a conventional audit or compliance role, although there are elements of both. The added angle is where consumers can contact the DPO directly, and the DPO is potentially an advocate for those consumers. The DPO must have access to senior management and can't take instruction on how to carry out duties. Businesses will be looking closely at how the DPO role evolves.

Which area do you think is most likely to lead to a fine?

The biggest fines will be around breaches. It won't necessarily be for not notifying the Data Protection Authorities (DPA), but it is more likely to be for the breaches themselves. When the investigation is happening, the DPA will look at what policies, controls and processes, and technical safeguards were put in place. If you have been noncompliant all along, the fine is likely to be worse.

How will the GDPR be policed and how active will the DPAs be in chasing full compliance?

It will probably be ad hoc and reactive to a large extent, but not totally. There will likely be investigations programs. For example, the German regulator decided to select 500 companies and examine their data transfer mechanism. The companies were picked based on certain criteria. There are some companies under the spotlight continuously anyway, either because of the regulator's perception of them or because of activism. Activism will emerge even more, as it did during the GDPR negotiations. It could be an interesting angle because a group could campaign and could capture the attention of the regulator.

Is there anything in the GDPR which will be helpful longer term?

It does harmonize the rules to some extent, although they aren't 100% harmonized. It also will be easier for businesses to operate across Europe.

Implications for Industries, Corporates & Investors

Implications for Industries

U.S. Internet

Mark May,
U.S. Internet Analyst

There are many elements of the pending new data protection and privacy regulations in Europe, and the final details, implementation, and impact are still largely unknown. That said, we see five main issues potentially having the greatest impact on the U.S.-based consumer Internet companies operating in Europe:

1. **Consent:** The new regulations require different and potentially more restrictive rules pertaining to the use of data for personalizing the online experience for Internet users, including the targeting of advertisements. Companies may need to first get explicit consent before using personal data for certain purposes, especially when using third-party data for 'non-essential' purposes. Moreover, consent settings may default to opt-out, and require users to opt-in (and in some cases potentially in situations they currently don't have to). Browser settings may now play a bigger role than in in-line banner ad cookie notifications, but how compliance with the rule will be achieved remains uncertain.

   Additionally, the new regulation related to data pertains to the need to get content from parents for younger users (i.e., below 16 years old, which is more restrictive than the 13 year mark for similar regulations in the U.S.). Again, the process that companies will use to get consent is still uncertain.

   IMPLICATION: The new consent requirements could have the impact of hampering the personalization of online services and creating a headwind to monetization (revenue). While we believe this represents a potential incremental negative for companies like Facebook and Alphabet/Google, larger companies that operate multiple essential online services will likely be advantaged over smaller players that operate fewer and/or less essential services as they may have a harder time convincing users to consent.

   This age-based consent rule could have the impact, of course, on properties whose demographics skew younger (e.g., Facebook's Instagram).

2. **Wider Net:** The GDPR expands the number and type of services included under its purview. Notably, messaging apps (e.g., Facebook's WhatsApp and Messenger) and cloud service providers (e.g., Amazon's AWS) are now covered by many elements of the new regulations. Cloud providers, for instance, are considered 'data processors' and they now have certain data privacy and protection responsibilities and liabilities. The increased focus on data privacy and protection as it relates to messaging apps can be seen in the recent pushback to Facebook's efforts to increase data sharing between its WhatsApp messaging app and its core Facebook platform. For both messaging app operators and cloud service providers, the new regulations have the potential to stymie innovation and increase financial liability. That said, the key owners of these platforms are large and well-financed, and have already been taking steps to meet these new rules both in practice and in spirit.

   IMPLICATION: New services, like Facebook's WhatsApp and Amazon's AWS, will now have to ensure compliance with new data privacy and protection rules, which could increase costs and potential liabilities. That

said, given the increased resources required to ensure compliance, the new regulations could also benefit large incumbents and make it harder for smaller players and startups.

3. **Fines:** The new GDPR introduces a more well-defined and relatively large potential fine for violation of its rules. In short, the regulation allows for fines of up to 4% of a company's global annual turnover (sales) for being found to have breached the data protection rules.

   IMPLICATION: The new framework for penalties and fines represents an incremental new risk for covered companies. While the potential penalties are sizable, especially for larger companies, the larger companies also have an advantage over smaller companies in terms of resources to ensure compliance.

4. **Faster Notifications:** A new element of the rules is a requirement for covered companies to notify the relevant supervisory authority of serious data breaches in a short time frame (i.e., within 72 hours).

   IMPLICATION: Covered companies (e.g., Amazon, Alphabet/Google, Facebook, Twitter, etc.) will likely have to implement new processes to enable them to assess and report on data issues more quickly. In addition, the requirement to notify faster could also create public relations risks, as companies may not only have to report more widely and frequently but they may also need to provide notification before they have full information about the issue.

5. **Rule Consistency:** Referred to as the "one-stop shop" goal, a key tenant of the revised regulations is to streamline and codify the 'rules of the road' across each European country.

   IMPLICATION: In theory the new GDPR codifies consistent regulations across all member states and should make it easier (and cheaper?) for all parties to comply with rules and regulations and to manage issues as they surface.

U.S. Small & Mid Cap Internet

Mark Kelley
U.S. SMID Internet Analyst

The regulations that take effect in 2018 will most certainly impact the online advertising ecosystem, to which many in SMID internet are exposed. For those most at risk, we would highlight content providers (all forms of digital) that have a "free" ad-based tier, as well as the entire adtech group, which relies heavily on both first- and third-party data. At first blush, one might come to the conclusion that any business model that can only function with third-party data would completely falter, but we believe this paints a story that is too black and white. For one, this would put far more power back into the hands of the largest Internet properties in existence (a sentiment that coincides with our colleague Mark May's thoughts) and would run counter to much of the anti-trust/regulatory language coming out of the EU for quite some time. Second, there is an entire group of heavily trafficked publishers that rely, at least in part, on third-party ad exchanges and, in turn, third-party sources of demand for their advertising inventory. As evidenced in some of the survey work above, we believe when consumers are faced with a choice between paying for a subscription to their favorite site(s) and content providers or receiving their content for "free" if they allow that publisher to sell advertising when they're consuming content, most tend to choose the latter.

The bottom line from our perspective is that the entire Internet relies on third-party trackers in some form (even the largest internet companies), whether it's for placing a value on an advertisement (data allows advertisers to estimate return-on-investment (ROI) based on age, sex, etc.), or for measurement purposes after an ad is purchased/served (did the consumer see the ad? For how long?). There is also a gray area when determining what "first-party" data is (would the data collected by an ad tech company that is hired by an ecommerce site and allowed to follow its consumers be considered first- or third-party data?), and we would expect some clarity from the regulators as we get closer to implementation – our case studies above suggest there is still room for specifics to be defined between now and then. We will be watching closely as these ambiguities are ironed out over the next year.

Global Software

Walter H. Pritchard, CFA
U.S. Software Analyst

In the software sector, we see impacts from GDPR in three main ways.

First, along with personal control over data and other changes to how consumers are tracked, the regulations are paired with greater implications of data breaches and leakage of consumer information. We expect and are already hearing participants in the IT security ecosystem targeting the opportunity associated with increased corporate spend to help better security infrastructure to prevent breach.

Second, we believe that with the structure around tracking and targeting consumers requiring standard and documented procedures, automation of this with software is likely to be key to ensuring compliance. We understand that competitive digital marketing software platforms are building in GDPR compliance to be able to target buyers in Europe as they drive towards compliance and potentially re-platform for 2018

Lastly, we see vendors of software data platforms (database, data warehouse, Hadoop, etc.), including cloud platforms, benefitting from continued growth in consumer data and the emergence of new business models of companies using this data to make money. Despite GDPR, we expect growth in data volumes to continue, in support of the transition to digital business models in a broad range of industries. We expect these data platforms can benefit from additional spend on GDPR compliance as we expect from the digital marketing platforms.

FinTech

Josh Levin, CFA
EMEA FinTech Analyst

The GDPR comes at an interesting time for European FinTech. Just as European regulators are enforcing stringent data protection requirements, other regulators will soon require banks in the EU --- with the customer's consent --- to share customer data with third parties. Payment Services Directive 2 (PSD2), the directive that mandates this data sharing, will take effect in 2018 and is designed to promote competition and innovation in the financial services space.

Banks have historically viewed customer data more as a liability than an asset. That is, banks have been primarily concerned about protecting customer data from breaches. As such, although banks have access to lots of data about their customers, by and large they have not developed new and innovative products with this data. Most banking technology on the consumer side is limited to online banking services. Sensing that the banks might not be up to the task without a competitive push, PSD2 seeks to lower the barriers to entry for companies which can in fact innovate.

