Tax evasion and avoidance

EU national challenges HMRC over new data sharing rules

Common reporting standard was designed as a way to counter global tax evasion

HM Revenue & Customs: 'HMRC shares some personal data with overseas tax authorities to ensure that the right tax is being paid' © Louisa Svensson/Alamy

Barney Thompson in London AUGUST 1, 2018

An EU national is challenging HM Revenue & Customs over new rules that require tax authorities around the world to automatically exchange information on millions of their citizens who live abroad.

In a complaint to the UK's data protection regulator, the EU citizen said the common reporting standard — a key measure against tax evasion developed by international experts that is now being gradually introduced by more than 100 countries — made her personal information vulnerable to cyber hacking or an accidental leak.

However, campaigners have defended the measure, saying it was an important tool in the fight against tax avoidance and evasion, notably through offshore financial centres.

The EU citizen who has made the complaint about the common reporting standard — who does not want to be identified — is currently domiciled in Italy but is described as having "a very international background".

She lived in the UK for several years and was tax resident in Britain, acquiring a unique taxpayer reference and a national insurance number. She also still has a UK bank account with a deposit of £4,000.

Even with this relatively small amount, her bank is required under the common reporting standard to disclose certain information to the HMRC, including the account number, balance, her name, date of birth and tax number.

In turn, HMRC must pass on the information to its counterpart in Italy, which it is due to do in September.

Exchange of information would be automatic

In theory, any UK bank account holder living in another country that abides by the common reporting standard falls under the scope of its rules.

Within the EU, almost 19m people are estimated to live in a different member state to the one in which they were born.

Like the US foreign account tax compliance act, on which it is based, the common reporting standard was designed as a way to counter global tax evasion by making the exchange of information between countries automatic rather than have tax bodies request it if they suspect wrongdoing.

The standard was developed by the Organisation for Economic Cooperation and Development, the Paris-based international body that co-ordinates co-operation between different tax jurisdictions.

Several countries have poor data security

In her complaint against the common reporting standard to the UK Information Commissioner's Office, the EU citizen said the exchange of information required by the rules will expose her to "a disproportionate risk of data loss and potentially hacking".

She added: "This risk has crystallised recently in light of incidents in which HMRC has lost data concerning UK taxpayers and recent data breaches concerning UK banks."

The [standard] has given the tax authorities the information they previously did not have access to, which enables them to pinpoint where tax evasion is happening

John Christensen, director of the Tax Justice Network

Her complaint cited how HMRC had lost the personal records of 25m taxpayers in 2007, as well as a media report in 2017 outlining how the tax authority's website was vulnerable to cyber attacks. HMRC subsequently took action to fix the weaknesses.

Among the countries that have signed up to the common reporting standard are several with poor data security records, added the woman's complaint.

Furthermore, data leaks such as during the TSB online banking failure this year and attempts by cybercriminals to hack the online tax details of British taxpayers illustrated the dangers around the mass exchange of sensitive personal information, it said.

As a result, the common reporting standard infringed the new EU-wide General Data Protection Regulation, which came into force in May, as well as European human rights laws, said the complaint.

Rules risk 'identity theft on a grand scale'

The Information Commissioner's Office has the power to impose temporary or permanent limits on the processing of personal data if it decides that GDPR rules are being infringed.

The office said: "We have received a complaint relating to HMRC and the common reporting standard and will be looking into the details."

Filippo Noseda, a partner at law firm Mishcon de Reya who is acting for the EU national, said the data breach risks involved in the standard "could lead to identity theft on a grand scale".

Mr Noseda acknowledged that rich clients of law firms would appreciate not having their tax details and activities shared between authorities.

But he added: "The endgame is not to go back to banking secrecy. We need to find a system that is balanced."

John Christensen, director of the Tax Justice Network, a campaign group, defended the common reporting standard, saying it needed to be broad to deter individuals from using offshore structures to avoid and evade tax.

"The [standard] has given the tax authorities the information they previously did not have access to, which enables them to pinpoint where tax evasion is happening," he added.

"Tax avoidance and evasion are . . . deliberately and purposefully depriving tax authorities of finances."

HMRC declined to discuss the EU citizen's case but added: "HMRC shares some personal data with overseas tax authorities to ensure that the right tax is being paid. HMRC only ever shares information when it's entirely lawful to do so. This includes complying with applicable GDPR requirements."

Mishcon de Reya LLP

Legal challenge to Common Reporting Standard (CRS) and Beneficial Ownership (BO) registers

Posted on *01 August 2018*

Mishcon de Reya has taken legal steps against the Common Reporting Standard (CRS) and the Beneficial Ownership registers to call into question the wider repercussions for fundamental rights and the relationship between individuals and the State. The majority of UK bank account holders living in one of the 100 plus countries that have joined the CRS will be affected by this, with many of these countries having lesser standards of data protection and/or information security.

The CRS and the Beneficial Ownership registers have been introduced to fight tax evasion and money laundering. In addition, Beneficial Ownership registers should (in the eyes of their proponents) provide additional economic benefits by making information about the ownership of companies fully accessible to the public. In the UK, ultimate beneficial ownership information has been available online since 2016 and other EU Member States will have to remove the need to demonstrate a "legitimate interest" by 2020. Practically, anyone owning a substantial interest in a private company based in Europe (or with a European subsidiary) will see their details published, regardless of where they are resident, the nature of the business or the nature of their involvement in that business.

However the rights to privacy and data protection are fundamental rights. They are the cornerstone of the General Data Protection Regulation (GDPR) – which came into force in May 2018 – and emanate directly from European Convention on Human Rights and the EU's Charter of Fundamental Rights. The transformational nature of the GDPR in defining the relationship between businesses and their customers is indicative of the strength of the fundamental rights to privacy and data protection. In order to be justified, any interference with these rights needs to have a clear legal basis, pursue a legitimate public interest (such as the fight against crime); and be proportionate, i.e. *limited to what is strictly necessary* to achieve the objective pursued.

Our contention is that the publication of sensitive data concerning the internal governance and ownership of private companies by the Beneficial Ownership Registers is not necessary to achieve the stated objectives. Similarly, we believe that the exchange of information under the CRS is excessive, as information is exchanged indiscriminately and affects all account holders regardless of the size of the account. The information exchanged under the CRS includes sensitive personal data (such as the name, date/place of birth and tax identification number of the account holder) as well as financial data about the financial account itself such as the account number and balance. This exposes compliant account holders to risk of hacking and data loss: it could lead to identity theft on a grand scale.

The challenge, as stated by a European data protection authority (Article 29 Working Party) in a letter to the OECD and the EU dated 12 December 2016, is to *"identify methods to pursue the legitimate aim of fighting tax evasion through efficient mechanisms that do not expose individuals' rights to disproportionate interference"*.

Multiple letters have been written to Her Majesty's Revenue and Customs (HMRC) and Companies House to ask for confirmation that they will not exchange or publish information under the CRS or the UK version of the Beneficial Ownership Registers (a.k.a. 'PSC' registers). HMRC has already formally refused to provide such confirmation.

Accordingly, a formal complaint has now been issued to the UK's Information Commissioner under the GDPR copying in the EU's data protection authorities.

Mishcon de Reya Partner Filippo Noseda [https://www.mishcon.com/people/filippo_noseda], who is leading this legal action, said:

"*After more than three years of assiduous campaigning on this issue and the publication of a comprehensive report* [https://academy.mishcon.com/the-report/] *by the Mishcon Academy* [*https://academy.mishcon.com/*]*, the time has come to take action. There is a wealth of objective evidence supporting our proposition not least the comparisons made between the CRS and the Data Retention Directive – the latter of which was effectively declared illegal by the European Court of Justice in 2016. In a democratic society, the rights to privacy and data protection are an essential safeguard to protect compliant citizens against potential abuses and must be treated with the appropriate seriousness by the authorities.*"

To find out more about the legal action please contact CRS@Mishcon.com [mailto:CRS@Mishcon.com].

Related links

EU national challenges HMRC over new data sharing rules **[https://www.ft.com/content/679e65a8-94a9-11e8-b67b-b8205561c3fe]** - *Financial Times* (subscription only)

People

- **Filippo Noseda** [/people/filippo_noseda]

Categories

- News [/news/#type-filter/1]
- Media [/news/media]
- Publications [/news/publications]
- Events [/news/events]

An

We Value Your Privacy

We use technology such as cookies on our site to personalise content, provide certain functionality, and analyse our traffic. Click *Accept* to consent to the use of this technology across our site. You are able to toggle on or off your consent preference based on individual purpose for all companies listed under each section below. You can change your mind and revisit your consent choices at anytime by returning to this site.