The question arises: to what extent do GDPR and PSD2 conflict or complement one another? On the one hand, to what extent will the burden of complying with GDPR discourage companies – established or start-ups – from taking advantage of PSD2? On the other hand, are the GDPR and PSD2 working towards the same end, namely that consumers can take ownership of their own data and allow third parties to use it only with their consent?

Many banks in the EU may be ill-prepared to deal with the GDPR's stringent requirements. The possible beneficiary of that ill-preparedness may be FinTech companies which can sell their services and products to banks in order to help them comply.

Payments, Processors & IT Services

Ashwin Shirvaikar, CFA
U.S. Payments, Processors & IT Services Analyst

Most large corporates today operate a patchwork of IT systems and hybrid automated/manual processes. In the past couple of years, the incidence of digital assets has grown, combined with the increased penetration of cloud-based delivery – but it has not led to the widespread replacement / retirement of legacy systems yet. Moreover the rapid growth of data sources described in this report continues to add to the complexity of the overall set-up.

With this as a backdrop, IT consulting and business process outsourcing (BPO) firms have started calling out the fact that the GDPR deadline is little more than a year away as a "burning platform" that must be exploited to overhaul systems, processes and data flows, especially given the penalty for non-compliance will be up to 4% of global annual turnover or €20 million, whichever figure is higher.

One aspect of this push is defensive in nature, i.e., the implementation of RegTech (described earlier in the report). It begins with a process of understanding where the corporate stands with regards the information of its EU-based clients. For example, banks have to understand how their national systems differ from the desired end-state before the process of upgrading the system can begin. Job listings with the word "Privacy" in them are rising, e.g., Data Privacy Consultant. BPO firms are targeting known areas of friction, like paper-based processes and documentation as well as the need to cleanse existing data as areas of the business that must be immediately changed. Putting in new data governance systems to comply with regulations and internal processes, ensure consistency of data definitions, eliminate redundant data sources and using standardized software packages are all important steps.

But there is also offense to be played. This involves accelerating a push to digitize the core systems and processes of an enterprise, implementing newer data analytics systems, upgrading talent and eventually using automation and AI-based techniques to minimize the incidence of manual interfaces.

For payments companies as well, GDPR represents a cost (to comply with the legislation), a complexity in terms of the seemingly competing objectives of GDPR and PSD2 and an opportunity to sell GDPR-related compliance solutions in areas such as data encryption and cybersecurity, customer consent management and data-sharing, etc.

IT Hardware

Jim Suva, CPA
U.S. IT Hardware & Tech Supply Chain

The new changes to privacy and data protection regulations from the GDPR and proposed ePrivacy regulations will have profound implications for the IT Enterprise Hardware companies and the customers they serve. Large IT Enterprise firms must rethink their information management processes and focus more on the business processes as customers seek to better understand their data assets and the exposure risk they may be subject to. In the past, large IT Enterprise firms were critical data controllers, now they must transition to information service managers; evident in their acquisition appetites, focusing on the strategic pieces to pivot to the new complex environment.

Cybersecurity has become a board-level issue, where there is a growing need for C-suite and Boards to understand their security posture through the lens of business risk, not just the technical security data and metrics. Large IT Enterprise firms are growing both through organic and inorganic investments; focusing on cloud security, data protection & privacy, and business analytics. Traditionally the security model focused on individual systems, networks, and applications. Given the changing landscape companies find themselves assisting their customers in avoiding a breach all together and attempting to prevent false positives from occurring. A data-centric security model that ensures end-to-end protection across all platforms and encryption of data assets will be critical for customers moving forward. Tools that can predict areas of weakness, find risk, and identify threats to the entire technology ecosystem will allow enterprise networking systems to work smarter against breaches. Large IT Enterprise firms with the greatest upside will incorporate machine learning analytics alongside security protocols to analyze and detect potential threats and immediately notify customers to reduce the cost of cyber breaches.

From a consumer hardware perspective, Apple has marketed itself as Silicon Valley's privacy champion, one that — unlike so many of its advertising-driven competitors — wants to know as little as possible about you. Emphasizing that Apple doesn't assemble user profiles, the company does end-to-end encrypt iMessage and Facetime and tries to keep as much computation as possible that involves your private information on your personal device rather than on an Apple server. But Apple's management have acknowledged the growing reality that collecting user information is crucial to making good software, especially in an age of big data analysis and machine learning and ability to personalize content or understand context especially since Siri (Apple's AI assistant) has come under fire for being weak next to Amazon Alexa or Google Assistant. Hence Apple has acknowledged using differential privacy in upcoming iOS updates. Differential privacy is a research topic in the areas of statistics and data analytics that uses hashing, subsampling, and noise injection to enable crowdsourced learning while keeping the data of individual users completely private. Differential privacy, translated from Apple-speak, is the statistical science of trying to learn as much as possible about a group while learning as little as possible about any individual in it. With differential privacy, Apple can collect and store its users' data in a format that lets it glean useful notions about what people do, say, like, and want. But it can't extract anything about a single, specific one of those people that might represent a privacy violation. And neither, in theory, could hackers or intelligence agencies.

According to IDC, blockchain is starting to move beyond the early innovation phase. While automating transactions is the main use case, IDC suggests the security implications of blockchain are starting to be acknowledged (albeit still too early). IDC maintains that the identity management aspects that are used in blockchain to create "evidence chains" that attest to a person's identity as well as the distributed and collated nature of blockchain technology could potentially grow the use for blockchain technology in the development of security strategies. IDC expects that the rate of adoption will increase linked to the confidence provided by three drivers: clarification of the implications and use cases, growing installed base, and greater availability of larger and more complex reference cases.

European Media

Thomas Singlehurst & Catherine O'Neill
European Media Research Team

We think the proposed changes in privacy and data protection regulations as embodied in the GDPR and the proposed ePrivacy regulation could have significant implications for the broader online ecosystem. The upside from concepts like artificial intelligence, machine learning, and the Internet of Things could all be somewhat undermined if companies are restrained from fully exploiting the potential of big data and data analytics. Looking at the impact on our coverage, however, its effect is somewhat diminished by the fact that the European Media sector has relatively limited exposure to online business models that are reliant on significant amounts of EU consumers' personal data. That is not to say that areas like online advertising aren't taking significant amounts of share, but rather that the companies that are directly benefiting from this growth by and large are not the domestic European media owners but rather (typically) the larger U.S. Internet names. Likewise, within the Professional Publishing space there are a handful of companies that have significant proprietary personal data sets, but to the extent these relate to non-EU citizens, again the risk is relatively de minimus.

Of the names that are potentially most directly impacted, we would highlight the agency groups which have benefited from the rise of digital to a greater extent than domestic media players. We would also note that, perversely, more traditional media channels – in particular areas like newspapers, radio, and outdoor – may benefit if more targeted forms of online advertising are compromised by the change in regulation.

Education companies, or indeed companies collecting large amounts of data on children, are also potentially affected because of a tightening of consent rules which now apply to all minors under the age of 16 (vs. 13 under the previous directives).

Beyond this, however, we would anticipate the impact on the European Media sector to be largely around the additional costs of compliance with the new rules, which may not be immaterial but which also are unlikely to be outsized relative to the broader market.

U.S. Media

Jason Bazinet
U.S. Entertainment, Cable & Satellite Analyst

While changes in the EU's privacy regulations – including the GDPR and ePrivacy – are significant, there are two reasons to suggest the impact on U.S. media firms will be very modest.

- First, U.S. media firms have limited economic exposure to the EU.
- Second, most of the exposure does not depend upon the online ecosystem (but is driven by studio results, traditional TV ads, and TV affiliate fees).

As these businesses migrate to more web-centric services – like online video delivery and targeted ads – the risks could grow. But, today, we view the impact as immaterial. Of the names that are potentially most directly impacted again, as in Europe, we would highlight the agency groups.

Telecoms

Dalibor Vavruska
Global Head of Digital Connectivity Strategy and CEEMEA Telecom Research

During most of their history, telecom operators have played the role of infrastructure providers focused on transmitting information (voice, messaging, images, videos, web-based, or machine communication) between geographical locations. Although flows of such information have changed profoundly during the past 20 years (from person-to-person voice calls towards consumption of centrally-managed high-resolution content and social networking), the role of the telecom industry in the process has changed to a lesser degree. Telecoms are still expected to mainly carry data between different points. Many investors still see telecoms as a proxy for data-transmitting infrastructure, envisaging growth and value creation driven by volumes of transmitted data instead of by the industry's expansion into new data-related services.