Strictly necessary Always on ☑

We need to use some cookies to ensure that the site operates correctly. For example, we must use a cookie to store your selection on this page.

Functionality ☐

Anonymous random ID not shared with any third parties used to power certain site functions that improve the site functionality based on the services that interest you. The following features rely on this cookie:

- Recent searches
- Suggested services

Anonymous Measurement ☐

Third party tools that we use to ensure that the site is working correctly and that we are providing the best possible service to our customers. No personally identifiable data is collected by these services to ensure you privacy. The following tools are used by Mishcon:

- HotJar

Vendor information: Hot Jar

- Privacy link [https://www.hotjar.com/legal/policies/privacy]
- Cookie Information [https://www.hotjar.com/legal/policies/cookie-information]
- Opt-out [https://www.hotjar.com/legal/policies/cookie-information]

Usage:

- Hotjar provides anonymous insight into website usage and helps us understand what users want, care about and do on the website.

Performance ☐

To measure the performance of our communications to our users we use tools provided by third parties to track which campaign is the most effective. The third party partners we use for this purpose are:

- Facebook

- LinkedIn Insight Tag
- Opentracker
- Vuture-Vx

Privacy policy: Facebook

- Privacy policy link [https://www.facebook.com/business/learn/facebook-ads-pixel]

Purposes:

The Facebook Pixel provides insight from visitors who have visited the Mishcon Facebook page or clicked on a Mishcon advert.

Privacy policy: LinkedIn

- Privacy policy link [https://www.linkedin.com/legal/cookie-policy]

Purposes:

The LinkedIn Insight Tag enables in-depth campaign reporting and provides insight into website visitors.

Opentracker

- Opentracker cookies [https://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies]

Purposes:

Opentracker is a solution for website and app traffic reporting and analytics. It specialises in business intelligence and serves as an analytics tool to track digital events and engagement important to our website – including clicks, logins, downloads and forms.

Vuture-Vx

- More on Vuture Cookies [https://vutu.re/cookies/cookies.aspx]

Purposes:

Vuture is a web based marketing platform that facilitates personalisation and provides insight into website usage.

Advertising Always off ☐

We don't use any targeting advertising cookies on mishcon.com

Third-party cookies

Google Analytics is used on mishcon.com to collect anonymous data. Storage of user data is for historical research.

Company
Google
LinkedIn
Vuture
See all cookies used Back to consents
Cancel Recommended
How can we help you?

How can we help you?

Subscribe: I'd like to keep in touch [/subscribe]

If your enquiry is urgent please call +44 20 3321 7000 [tel:+4420332217000]

I'm a client

First name * Last Name*

First name* Last Name*

Enquiry details *

Please describe your enquiry*

Mishcon Contact

Mishcon Contact

Email*

Email

Phone*

Phone

Contact method

Email Me Call Me

I'm looking for advice

First name* Last name*

First name* Last name*

Enquiry details*

Please describe your enquiry*

Please select relevant department * Please select department

Email*

Email

Phone*

Phone

Contact method*

Email Me Call Me

Something else

First name* Last name*

First name* Last name*

Nature of your enquiry* Who do you want to contact?*

Enquiry details*

Please describe your enquiry*

Email*

Email

Phone*

Phone

Contact method*

Email Me Call Me

withersworldwide

CRS and beneficial ownership

16 MAY 2016

CATEGORY:
ARTICLE

In today's difficult economic climate, countries need more than ever to ensure that they collect all the tax revenues that are due to them in order to fund public expenditure and reduce public debt. The arrival of new technologies has made it easier to collect and exchange information to fight tax evasion.

As the Panama Papers have shown, financial information can be easily stored and retrieved electronically on a global scale. Unsurprisingly, therefore, Governments have been considering the introduction of a global system for the automatic exchange of information. Although the implementation of this system has proceeded at speed, and with minimal scrutiny, it raises major questions about several issues:

1. 'Fantastically corrupt countries'

David Cameron's unguarded comments to the Queen, which were caught on camera, are a stark reminder of the dangers faced by individuals in many parts of the world. Indeed, a number of countries that have embraced the OECD's global standard for information exchange regularly appear on international corruption and crony-capitalism indexes, such as the 2015 Corruption Perceptions Index (CPI) published by Transparency International and the 2016 crony-capitalism index published by the Economist. This raises serious concerns about the potential use of information obtained through automatic exchange, and it may not be a coincidence that a large number of corrupt countries that have joined the information exchange bandwagon.