Even in the age of the telegraph and fixed-line telephony some electronically transmitted information required confidentiality and privacy protection, due to commercial, personal, or national security sensitivities. Since telecoms used to be electronic communication monopolies, they have naturally been expected to protect the confidentiality and privacy of customer information, such as customer details and data about communications (e.g., date, time, location, and type of communication for individual users) as well as the content of such communications (calls, messages, or Internet traffic). Unsurprisingly, telecoms have therefore often been subject to stricter data privacy regulation compared to other industries. Such requirements appeared entirely sensible in the past.

However, in the upcoming digital age, this logic may change, as telecoms have ceased to be monopolies and dominant infrastructure players, and some of them are moving out of their comfort zone of purely transmitting data towards analyzing and processing data. We see the following as driving this trend:

1. **Lack of growth in telecom legacy businesses:** Telecoms may continue struggling to grow while the Internet services industry still exhibits significant growth opportunities. Given the disruptive nature of new technologies such as fiber-to-the-home (FTTH) and 4G/5G, which provide abundant and in some cases unlimited bandwidth at very low marginal cost, the future growth of the telecom's legacy businesses is not at all certain. The global Internet industry has meanwhile grown larger and more powerful. It is also increasingly active in services such as voice communication and messaging, provided directly to the end users, effectively bypassing the telecom operators. All this is pushing the telecom industry to explore new growth opportunities more strongly than before.

2. **Rising commercial appeal of telecom big data:** The Internet industry has already demonstrated how to successfully monetize customer data. Newly emerging big data analytics tools (e.g., voice recognition, automated voice call transcripts, artificial intelligence tools applied to such communications etc.) promise to extract even more value from such data. While having scale disadvantages compared to the global Internet leaders in terms of customer numbers, telecoms have access to far deeper data about their customers. With new technologies such as Software Defined Networks (SDN) and Internet of Things (IoT), the amount of attractive data owned by the telecoms will only grow. Commercial utilization of such data hence appears increasingly appealing.

3. **Opportunity to secure customer trust due to limited business reliance on sensitive customer data:** As consumers become more privacy-aware, assuming that certain regulatory hurdles are overcome, telecoms could try to position themselves into the role of trusted digital service providers. This is because many Internet business models are based on provision of 'free services' entirely funded by the commercial utilization of customer data. Instead, telecoms often receive relatively stable revenue from their customers, some of which may be willing to pay even more for extended privacy protection.

So what exactly can telecoms do with their customer big data? Below are examples of what may be theoretically possible. Obviously, not all of this is practical or feasible today due to regulatory frameworks in place. We will address some of these issues later. However, we take a view that regulation tends to change over time. To understand and predict changes to the industry landscape, it is important to see the underlying commercial logic in the new industries. In our Citi GPS report Re-birth of telecoms into a new digital industry from November 2016 we showed Verizon, SingTel, and O2 CZ as companies that had highlighted big data as part of their strategy. The report also has a contribution from Christopher Schlaeffer, Chief Digital Officer of Vimpelcom, which recently announced a major digitally-driven strategic transformation in part driven by big data. However the list of digitally and big data-savvy telecoms is certainly far longer. Telecoms can, in our view, use big data in the following ways:

- **Use their own big data to more effectively market legacy telecom services:** (e.g. product bundles, roaming offers etc.). Examples include analyzing customers' calling patterns, family members on the network, their attempts to search for information about competitors' offers, their international travel etc. We think that a number of operators including Megafon in Russia are already using such big data, at least on part of their subscriber base.

- **Use their own big data to offer more differentiated connectivity services:** in terms of speed, quality, capacity coverage, performance guarantees, latency, content blocking/filtering etc. Examples currently include zero rating (free bandwidth offered for specific content, for example to the U.S. or recently announced by Vimpelcom), Internet.org (a constrained version of the Internet for developing countries), or ad blocking. These services are currently seen as somewhat controversial, because of the commonly prevailing net neutrality principles. Hence, they may not yet be as widespread as we expect them to become. We are also not yet aware of any of such services specifically tied to big data analytics. However, given the current industry trends, not only in the U.S., we think that such opportunities may not only become relevant, but potentially commercially significant for telecoms.

- **Use their own big data commercially beyond the connectivity market:** This is mainly about use of such data (e.g., customer location or their on-line habits) in advertising and e-commerce, but in the future also in areas such as the Internet of Things. Examples include Verizon's acquisition of Yahoo, but in a smaller scale also various partnerships between telecom operators and retail companies.

- **Use of their own big data to offer fundamentally new digital services:** Results from big data analytics could be valuable for both consumers as well as businesses. Global Internet companies are already offering a range of services based on big data analytics, particularly in social networks, but also location-based services such as 'find your friend'. The question whether telecoms can find material opportunities in this area remains open. That said, telecoms can certainly provide valuable data to their B2B commercial partners. Meanwhile, as potentially trusted digital providers in the consumer market, telecoms could offer privacy management services to consumers (e.g. Telefónica's initiatives in Germany).

The power of big data comes from the depth of information in it. Combining big data from different parties could therefore materially boost its value. The recent Verizon/Yahoo or Megafon/Mail.ru combinations of telecom and internet companies represent attempts to utilize such synergies. Big data, but also privacy protection, are effectively becoming new valuable commodities, which will be traded in the new digital economy. This market is naturally in its very early stages, but it is possible to see that telecoms should have a role in it.

Telecom big data skeptics would likely raise two points: the current regulatory constraints and the currently prevailing corporate cultures in telecoms, which make it difficult for the industry to innovate, also in big data. Although specific regulations tend to vary region by region, telecoms tend to be constrained by the following:

- Privacy regulations specifically prohibiting them from certain uses of customer data.

- Regulations obliging them to share customer data with certain authorities in a way that does not apply, for example, to the Internet companies, affecting the perception of telecoms as protectors of privacy.

- Net neutrality regulations that constrain their ability to differentiate products.

Most of such concerns naturally have their merits, at least in the short term, but telecom big data optimists may counter with the following:

- Current data privacy regulations, or even those being designed today, are unlikely to fully suit the future markets for big data and privacy protection. This is simply because such markets are still barely emerging and regulations tend to be backward looking. Strong market opportunities in those areas may hence influence future policy shaping anyway.

- Not all today's regulations are unambiguous. Net neutrality is, for example, being enforced to varying degrees in different markets. It is possible to say that 'pure' net neutrality does not even exist, as most operators apply some sort of traffic management. Similarly, on the privacy front, there may be 'grey areas' already in which some operators are able to use certain customer data as long as they do not cross certain lines (e.g., selling such data, sharing such data on individual customers as opposed to aggregated etc.).

- National regulators have genuine reasons to create a 'level playing field' for national big data players vs. the international ones, because of their efforts to build national digital economies as well as for security and strategic reasons. Given the amount of big data already owned by the telecoms and scale economies in the big data industry, telecoms may have a chance to become leading national big data operators.

Let's now look into the prevailing corporate culture at the legacy telecom operators. It has three attributes:

1. **Infrastructure focus:** This is natural since telecom infrastructure, often non-innovative assets such as cables and towers, accounts for a significant part of the telecom value. Interest in preserving the value of this infrastructure naturally becomes the leading interest of managements of telecom companies. Such interests may in some cases be in conflict with innovation.

2. **Ownership and vertical integration focus:** Legacy telecom operators tend to build their competitive advantages around exclusively owning crucial assets, including networks, along the vertically integrated chain. They are generally cautious about strategically re-focusing their business into specific areas while exploring resource sharing, partnerships or outsourcing in a large scale.

3. **Lack of innovation:** As we already said, excessive infrastructure focus could be counter-productive in regard to service innovation. Due to scale economies, infrastructure innovation is done practically entirely by the vendors as opposed to telecom operators. Investors do not expect telecoms to innovate. Hence, they are reluctant to pay a premium for those that do, making it hard for operators' management to justify major innovative moves.

Telecom big data skeptics may see the above points as yet more proof of their case. Big data opportunities are likely to be seen as relatively small compared to the size of vertically integrated telecoms. In an over-regulated and non-innovative environment, the prospect of major achievements by telecoms in this area may appear slim. However, despite all this, some large operators such as Verizon, SingTel and Megafon have been making material investments driven by the big data theme. Why? Part of the answer may come from Verizon CEO's statement saying that in order to survive telecoms have to disrupt their own business model. The industry appears to have a long-lasting growth and value creation problem, which shows no signs of going away. Big data along with IoT are key potential opportunities for the industry. Their attractiveness is further boosted by policymakers' focus on building digital economies and technological trends such as software-defined networks (SDN) in 5G networks.

In order to explore the big data opportunity, telecoms in our view need to successfully negotiate the right regulatory framework, especially in the areas of data privacy and net neutrality. At the same time, the industry will need to become more agile and supportive of potentially disruptive innovation. We think that both can be achieved by re-focusing from infrastructure and vertical integration towards areas where the new opportunities lie, which include big data. Such moves may expose the service part of the telecoms to new risks, However, not exploring such avenues could lead to a major missed opportunity for the industry, possibly leaving the telecom business model in an uncertain state.

U.S. Telecom and Infrastructure

Michael Rollins, CFA
U.S. Telecommunication & Communications Infrastructure Analyst

We view the proposed changes in data privacy and data protection as having a mixed impact on U.S. telecom operators and a potentially positive impact on infrastructure providers, specifically data center operators. At its heart, there will be compliance costs for those companies that have access to data created by EU citizens but this could give rise to increasingly localized storage of that data and increase the storage requirements both in size and locale.

Enterprise telecom service providers based in the US are often global in nature, whether by owning network assets in Europe or having European-based customers in the US. The provision of connectivity is increasingly becoming a commodity, so companies are looking to move from being a 'dumb pipe' to working more in the application and data layer. The need for enhanced data privacy and protection could increase the cost of providing those services, whether needing to gain consent where none was needed or to process and store the data in a specified location.

Telecom services companies are also looking to become increasingly global in their application and data services, such as connected car and hosted application services. Through the use of the cloud, the source of the data and where it is processed and stored has been separated by the use of virtualized systems. Changing how companies architect those systems could increase costs and make the provision of those services less attractive.

For data center companies, we see this as positive to the extent it forces more storage to be done locally and increase the addressable market for colocation or wholesale data center space. While infrastructure companies are less concerned about the specific rules around privacy, they could in turn benefit from the increased regulation on their customers who need incremental space and/or power. To a lesser extent, fiber network providers could find incremental demand to connect new data centers.

European Banks

Ronit Ghose, CFA
Head of European Banks Research

Banks are particularly impacted by the new regulations, given the quantity of sensitive customer data they hold (and share) in order to provide services such as payments, lending, and deposit gathering. They have also been a particular focus for cyber criminals, looking to steal data either to use for their own benefits or ransom firms for its recovery (see U.K. Banks & Cyber Security: The Growing Threat from Cyber Attacks; Risks & Opportunities). In addition, banks are increasingly innovating through new technology, such as big data and artificial intelligence (see Citi GPS: DIGITAL DISRUPTION - REVISITED: What FinTech VC Investments Tells Us About a Changing Industry), with the GDPR framework potentially acting as a hindrance to the data sharing that these new technologies require. The direct impact of the new regulations could be to raise costs, both compliance and fines (up to 4% of global annual turnover under the GDPR), and slow innovation through FinTech. However despite the potentially higher costs, the current tough regulatory environment in which the European banks operate means that they are well positioned to adapt to the proposed changes in privacy and data protection regulations as embodied in the GDPR and the proposed ePrivacy regulation. Within our coverage we would highlight the smaller banks as most impacted, given their relatively smaller compliance budgets.

FinTech startups could be in a tougher position. Many FinTech companies leverage new sources of data (e.g., social media) for credit decision making. These start-ups need to revisit their business models to ensure that customer data is properly stored and disclosed in compliance with the legislation. Start-ups also require access to

data that could be anonymized to protect customer privacy. From this perspective, GDPR restricts business model innovations in the FinTech start-up sector to some extent. Over the longer term, however, customers get better data and privacy protection, which should be supportive of the long-term prospects of FinTech business models.

Insurance

Andrius Budnikas & James Oram
European Insurance Research

Customer data is a key component of several vital operating functions for all personal lines insurance companies – pricing, reserving, and risk management – in addition to other generic processes such as distribution and marketing. As a result, insurers have built up large volumes of customer data over time in order to create, price and sell their products. Consequently, any changes in regulation relating to the use of such data could have a material impact on the insurance industry.

Based on communications with the companies under our coverage, it seems that compliance with the regulations is still a work in progress but significant steps have already been taken — additional data and compliance staff have been hired, dedicated project teams have been created and detailed risk assessments have been carried out. However, there are still several areas of outstanding uncertainty, on which the industry is currently seeking further clarification. These include: (1) Insurers believe that a common industry standard will need to be agreed because the transferal of data from one user to another is arguably more pertinent for insurers than other sectors due to the regularity with which customers switch providers. This may take time to agree and implement and needs clear direction from regulators and trade associations; (2) Legislation changes will be required to allow the industry to continue to process certain data points that are integral to their product offering. Commitments have been received from government bodies that this will be in place but it is by no means guaranteed at this stage; and (3) Certain fundamental elements of the new regulations are still subject to final clarification: a more precise definition on profiling; what is considered necessary for the performance of an insurance contract; and what constitutes effective consent.

Aside from the time and cost associated in preparing for the new regulations, there may be other, more nuanced effects that will vary from company to company depending on several factors, including business mix and existing data capability. For example, those (re)insurers that focus on predominantly commercial risks (i.e., their clients are companies or other insurers) are less reliant on personal data in their day-to-day business, albeit they will still need to be compliant. In contrast, personal lines insurers will face a far greater burden from the new regulations. Not only is customer data a key part of their existing business models, a number of these companies are increasingly focusing on their cross-selling capability (i.e., selling home insurance to existing car insurance customers, or even exploring non-insurance opportunities) as a means of growing premium volumes and improving margin. This is heavily driven by the inter-availability of data between different underwriting functions and we believe that this could become incrementally more difficult if there are restrictions on the use and transfer of such data.

In terms of opportunities, we believe that an increasing focus on data management and protection could boost demand for ‘cyber’ insurance which indemnifies companies/ institutions against data breaches, hacking etc. Demand for this product has historically been in the U.S. but changes to European regulation could make it far more common among European corporates. This could create a strong growth opportunity for several (re)insurers that specialize in these lines of business.

Business Services

Ed Steele & Marc van't Sant
European Business Services Research

Within the Business Services sector the most reliant on data are the information services businesses, companies like Experian. These companies handle significant data sets, including data on individuals, to help organizations understand consumer behavior, predict consumer trends, manage credit risk and protect from fraud.

The implementation of the GDPR brings with it four specific issues for the information services businesses to contend with:

- **Managing Consents:** The GDPR requires that data subjects give '*specific, informed and unambiguous*' consent for the data processor or controller to use personal data in a specific way and that this is required for any collection and processing of sensitive data. For companies that sell access to large data sets of personal data – for example credit bureau – gaining consent may be problematic. One potential mitigation factor may be 'legitimate interest'. As we note in the section in the GDPR, however, even the wording around 'legitimate interest' has changed to include a 'reasonable expectation' condition which may make the use of the legitimate interest basis, overall, more difficult to justify.

- **Understanding EU Consumers' New Rights:** The GDPR strengthens consumers' rights in a number of different areas. Consumers now have an absolute right to object to data processing for direct marketing purposes, a right to get an exception from 'automated decision making', the right to access data, the right to data portability and the right to erasure. All of these potentially create challenges for companies that store and use large amounts of personal data, but it is perhaps the latter that is most challenging.

- **Breach Notifications/Demonstration of Compliance:** The GDPR now requires data controllers to notify authorities of a breach within 72 hours of becoming aware of them, something which will represent a significant logistical challenge for companies with significant amounts of data and an extended network of controller/processor relationships. The requirements to demonstrate compliance (necessary security protocols, evidence of privacy by design/default and legal basis of all processing) will also likely entail material resources.

- **Sanctions:** As with all sectors, the significantly enhanced sanctions are an acute risk. All information services businesses have to a degree faced reputational challenges associated with data breaches, but for typically non-consumer facing entities these have been minimal. Hitherto the financial penalties associated with poor data protection have been insignificant. The increased fines (up to 4% of global annual turnover) raises the risk profile associated with data protection significantly.

All of these issues are significant administrative – and in some cases existential – challenges for the information services businesses in Europe. There is, however, one important silver lining. To the extent that information services/data broking companies can maintain compliance, larger companies will have a significant advantage in terms of resources and market position. In the short-term, therefore, this may well mean more investment in systems and processes, but longer-term, once compliance is achieved, the implementation of the GDPR may actually reinforce the larger players' market positions.

European General Retail

Dan Homan
European General Retail & E-commerce

In our opinion, the changes in privacy and data protection regulations as embodied in the GDPR and the proposed ePrivacy regulation are unlikely to result in a fundamental impact for the European General Retail industry. The nature of retail customer behavior means that a high proportion of interaction involves one-off payments, with very few long-term contracts. In combination with the potential for damage to brand equity from a bad press this means that data protection is already embedded into corporate policy.