2. The missing $951m – the issue of cyber-security

As David Cameron's private conversation with the Queen also shows, information that is intended to stay private can easily be intercepted and put to different uses. Recent news about cyber-security breaches – such as the attack on the SWIFT system that led to the unauthorised transfer of $951m (of which $81m could not be recovered) belonging to the National Bank of Bangladesh; and statistics released by the UK authorities showing that two-thirds of large UK businesses are hit by cyber-attacks and that the UK tax authorities are hit by 15m malicious emails annually (leading the government to pledge 1.9bn towards cyber-security) – clearly show the risks posed by automatic information exchange. The recent case involving TalkTalk (the UK telephone and broadband provider) shows the risk of data loss for customers (on 12 May 2015, TalkTalk announced that a recent hacking attack (which resulted in the personal data of nearly 160,000 people being accessed, including phone numbers and bank details) cost the company 42m – or half of its profits. In the words of a cyber-security expert: 'Getting their hands on all the personal and financial data involved in a tax return is a cyber-criminal's dream. Armed with an individual's banking and financial history, their employment information, date of birth, address and login details, a criminal could carry out a sophisticated identity theft. For instance, they could potentially take out a mortgage in that person's name.
In the case of the new EU public registers of beneficial ownership not only hackers, but also common criminals may gain access to sensitive information. Although the EU rules provide that access to the new registers will require the demonstration of a 'legitimate interest', a number of countries (such as the UK) have already opted for full public access, which shows the disproportionate nature of the new measures.

3. A word of warning from the European Court of Justice and data protection agencies

In the recent 'Facebook' case, the European Court of Justice (ECJ) held, inter alia, that:

- 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life'
- 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.'

- 'Legislation [that] authorises, on a generalised basis, storage of all the personal data (…) without any differentiation, limitation or exception (…) is not limited to what is strictly necessary [to achieve the legitimate public objective pursued]'

Unsurprisingly, therefore, a number of European data protection bodies have raised concerns about the new rules on automatic exchange of information. These include –

- the European Data Protection Supervisor (EDPS);
- the Article 29 Working Group (that was established under Art. 29 of the European Data Protection Directive);
- the AEFI Group of experts appointed by the EU Commission to supervise the implementation of the EU Automatic Information Exchange Directive; and
- the Human Rights Directorate of the Council of Europe.

In particular, the European Data Protection Supervisor lamented that 'a number of corrections should have been made (…) to better address data protection issues' and the AEFI Group warned the EU about the risks of rushing through the new rules. In the words of the independent experts 'The Council and the Member States are urged to provide an achievable implementation timetable. Consideration should be given to a phased approach to implementation. This could be achieved by pushing back reporting by 1 year, with the reporting being made in 2018 in respect of both 2016 and 2017 data. (…) The Commission, the Council and the Member States must conduct a careful analysis of legal, constitutional and data protection implications of [the new Directive] and ensure that all steps have been taken to comply with data protection rules.' (…) Ultimately, if the reporting is rushed, the quality of data that governments will be exchanging will be lacking.'

4. When politics gets in the way of policy

In a democratic society based on the rule of law, one would have expected governments to sit up and take notice of the advice proffered by data protection experts, as well as consider the implications of the ECJ's rulings. However, too much is at stake, as the seeds for the global standard of automatic information exchange were sown at the G20 London Summit of 2 April 2009, when governments were struggling to save the world from financial collapse, and the effects of indiscriminate information collection and processing had yet to be revealed by Ed Snowden in 2013 (the ECJ judgment in the Facebook case relied heavily on the effects of those revelations).

Before Snowden, and ever since 9/11, governments were singly focused on collecting information on individuals without any regard for the fundamental rights of privacy and data protection, something that came back to haunt them. For example, the UK Intelligence and Security Committee recently warned the government that 'Given the background to the draft Bill and the public concern over the allegations made by Edward Snowden in 2013, it is surprising that the protection of privacy – which is enshrined in other legislation – does not feature more prominently'.

However, recent events have made it politically unthinkable for governments to pause for breath in their campaign launched nearly seven years ago, when the world was different. The stakes appear to be too high, not least for the OECD, which ironically is comprised of unelected bureaucrats that enjoy extensive privileges, such as exemption from taxation in respect of their salaries. This, and the fact that the new rules have been pushed through by ministers (G5 and G20 leaders – see the introduction to the OECD Commentary) with little involvement from parliaments, shows that the new rules suffer from a democratic deficit.