We think consumers will want to keep the functionality that current retail websites provide, such as shopping baskets and shopping suggestions and therefore will continue to consent for data to be used. Even so, the right to be forgotten may be used further as a means to eliminate spam marketing.

The impact on retailers is likely to be limited because data usage and analytics are an offshoot of the underlying operations rather than a central part of the business model. If there was an impact, we would expect it to be largest in these two areas:

- **Compliance burden:** Retailers are going to need to allocate additional resources to make sure that systems are compliant with the new, expanded regulation. This will include defining what constitutes personal data as well as understanding how data is processed and utilized through own channels and third parties.
- **Customer acquisition:** Almost every retailer is now utilizing online advertising to recruit customers and the innovation and sophistication in this area has driven ever more targeted and cost-efficient customer recruitment. If regulations curtail the ability to target consumers then retailers may find the return on online marketing investment is reduced.

Those retailers with larger online presence and more sophisticated marketing and data analytics are likely to be more impacted by these changes in regulations while the additional compliance burden will have a larger impact on small retailers which have less ability to absorb the additional cost burden.

U.K. SMID

Michael Goltsman, CFA
U.K. SMID Research

As with most other sectors, in advance of the proposed changes to the privacy and data protection regulations, U.K. SMID companies will need to re-assess how they capture, store and process customer data. For most of the companies under our coverage, the proposed regulatory changes will require additional time and cost investment in order to ensure compliance. However, there are also a number of beneficiaries within our U.K. SMID coverage. Notably the cybersecurity names will benefit as the growing need to secure personal data will support demand for their products and services.

Airlines

Andrew Light
European Airlines

European airlines possess a significant amount of customer personal data, particularly low cost carriers (LCCs), for whom about 95% of bookings are directly between the end-traveler and the airline. Legacy full service carriers (FSCs), such as the three largest flag carrier airline groups, possess less personal data because 70% of their bookings come via travel intermediaries, such as global distribution systems (GDSs), travel management companies (TMCs) and online travel agencies (OTAs). These FSCs are striving to bypass these intermediaries, not only to reduce distribution costs but also to obtain access to more customer personal data (e.g., email addresses and credit card details) in order to be able to up-sell or cross-sell

ancillary services to them. The FSCs have also developed large and sophisticated frequent flyer programs (or customer loyalty programs) in order to improve their knowledge of customers (e.g., corporate business travelers who invariably book via intermediaries), engender their loyalty, make targeted offers to them and generally use customer data analytics to inform strategic decisions, such as planning new routes.

In addition to basic personal data, such as email and physical addresses, airlines may possess other critical personal data, such as trip histories, previous ancillary purchasing behavior, passport details, credit card details, personal preferences as well as upcoming trips, and even a customer's physical location when on a trip on that airline. In possession of critical personal data, such as passport details and credit card details, airlines generally have very secure data storage already and are well aware of data protection and ePrivacy issues at EU and global levels.

Airlines try to capture as much personal data as possible when a customer first makes a booking, so that future bookings can be made more easily and spontaneously. Most airlines ask customers to opt-in to receive future offers and then use big data, client relationship management (CRM) and data science tools to tailor these offers in order to offer the right product to the right person at the right time. Offers include both the airline's own products, including up-selling to higher classes, as well as ancillary offers (e.g., car rental, hotels). Customer data is generally not shared with the providers of these ancillary services. Airlines make these offers at the time of booking as well as at various times prior to departure, including just prior to boarding the aircraft. They also use their mobile apps to inform passengers of reminders of and any changes to their flights. Some airlines would like to stay in touch with customers throughout their trip and sell other destination services while they are away from home but this may be constrained by the proposed ePrivacy Regulation because we think airlines only have a legitimate right to know and leverage the physical location of customers when they are at the airport.

The airlines we cover already ask customers to opt-in to receive personalized offers. We are therefore not unduly concerned that the EU's GDPR and ePrivacy Regulation proposals will have a significant revenue impact on their ability to make personalized offers, although there might be a small impact from less online advertising if users do not change the default setting on their web browsers to block advertising cookies. Indeed, the elimination of spam emails that the new proposals seek to achieve could mean that airlines' personalized messages and offers might actually get noticed by recipients rather than being drowned out. The more important issue for airlines, in our opinion, is the heavy burden placed on companies to ensure organizational readiness and compliance to the new rules by May 2018, given the hefty penalty of non-compliance (e.g. fines of up to 4% of global annual turnover in an industry that makes an average operating margin of 5-7%) and the need to report data breaches within 72 hours of occurrence.

Key Issues for Corporates & Investors

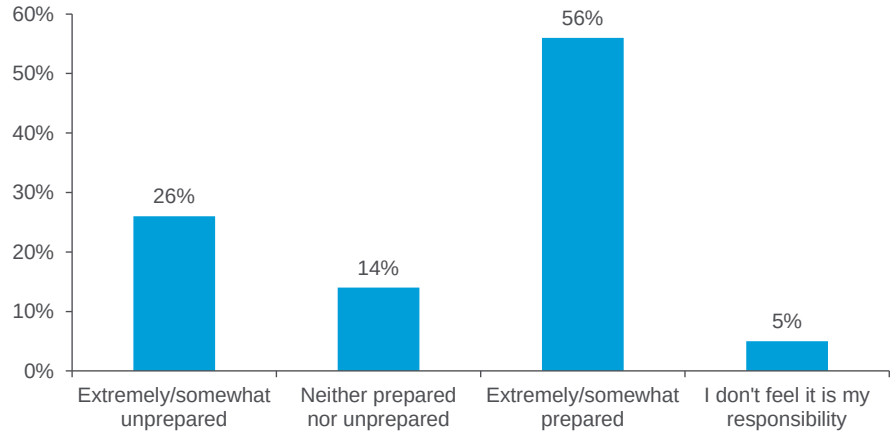
So, to recap on the five main conclusions:

- Although the opportunities from data are significant**, a lot of commentators have underplayed and potentially underestimated the challenges associated with ensuring ePrivacy** and adequately protecting personal data.
- **The implementation of the GDPR in May 2018 represents one of the most significant events in ePrivacy/data protection regulatory history.** The regulation is a game changer in terms of not only its scope and ambition, but also the significant penalties for non-compliance.
- **The aim of the evolving data protection regulation in Europe is to shift power back to consumers, and ultimately increase transparency and trust in how companies use consumer data.** Best case, consumers become more trusting if they are better educated on how data is used. The outcome being that data quality improves, and data as an asset increases in value. However, there is a risk that in attempting to achieve its aim, Europe's approach is too heavy handed, resulting in a vast reduction in data being shared with companies, particularly in relation to third-party tracking. Adtech and online advertising funded media rely on the ability to track consumers using third-party trackers.
- **The very companies that the GDPR was potentially designed to constrain will probably end up being least affected.** Of course there will be increased regulatory costs associated with compliance, but those larger companies that already have consumer trust and the necessary resources to remain compliant with much stricter and more complex EU rules, will likely be less disrupted than smaller enterprises. For all companies, it will likely require a cultural change in relation to how personal data is collected, stored and used.
- **The asymmetric approach toward regulation between different regions** (contrast the dirigiste approach of the EU vs. the more laissez-faire, principles-based approach of both the U.S. and Asia Pacific) **could lead to a similar level of asymmetry in terms of access to investment and 21st century consumer services** – artificial intelligence, machine learning, and the Internet of Things. In other words a world of digital-haves and digital-have-nots where, ironically, 20th century notions of borders and citizenship are the primary factors determining where people sit.

It is in the interests of companies to provide comprehensive data privacy assurances. The World Economic Forum estimates that capturing share of data privacy-conscious consumers (net of implementation costs and revenue forgone from non-monetization of third-party consumer data) should put about $330 billion at stake in 2015-25. The number of consumers moving to companies with strong data privacy measures is estimated to grow from 5% in 2015 to 25% in 2025.

It is worrying that with little over a year to go, GDPR readiness is not higher. A DMA survey in the U.K. found 26% believe their company is extremely/somewhat unprepared for the GDPR, and 14% are neither prepared nor unprepared.

Figure 76. How Prepared is Your Company for These (GDPR) Changes?



Source: DMA: 'DMA Insight: GDPR and you 2016 chapter 2' Survey conducted Sept-Dec 2016

With that in mind, we have prepared a list of 15 questions we think companies should be asked in relation ePrivacy and data protection:

1. Are you aware of the EU General Data Protection Regulation (GDPR) and the proposals associated with the first draft of the proposed ePrivacy Regulation?

2. If so, are you aware of the requirements of the new regulations and of the sanctions in the event of non-compliance?

3. What kind of framework, security, and training do you have in place in relation to data protection? Do you have an official privacy/data protection team in place? If so, does your Chief Privacy Officer report to the board/senior management? What is his/her name?