5. When nobody listens, it's time to speak up

Unfortunately, nobody seems to be willing to raise the disproportionate nature of the rules developed by the OECD and endorsed by G20 governments. Not offshore jurisdictions, who are perceived as inherently dodgy and in many cases depend upon G20 countries. Not the banking community, which has been reeling from a loss of credibility due to a string of appalling scandals. Not even professional bodies, which appear unable or unwilling to elaborate a cohesive message around the underlying legal issues.

In the light of incessant press campaigns and revelations, people might be excused for taking a cautious approach. However, the issues raised by a system of indiscriminate exchange of information without safeguards for individuals' right to privacy goes to the heart of democracy. I am, of course, not talking about the right to privacy of tax evaders – who do not deserve it – but of the right to privacy of everybody else.

For this reason, I have written to the European Data Protection Supervisor, the Art. 29 Working Group, the AEFI Group of Experts and the Human Rights Directorate of the Council of Europe urging them to take urgent action.

6. Don't throw out the baby with the bathwater

As the fight of tax evasion is an important objective, the letter to these bodies contains proposals which would enable countries to collect their taxes in a way that would respect the fundamental right to privacy, especially in cases where confidentiality is a real concern (e.g. in countries where corruption is rife). These proposals include the implementation of final withholding tax agreements (under which financial institutions would withhold the correct amount of tax and transfer it to the relevant tax authorities), and the idea – which was first mooted by another professional – of introducing a global clearing house which would provide financial institutions with the relevant tax calculations based on data fed into a single secure system, thus by-passing direct data traffic between poorly resourced tax authorities.

In addition to reducing the intrusion into individual's private life to the minimum, the taxpayer's option to choose between information exchange and withholding tax would reduce the administrative burden for tax authorities, which under the current system of global exchange of information would have to make sense of many terabytes of complex information.

STEP
ADVISING FAMILIES ACROSS GENERATIONS

INDUSTRY NEWS

EU citizen alleges CRS account data sharing is unlawful

Thursday, 2 August, 2018

An Italian-domiciled woman has lodged an official complaint with the UK's Information Commissioner, alleging that the disclosure of her personal and financial information to other countries under the OECD's Common Reporting Standard (CRS) infringes the European Union's *General Data Protection Regulation*.

The unidentified woman is being represented by Filippo Noseda TEP, a partner at law firm Mishcon de Reya. Noseda has been challenging the CRS since 2015, on the grounds that it has serious repercussions for fundamental rights such as privacy, and for the relationship between individuals and the state.

The recent EU initiative to introduce central registers of beneficial ownership of companies has the same drawback, he says. 'Practically, anyone owning a substantial interest in a private company based in Europe, or with a European subsidiary, will see their details published, regardless of where they are resident, the nature of the business or the nature of their involvement in that business.'

Noseda contends that the publication of sensitive data concerning the internal governance and ownership of private companies by the beneficial ownership registers is not necessary to achieve the authorities' stated objectives. 'Similarly, we believe that the exchange of information under the CRS is excessive, as information is exchanged indiscriminately and affects all account holders regardless of the size of the account.'

The information exchanged under the CRS includes personal data such as the name, date/place of birth and tax identification number of the account holder, as well as financial data about the financial account itself such as the account number and balance.

'This exposes compliant account holders to risk of hacking and data loss', warns Noseda. 'It could lead to identity theft on a grand scale.'

According to Mishcon, any interference with these rights can only be justified if it has a clear legal basis; pursues a legitimate public interest such as the fight against crime; and is proportionate, i.e. limited to what is strictly necessary to achieve the objective pursued. The firm has written to HMRC asking for assurances that they will not exchange or publish information under the CRS or the UK's beneficial ownership registers (also called Persons with Significant Control or PSC registers). Not surprisingly, HMRC has refused to do so.

Mishcon has now decided to take formal action via its Italian-domiciled client. The client has an international background, having been UK tax resident for several years, and still has a UK bank account with a modest balance. It is this account that will be reported via HMRC to foreign tax authorities, along with her name, date of birth, and UK tax identification number. She has told the UK's Office of the Information Commissioner – the data protection regulator – that these disclosures amount to a disproportionate risk of data loss and potential hacking.

'In a democratic society, the rights to privacy and data protection are an essential safeguard to protect compliant citizens against potential abuses', says Mishcon de Reya. 'They must be treated with the appropriate seriousness by the authorities.'

Sources

- Mishcon de Reya
- Mishcon (report on CRS privacy implications, January 2018)
- Withers (May 2016)

Common Reporting Standard and EU beneficial ownership registers: inadequate protection of privacy and data protection

Filippo Noseda*

Abstract

This article contains a summary of a technical presentation given on 7 September 2016 to the independent EU data protection body established under article 29 of the EU data protection directive ('Article 29 Working Party' a.k.a. 'WP29'). Like numerous other European privacy and data protection bodies, WP29 raised concerns in the past about the proportionality of the Common Reporting Standard (CRS). The scope of the presentation was to illustrate the actual impact of the CRS based on practical examples analysed in the light of general tax law principles. A similar presentation was made to the Council of Europe's Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in June 2016. (The Council of Europe is the platform used by 103 countries to implement the CRS on a multilateral basis.) This note is provided for general information purposes only and it should not be reproduced or copied (in whole or in part) without the written authorization from the author.

Concerns about the general structure of the Common Reporting Standard

The Common Reporting Standard (CRS) is essentially a tax measure that was designed to combat tax evasion in the country of residence of the relevant account holder. As such, any privacy and data protection analysis should take into account specialist insight.

In terms of the CRS's *general structure*, I refer in particular to the *generalized* basis of information exchange and the fact that information is exchanged in a manner that is *independent of the detection of any actual risk of tax evasion*.

> *The CRS provides for an exchange of information that is generalized and independent of the detection of any actual risk of tax evasion*

It is for data protection authorities to consider technical data protection issues in detail. However, it is noteworthy that the ECJ held as recently as 6 October 2015 that legislation permitting public authorities to have access, on a generalized basis, to the content of electronic communication, without any differentiation, limitation, or exception and without providing for any legal remedies, did not respect the essence of the fundamental rights to privacy and data protection.[1]

The bigger picture

The commentary published by the Organization for Economic Cooperation and Development (OECD) confirms that the CRS was developed between 2009

* Filippo Noseda, Solicitor, Withers LLP, 16 Old Bailey, London EC4M 7EG, UK.

1. *Schrems v Data Protection Commissioner*, Judgment dated 6 October 2015, Case C-362/14 <http://curia.europa.eu/juris/liste.jsf?num=C-362/14> accessed 1 January 2017.

 doi:10.1093/tandt/ttw243

and 2012 with the objective of capturing and exchanging the maximum amount possible of information, with very little concern for privacy and data protection issues.

Outside the field of taxation, the excesses of generalized data collection and exchange were exposed in 2013 by Edward Snowden, resulting in a public outcry and a counter-revolution to reassert the prevalence of the fundamental rights of privacy and data protection. In the EU, this culminated in the ECJ's decision of 6 October 2015 in the *Schrems* case and the EU data protection reform on 27 April 2016, which was introduced to '*allow people to regain control of their personal data*'.[2] Outside the field of taxation, public concerns for the right to privacy and data protection have been further strengthened by a number of high-profile cases and data breaches that took place at the end of 2015 and the beginning of 2016, including the *Apple v FBI* case[3] and the $81m heist against SWIFT.

The broader views of society in relation to privacy and data protection appear to be based on two contrasting sentiments depending on whether the debate focuses on the field of taxation or not. However, the right to privacy is *not a relative value*. Instead, *any* interference with an individual's right to privacy has to comply with the *same requirements* of legality, legitimate interest, and proportionality, as outlined by the European Commission's Article 29 Working Party (WP29) in the past.

Data security

Over the past two years, several hacking incidents showed the inability of governments and supranational authorities to protect sensitive data of ordinary citizens. In addition to the attack against SWIFT (which led to the theft of $91m), it has been reported that government authorities in several countries (including the USA, Turkey, and the Philippines) lost sensitive data (passport details, fingerprints, background checks, social security numbers, etc) concerning tens of millions of citizens to hackers.[4]

Under the CRS, information about:

- the identity (name, tax identification number, date and place of birth); and
- detailed bank account information (account number, account balance, amount of income and sale proceeds, etc) of virtually every individual with a bank account abroad will be captured and exchanged electronically between banks and their tax authorities, and between tax authorities around the globe. This will provide the international hacking community, financial criminals, and 'dark web' users with an unprecedented opportunity.