4. How reliant is your business on the use of personal data? How central would you say use of data/data analytics is to your business model?

5. How do you monitor what data you hold? What consumer data do you currently hold and in what format (physical/electronic)? Do you know where the personal data you hold is stored (especially if it is in the cloud) and who has access to it?

6. Do you have an accurate picture of what consents you have for your existing data resources? How will you go about obtaining necessary consents post implementation of the GDPR? To what extent are you currently able to inform customers of what data you hold and erase it on request? How do you think about the balance between utilizing data while maintaining consumer trust longer term?

7. Does your company sell or share data with third parties in any way? Do you process all consumer data yourself or do you hand off data to third-party processors?

8. If the latter, to what extent are you comfortable that contracts with outsourcing partners (including providers of cloud services) have sufficient provisions for ePrivacy and data protection and what resources are you putting in place to make sure commitments are met?

9. To what extent is data circulated within your institution, i.e., between business lines in the same geography and/or between different geographic regions?

10. To what extent are there competing regulations (e.g., anti-money laundering screening for financial institutions) that potentially come into conflict with new ePrivacy/data protection regulations?

11. With all of this in mind, what are you doing to ensure that you are going to be compliant with the GDPR by May 2018? Are there any areas where you see implementation challenges?

12. The regulator appears to be pushing for a cultural change in the approach to data protection – how do you go about instituting that cultural change? Does there need to be a change in incentive structures within the organization?

13. Financially, how do you think about the costs associated with data protection and privacy – do you expect a material change? Are there any financial benefits from the requirements of the GDPR?

14. Does the idea of more stringent rules on data protection and ePrivacy (and significant fines for non-compliance) make you think differently about the importance of data protection to your organization? Will any of your operations (that handle data) have to fundamentally change how they operate in order to comply with the upcoming regulation, or be materially impacted by the regulation?

15. Is there anything you use data for currently that you will have to stop doing? Any areas of business/product/service development that appear unworkable in light of the regulation? Does the GDPR make you reconsider what services/products you offer within the EU (relative to other regions/geographies)?

Glossary

Adequacy – A standard used by the European commission to assess countries outside the EEA and whether personal data can more freely between an EEA economy and the other, third, economy. If protections in the third economy are deemed 'adequate,' then data can be transferred freely. A successful adequacy decision depends on the European commission believing that the third economy has sufficient data protection. Adequacy means no additional approvals are needed for data to be transferred to it from the EEA.

Anonymization - This is where personal data is *irreversibly* changed such that specific individuals cannot possibly be identified from the data at any time in the future. This differs from pseudonymization (see below) in that here it must not be possible for individuals to be recognisable ever.

Application Programming Interface (API) – This is a set of basic mechanisms that allow different components in a computer to communicate with one another.

Article 29 Working Party – A technical, advisory, body within the European commission comprised of representatives from all European national data regulators. They issue advisory opinions on a range of issues.

Artificial Intelligence (AI) – A machine mimicking 'cognitive' functions or human actions such as learning or problem solving.

Asia-Pacific Economic Cooperation (APEC) – This is a forum for 21 Pacific Rim member economies that promotes free trade throughout the region.

Automated Decision Making – This is where decisions about individuals are made through entirely automated means. This means the decision is *entirely* automatic, without any human revision or input. If a worker's remuneration, for example, is liked to automatically measured productivity, this is automated decision making.

Binding Corporate Rules (BCR) - Internal rules (such as a Code of Conduct) adopted by multinational group of companies which define a global policy with regard to the transfers of personal data within the same corporate group, including to entities located in countries which do not provide an adequate level of protection.[35] This allows free transfers of data within a corporate group even when not to countries with adequate domestic protections. These are processed and approved by national data regulators, such as the ICO in the U.K. (see below).

Cross-Border Privacy Rules (CBPR) - The APEC Cross-Border Privacy Rules system is a voluntary scheme to encourage personal data flows among APEC economies. Organizations that control data can voluntarily apply to join the scheme. This then requires companies meet certain data protection standards. To be eligible, companies must be subject to the laws of a participating economy. Currently, only companies in the U.S., Mexico, Japan, and Canada participate.

Cross-Border Privacy Enforcement Arrangement (CPEA) – This is a framework for regional cooperation in the enforcement of Privacy Laws. Participation is voluntary. The CPEA aims to facilitate information sharing, provide mechanisms to promote effective cross border enforcement cooperation, and encourage the sharing of best practice.

[35] European Commission

Cookie – A small package of data sent from a website and stored on the user's computer by the user's web browser. Cookies generally fall into two forms. There are session cookies that record 'stateful' information, used to ensure good website functionality — for example, remembering the content of an online shopping cart. Such data is deleted once the browser is closed. Secondly, there are tracking cookies that store and communicate data on wider online activity.

Cookie-syncing – Different trackers exchanging user data across different platforms, which involves the mapping and matching of user IDs from different platforms, to better target audiences with online advertising.

Consent – a basis on which personal data can be stored and processed under most data protection regimes. This varies from regime to regime. Under the GDPR, consent has to be freely given, specific, informed, and unambiguous to be legitimate under the GDPR. In addition, under the GDPR, consent must be verifiable and individuals must be able to withdraw it at any time.

Cloud Computing – Storing, managing and processing data through a network of remote servers, often not owned or managed by the user in question, rather than a local network or computer.

The Competition Markets Authority (CMA) – This is a public U.K. regulator that aims to ensure sufficient levels of market competition, as well as detecting and preventing uncompetitive practices.

Cross-Device Tracking – These are techniques used to detect single Internet users when they use a myriad of different devices. They will be used to ensure that data on someone's phone Internet browsing history is matched to that on their computer, for example.

Cyber Security – This denotes systems and activities that protect computer systems from the theft or damage to hardware, software, or information. Additionally, this includes activities relating to the protection of networks from disruption, and disruption to the services they are used to provide.

Data Brokers – Organizations that fuse data from a range of difference sources, processing it to develop more insightful data. This data is usually then passed on and sold to other organizations.

Data Controller – This is a person or organization that has at least some say in what personal data is collected, and how it is processed and used.

Data Minimization – The principle that an organization should not collect or hold more data than is necessary to fulfil the purpose the data was initially collected for.

Data Processor – These organizations process data on request from another individual with control of the data. In the context of personal data, they execute the wishes of data controllers (see above). Processors have no say over what the data is used for, nor how it's processed overall.

Data Protection Officer (DPO) – A new position specified by the GDPR and required of companies undertaking innovative or high volume, processing of personal data. This individual is responsible for ensuring compliance with regulation, and acting as a permanent point of contact with data protection authorities. The data protection officer is required to report to the highest management strata of a company.

Data Protection Authority – This is a national regulator responsible for the protection of personal data. In the U.K., for example, this is the Information Commissioner's office. This is required by EU legislation.

Data Portability – This is a new right afforded to customers under the GDPR that allows customers to obtain and re-use their data across different services and platforms. This requires data companies develop common standards in consumer data storage so that records can be easily transferred and utilized across different data controllers.

Data Subject – A living individual to whom personal data pertains.

Data Transfers – Copying data from one computer to another. In the context of the GDPR, data transfers largely refer to the transferring of personal data outside of the European Economic Area.

Derogation – The relaxation of a law in a specific context. This is in contrast to an abrogation that amends a law by imposing new, contradictory, measures later. Instead, here, exceptions are built into the law itself.

Digital Advertising Alliance (DAA) – An independent, non-profit body that develops common practice and standards for digital advertising. It has developed a set of principles that apply to data gathering and use in advertising.

Digital Single Market Strategy – European Commission strategy that aims to ensure uniformity in digital industry standards. The ultimate aim is to create a better integrated market in digital industries across Europe.

Directive – EU legislative instrument in which common goals are agreed at the European level and then realized by member states through national legislation. Directives afford states a degree of flexibility as they can choose how best to realize the common aim in the context of existing national legislation. European Regulations, by contrast, apply directly to all those in member states. They provide more uniformity, but are much less flexible and more disruptive as a result.

Direct Marketing – This is the selling of products or services directly to the public, e.g., over the Internet.

Domain Name system (DNS) – This is a decentralized naming system for computers, services or any resource connected to the Internet. The predominant application of such a system is to convert domain names into IP addresses.

Do Not Track (DNT) – This is a system whereby individuals on the internet can use their browser settings to block tacking by websites. Attempts have been made by the World Wide Web Consortium (W3C - see below) to develop a standardized system across browsers and websites.

DoT- U.S. Department of Transportation

ePrivacy Directive – A European directive first passed in 2002 and subsequently amended in both2009 and 2016. Its aim is to ensure privacy in online communications. It deals with regulation in a range of areas including the confidentiality of data traffic and the use of spam. Crucially, since 2009, it has regulated the use of cookies.

The European Economic Area (EEA) – This is a common economic free trade zone among European Union members and several other countries located on the

European continent. It has common regulatory standards, and ensures free movement of persons, goods, services and capital among member countries. This is not to be confused with the European Union itself (see below).

The European Union (EU) – This is a political and economic union of twenty eight member states. It has seven component institutions, of which five are particularly notable. The European Council has a key agenda setting role, and is comprised on the heads of state or head of the government of each member nation. The Council of Ministers and the European Parliament are the organisation's legislative bodies. The European Commission is the 'government' of the European Union, holding key executive power. Lastly the Court of Justice of the European Union ensures the common application and interpretation of European Law.

The Court of Justice of the European Union (CJEU) - This is responsible for ensuring European law is applied accurately and uniformly. It has two courts, the European Course of Justice (ECJ) and the General Court, that hear legal applications from national courts and individuals respectively. It holds ultimate interpretive power in European Law.

European Data Protection Directive 1995 (DPD) – This regulated the processing of personal data in the European Union before the passage of the GDPR. As a Directive (See above), this only set out aims that were subsequently realised through national legislation.

European Data Protection Board (EDPB) – This is a new body that is being established within the European Union that will replace the Article 29 Working Party. It will still be comprised of representatives from National Data Protection Authorities (see above), as well as a non-voting representative from the European Commission. This body will now also have a secretariat.

Fingerprint-based tracking – This is a form of data tracking that identifies a specific device by corroborating a range of different settings and characteristics that, when combined, are specific to that device. The variables could be as wide ranging as screen colour and text rendering, as well as colour profiles. Once the device is identified, browser, and behavior data is then stored and used to develop a profile.

First Party Data – This is data that has been collected by the firm in question from customers. The implication is that such data is often collected with a greater degree of awareness on the part of the consumer.

Foreign Intelligence Surveillance Court (FISA Court) – A U.S. federal court established under the Foreign Intelligence Surveillance Act of 1978 to oversee requests for surveillance warrants against foreign spies inside the U.S. by federal law enforcement and intelligence agencies. Requests usually made by the National Security Agency or Federal Bureau of Investigation (FBI).

Federal Communications Commission (FCC) – This is an independent agency of the United States government to regulate electronic communications.

Federal Trade Commission (FTC) – This is an independent agency of the United States that is primarily focused on consumer protection and preventing anti-competitive practices.

The Government Communications Head Quarters (GCHQ) – This is a British Intelligence and Security organization responsible for collecting intelligence from networks and ensuring the integrity of key U.K. data centers and information networks.

The General Data Protection Regulation (GDPR) – A new European regulation intended to strengthen and homogenise personal data protection regulation. Unlike past European Data Protection, it will regulate any organisation processing the personal data of a European national. Additionally, it will also impose much steeper fines if rules are broken.

Global Positioning System (GPS) – This is a satellite-based navigation system made up of a network of 24 satellites. It can be used to locate devices.

The Global Privacy Enforcement Network (GPEN) – This is an organisation founded by the OECD that facilitates coordination between Privacy Enforcement Authorities. It was founded alongside the adoption, in 2007, of a new set of OECD data protection principles.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González- This was a crucial case in the history of European Data Protection. Here, the Court of Justice of the European Union (CJEU, see above), ruled that individuals had a 'right to be forgotten' (see below). This ruling was based, predominantly, on individuals having control over their own data, and subsequent ability to largely determine what data about them was publically available.

The Hypertext Transfer Protocol (HTTP) – This is the foundation of data communication on the internet. It works on the basis of a series of fundamental hyperlinks. In this system, a 'client' (a user browsing the web) submits a HTTP request to a server that then returns the website the client initially requested.

HyperText Markup Language (HTML) - The predominant mark-up language for creating web pages and web applications.

HTML5 – This is the latest evolution in HTML (see above). This newer version has a wider range of technologies that allow the construction of more varied and powerful websites and applications.

The Information Commissioner's Office (ICO) – This is an independent U.K. body set up to uphold information rights. This includes handling and following up complaints on data protection (among other things), as well as sanctioning firms that fail to meet data protection standards.

Internet of Things (IoT) – Everyday objects containing networked computing devices that are able to send and receive data.

Internet Protocol (IP) Address – This is a numerical value assigned to each device on a network. They service two principle functions. The first is to identify the given device on the network; the second is to locate it. On this basis they facilitate basic online communication.

Jan Philip Albrecht – A Franco-German Politician and Green Member of the European Parliament. His main political focus is on issues relating to mass surveillance, privacy and data protection.

Legitimate Interest – This is a basis for processing under the General Data Protection Regulation. It allows processing without consent when it is deemed to be in the 'legitimate interests' of the data controller. Examples of this include cases where processing prevents a controller being the victim of theft, for example. The GDPR has tightened the conditions around the legitimate interests basis for processing. This will now be much harder to use as a basis for processing data on children. Additionally, the expectations of data subjects have now become a relevant consideration.

Machine Learning – Machine use of data to develop algorithms that can make predictions based on historical relationships and trends.

Machine-to-Machine Communication– This refers to direct communication between devices through a network. This allows machinery to collect and process information, as well as making automated decisions on the basis of information collected. This is an integral element of the internet of things (See above).

Max Schrems - Austrian lawyer, author and privacy activist. He is most well-known for his campaigns against Facebook for its alleged transfer of personal data to the U.S. National Security Agency (NSA) as part of the NSA's PRISM program. His activism played a key role in the European Courts ruling that past arrangements for data transfers with the United States did not provide adequate levels of data protection.

Metadata – Metadata is 'data that provides information about other data.' This is the equivalent of an index in a book, providing information on the character and content of other data points. There are three types of such data. Descriptive metadata is used to identify and find key pieces of data- such as an index. Structural meta-data indicates how objects are put together and administrative metadata provides information that helps manage resources.

Model Contract Clauses– These are off the shelf contract clauses developed by the European Commission that can be attached to existing contracts to secure sufficient levels of data protection for transfers outside of the EEA. There are currently two types, one set of clauses for transfers between data controllers and another for transfers between controllers and processors.

The National Security Agency (NSA) - This is an intelligence organization of the United States government. It is responsible for global monitoring, collection, and processing of information and data for foreign intelligence purposes.

Network and Information Security Directive (2016) - A European Directive which sets out network and information system security standards within the European Union. It establishes new security and notification requirements for Operators of Essential Services (such as banking, financial market infrastructure, utilities and digital infrastructure) and Digital Service Providers (such as search engines and cloud services).

The Organisation for Economic Cooperation and Development (OECD) –This is a 35 member, intergovernmental economic organisation that aims to stimulate economic development and world trade. Its membership includes some of the world's largest, and the world's most developed economies.

Over the Top (OTT) – This is the delivery of content, such as audio, video and other media, over the internet without the involvement of a traditional broadcaster.

Personal Data or Personally Identifiable Information (PII) – Under the GDPR PII is information that can be used to identify, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal data includes name, phone number, email address.

Pixel Tags – These are a form of Web Beacon (see below) that are implemented through an embedded image.

Programmatic Media Buying – This is an automated method for buying digital advertising where the characteristics of buyers are detected and then automated methods are used to match the advertising space with a specific advertiser in real time via a bidding mechanism.

Privacy by Default – The privacy settings for a new product or service are set at an appropriate level to minimise risk associated with processing and storing personal data.

Privacy by Design – This is an approach to systems engineering which takes privacy into account from the design to execution phase. This complements Privacy by Default that says that where an aim can be achieved using a less risky execution approach, then this approach should be taken. Privacy by design says that, where a strategic aim can be achieved through a more effectively designed approach, from a privacy point of view, then the more effective design must be adopted.

Privacy Impact Assessment (PIA) – A tool or process that organisations can use to identify and minimise privacy risks in the collection, use and disclosure of personal information.

Privacy policy – Published policy available to consumers that explains how personal data is collected, stored and will be used by a company.

Privacy Recognition for Processors (PRP) – This is a voluntary certification under the APEC Privacy Rules system that allows data processors to demonstrate their ability to adhere to personal data protection standards. This is important as processors are not directly regulated by the APEC structure, but rather controllers are responsible for ensuring they only use processors who will adhere to data protection standards.