WP29 and other data protection bodies—including the European Data Protection Supervisor (EDPS) and the Council of Europe's committee on automatic processing of personal data—have already raised serious concerns in relation to the proportionality of the CRS. These include the general and automatic nature of information exchange, the fact that automatic exchange is independent of the detection of any actual risk of tax evasion, and other concerns based on *general principles of privacy and data protection law*.

A ticking bomb

Discussing 'DAC2', a European Council Directive on mandatory exchange of information, the group of experts appointed by the European Commission ('AEFI Group') issued a stark warning addressed to the EU institutions:

> On many aspects, DAC2 may be compared with the Data Retention Directive which has recently been

2. <http://europa.eu/rapid/press-release_IP-15-6321_en.htm>.

3. In an interview with *Time Magazine*, Apple's CEO referred to the right to privacy as *'one of the founding principles of the country'* <http://time.com/4261796/tim-cook-transcript/>. It is noteworthy that a wide segment of public opinion sided with Apple's controversial decision, showing a single-minded focus on the right to privacy *of law-abiding citizens* (even if it meant frustrating an investigation in a hideous crime).

4. Since the presentation to WP29, Yahoo! confirmed that the data of 1 billion of its users has been lost to hacking, confirming the data protection concerns surrounding the implementation of the CRS.

> declared illegal by the CJEU. DAC2 must respect the principle of proportionality. . . . A legal challenge might arise from the current version of DAC2 mainly because of the magnitude of the data to be collected and reported and the fact that it does not guarantee taxpayers a permanent access to their data and a mandatory notification in case of breach. . . . In its current version, DAC2 might be challenged because it does not request the existence of such sufficient cause or indicia of unlawful behaviour. . . . The AEFI Group is concerned that information exchanged may happen to be irrelevant for taxation purposes in the receiving jurisdiction (home country) under domestic law and that reporting in such cases might be treated as being in breach of data protection law.

On many aspects, the CRS may be compared with the Data Retention Directive which has already been declared illegal by the European Court of Justice

This quest for *total transparency* first introduced under the CRS seems to have spilled over to the field of public registers of beneficial ownership. Thus, despite the safeguards imposed by the Fourth Anti-Money Laundering Directive of 20 May 2015:

- At the beginning of 2016, the UK introduced public registers of 'People with Significant Control' in respect of UK companies and limited liability partnerships ('PSC registers') that may be accessed *by anyone*.
- On 10 May 2016, France introduced a *fully public* register concerning trusts (since declared unconstitutional by the French Constitutional Council).[5]

On 21 October 2016, The French Constitutional Council declared that France's public register on trusts was unconstitutional

Political inactivity in relation to the safeguard of fundamental rights in the context of the CRS and public registers requires a vigorous response ahead of the full implementation of the new rules. In the case of the CRS, this will take place at the beginning of 2017 for a number of countries ('early adopters'), as well as the EU).[6]

The lack of political engagement is the more perplexing as there are a number of existing alternatives, which would enable countries to combat tax evasion in a proportionate way. These include traditional information exchange mechanism (Article 26 OECD Model Tax Convention), Tax Information Exchange Agreements (existing case law shows that they work) and calibrated automatic exchange agreement that enable taxpayers to choose between exchange of information and a withholding tax that reflects the level of taxation in their home jurisdiction. This is the solution contained in two agreements signed by Switzerland and two EU Member States (Austria and the UK), before the G-20 and the OECD decided to go down the Foreign Account Tax Compliance Act (FATCA) route instead and unleashed the CRS storm.

The lack of political engagement is the more perplexing as there are a number of existing alternatives

Implementation process—current threats

In order to be compatible with the European Human Rights Convention and the EU Charter of Fundamental Rights, an interference with an individual's right to privacy and data protection must be (i) in accordance with the law; (ii) in pursuit of recognized legitimate aims (which include the prevention of crime); and (iii) necessary in a democratic society.

5. Decision n° 2016-591 QPC du 21 Octobre 2016, available online at <www.conseil-constitutionnel.fr/decision/2016/2016591qpc.htm> accessed on 1 January 2017.

6. In the EU, the CRS has been implemented through the EU Revised Directive on Administrative Cooperation ('DAC2'), Directive 2014/107/EU <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0107>.