Privacy Shield – This is the new voluntary regime replacing 'Safe Harbor' (see below). American companies can volunteer to participate, with membership allowing companies to transfer data freely from their European to American operations. This has a more robust program of enforcement under U.S. Law. This was recognised as 'adequate' by the European Commission (see above) in July 2016

Pseudonymisation – A process by which commonly recognisable identifiers, such as names and addresses, are replaced with artificial pseudonyms, such as ID numbers. Here, in contrast to anonymization (see above), the data could, hypothetically, be manipulated to identify individuals, but for most this is impossible. This process can, however, be reversed.

Recitals – in European legislation, recitals set out the reasoning for, and provide clarification on, certain elements of a piece of legislation.

Regulatory Fitness and Performance programme (REFIT) – This European Commission initiative that assess the regulatory fitness of current EU rules and examines whether they have contributed to the achievement of their main objectives. This initiative also aims to identify possible redundancies (i.e. in case the same obligations are covered by another EU legal instrument), inconsistencies and opportunities for simplification.

Right to Access – This is a right afforded to individuals under the GDPR to know whether their data is being processed and access it if they choose to do so.

Right to be Forgotten – This is a right afforded to individuals under the GDPR to request the deletion of any personal data relating to them. In particular, this has come to apply to publically available data, with some limited exceptions. This right was first highlighted in the Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González case (see above).

Schrems vs Data Protection Commissioner (2015) - In this case, now commonly known as 'Schrems I', Max Shrems (see above) challenged the transfer of his data to the United States by Facebook following the publication of the Snowden revelations. Following his complaint to the Irish Data Protection Commissioner, the complaint ultimately led the Court of Justice of the European Union to invalidate the Safe Harbour agreement (see below) that allowed free transfers of data between the EEA and the United States. Mr Schrems has now brought a second case, colloquially known as 'Schrems 2, 'regarding the use of 'model contract clauses,' (see above).

Safe Harbor – This was an agreement between the European Union and the United States that allowed the free transfer of data out of the EEA to the United States. This was a voluntary regime that American companies enrolled in; this required these companies met certain additional standards of data protection.

Software Defined Networks (SDN) - An umbrella term describing a range of approaches that seek to improve the functionality of networks by making them more integrated, flexible, and agile. A key aim of such technology is to develop a network that can be managed centrally using software, in the same way single data centres are managed. This would allow the more efficient direction of traffic.

Structured Query Language (SQL) - This is a special purpose language used in programming for data management in either a relational database or data stream system.

Targeted Advertising – This is a form of advertising that focuses on the traits of consumers in order to focus advertising messages towards those that the advertiser believes are most likely to be receptive to the advertisement.

Third-party data – This, in contrast to first-party data, is data that has not been directly acquired from customers by the data controller. It may be a data that a data processor has been permitted to collect, or data that is bought by an organisation from a third-party data supplier. This typically makes it harder for consumers to effectively monitor who has their data and how it is being used.

Web Beacons – An unobservable graphic image that is placed on a website or email, often used in conjunction with cookies (see above). Among other things, they read and place cookies, monitoring the behavior of users

World Wide Web Consortium (W3C) - This is an international group working to develop common web standards that can ensure the continued growth of the internet. The group's main activity is to develop protocols and good online practice.

World Privacy Forum – This is a U.S.-based, non-profit, research group that works to educate and explore issues surrounding data privacy. Special focus is given by this group to privacy issues surrounding the use of digital technologies.

Citi Global Perspectives & Solutions (Citi GPS) is designed to help our clients navigate the global economy's most demanding challenges, identify future themes and trends, and help our clients profit in a fast-changing and interconnected world. Citi GPS accesses the best elements of our global conversation and harvests the thought leadership of a wide range of senior professionals across the firm.

All Citi GPS reports are available on our website www.citi.com/citigps

Digital Disruption - Revisited
What FinTech VC Investments Tells Us About a Changing Industry
January 2017

2017 Investment Themes
A Wind of Change
January 2017

2017 Corporate Finance Priorities
January 2017

Car of the Future v3.0
Mobility 2030
November 2016

Infrastructure for Growth
The dawn of a new multi-trillion dollar asset class
October 2016

Virtual & Augmented Reality
Are you sure it isn't real?
October 2016

Re-Birth of Telecoms into a New Digital Industry
Time to Dump the Dumb Pipe
October 2016

Disruptive Innovations IV
Ten More Things to Stop and Think About
July 2016

Digital Disruption
How FinTech is Forcing Banking to a Tipping Point
March 2016

The Coming Pensions Crisis
Recommendations for Keeping the Global Pensions System Afloat
March 2016

Technology at Work v2.0
The Future is Not What It Used To be
January 2016

Global Political Risk
The New Convergence between Geopolitical and Vox Populi Risks
January 2016

Investment Themes in 2016
New Normal or No Normal
January 2016

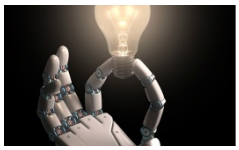
2016 Corporate Finance Priorities
January 2016

Energy 2030
Financing A Greener Future
November 2015

The Global Art Market
Perspectives on Current Drivers & Future trends
November 2015

The Curtain Falls
How Silicon Valley is Challenging Hollywood
October 2015

Energy Darwinism II
Why a Low Carbon Future Doesn't Have to Cost the Earth
August 2015



Disruptive Innovations III
Ten More Things to Stop and Think About
July 2015

Car of the Future v2.0
Mobility Transformation: Full Steam Ahead
May 2015

Beyond China
The Future of the Global Natural Resources Economy
March 2015

Technology at Work
The Future of Innovation and Employment
February 2015

Investment Highlights in 2015
Dealing with Divergence
January 2015

Corporate Finance Priorities 2015
Driving Corporate Growth in Divergent Markets
January 2015

The Re-Birth of Telecom Monopoly
Is the Industry Broken & Heading Back to its Monopolistic Roots
November 2014

Energy 2020: Out of America
The Rapid Rise of the US as a Global Energy Superpower
November 2014

Asset Allocation for a New Era
Diversification, Not Rotation, is the New Watchword
October 2014

Future Opportunities, Future Shocks
Key Trends Shaping the Global Economy and Society
October 2014

Taking It To The Streets
The New Vox Populi Risk
May 2014

The Car of the Future
Transforming Mobility As We Know It
May 2014

Disruptive Innovations II
Ten More Things to Stop and Think About
May 2014

Upwardly Mobile III
Mobility Unchained: From Mobile Commerce to IoT
January 2014

2014 Year Ahead
Investment Themes
January 2014

Abenomics
Four Arrows to Target Four Challenges
October 2013

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets Inc. and is distributed by or through its locally authorised affiliates (collectively, the "Firm") [E6GYB6412478]. This communication is not intended to constitute "research" as that term is defined by applicable regulations. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are his/ her personal views and do not necessarily reflect the views of his/ her employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice.

You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests.

This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication.

The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted.

The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy.

The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks.

Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources.

This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom.

Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

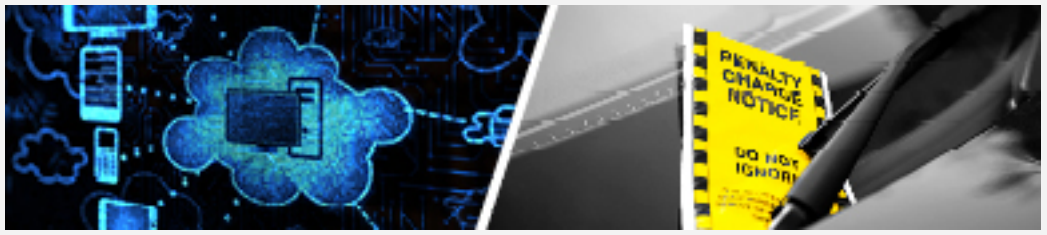
IRS Circular 230 Disclosure: Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside of Citi. Any statements in this Communication to tax matters were not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

NOW / NEXT

Key Insights regarding the future of ePrivacy & Data Protection

REGULATION

The opportunity from data is clear but in the rush to exploit the data opportunity, not all companies have paid enough attention to or fully factored in the necessary safeguards for either cybersecurity or privacy. / The implementation of the GDPR in May 2018 represents a game changer in terms of not only its scope and ambition, but also the significant penalties for non-compliance with fines up to 4% of global annual turnover.



SHIFTING WEALTH

Consumers across the world profess to be concerned about privacy issues but also appear not to significantly moderate their behavior when faced with a data breach. / The aim of the evolving data protection regulation in Europe is to shift power back to the consumers and ultimately increase transparency and trust in how companies use data.

TECHNOLOGY

Although there appears to be a global consensus that privacy and data protection are important issues that need to be addressed by regulation, the asymmetric approach across regions is likely to make compliance a challenge. / These differences could lead to a similar level of asymmetry in terms of access to investment and 21st century consumer services – artificial intelligence, machine learning, and the Internet of Things.