Blanket and indiscriminate nature of automatic exchange under CRS—(Proportionality I)

WP29, the EDPS, and the Council of Europe's T-PD have already identified a number of issues in relation to the proportionality of the CRS. Questions must also be raised in relation to the compatibility of the CRS with the principles laid down in the ECJ's decision in the *Schrems* judgment of 6 October 2015, where the ECJ held, *inter alia*, that:

a. Legislation permitting the public authorities to have access on **a generalised basis** to the content of electronic communication **must be regarded as compromising the essence of the fundamental right to respect of private life**;
b. Legislation that authorises storage of all the personal data on a generalised basis, **without any differentiation, limitation or exception** is not limited to what is strictly necessary.
c. Legislation **not providing for any possibility** for an individual **to pursue legal remedies in order to have access to personal data relating to him, to obtain the rectification** or erasure of such data, **does not respect the essence of the fundamental right to effective judicial protection**, as enshrined in Art. [8 of the European Convention on Human Rights and] Art. 47 of the EU Charter of Fundamental Rights. (emphasis added)

Questions must also be raised in relation to the interaction between the CRS and the new EU data protection framework adopted on 27 April 2016, notably the General Data Protection Regulation[7] and the Data Protection Directive for the police and criminal justice sector,[8] both of which were introduced to '*allow people to regain control of their personal data*'.[9]

Excessive level of information gathering under CRS—(Proportionality II)

The CRS requires the gathering and exchange of vast amounts of information that is often not foreseeably relevant—or is even outright and clearly irrelevant—to the enforcement of domestic taxes.

Specific concerns about the actual mechanics of the CRS

During the presentation, the author discussed a number of specific CRS scenarios confirm and amplify the existing concerns about the proportionality of the CRS, notably:

a. **The exchange of information concerning the *value* of investments:** In circumstances where it is clear that the taxpayer does not owe any tax in his/her country of residence in respect of the value of those investments (eg in countries that do not levy a wealth tax).
b. **The exchange of information in relation to *taxpayers who benefit from a special tax regime*:** In circumstances where it is clear that the information exchanged is not relevant in their country of residence in order to determine and monitor their tax liability. During the presentation, the following special tax regimes were considered: (i) '*cadre étranger*' (*Belgium*), '*régime des impatriés*' (*France*), 'habitual non-resident' taxpayers (*Portugal*), so-called 'Beckham Law' (*Spain*) and the 'remittance basis' for 'non-domiciled' taxpayers (all European common law jurisdictions, notably *Ireland, Malta, Cyprus, and the UK*).
c. **The exchange of information concerning individuals in relation to companies, trusts, foundations, etc based on a single 'one-size-fits-all' concept (ie the concept of 'Controlling Persons'):**

7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC>.

8. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. This directive is accessible online at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC>.

9. <http://europa.eu/rapid/press-release_IP-15-6321_en.htm>.

The concept of 'Controlling Persons' (which is absent in FATCA) is independent of any domestic tax attribution rules under domestic law ('Controlled Foreign Companies' rules, 'Transfer of Assets Abroad' rules, etc) and is at odd with the ECJ case law in this area (notably the Cadbury Schweppes case).

d. **Taxpayers without any taxable income/gains in the relevant tax period:**

The reporting of the value of the taxpayer's assets is also not relevant in circumstances where the taxpayer does not have any taxable income and/or gains in the relevant tax period, either in absolute terms or after deduction of expenses/losses in accordance with the domestic rules in the country of residence of the taxpayer.

e. **Reporting scenarios in the case of Charities:** Charities are not generally exempt from reporting under the CRS and, in practice, the reporting profile of a charity depends on whether it is:

1. an 'active non-financial entity' (active-NFE)—in which case there is no reporting[10]; or
2. a financial institution—in which case the charity has to report any individual who has an 'Equity Interest' in the charity.[11]

The *general nature* of information gathering and the *automatic nature* of information exchange under the CRS may easily translate into a life in danger, regardless of the existence of any tax liability, for charities engaged in work in jurisdictions where the local authorities are resistant or opposed to their activities.

f. **The complexity of the drafting technique used in the CRS:** The CRS is broadly a derivation of FATCA,[12] which a US commentator defined as 'monstrous' and 'daunting even to the most knowledgeable experts [of US tax law]'.[13] Over the past year, EU-based banks, account holders, and their advisers are struggling to follow the

10. The reason for the exclusion of active entities from the scope of the CRS stems from the US FATCA, which was introduced essentially to counter the activities exposed by banking scandals; those showed how private banks helped US taxpayers to hide money and investments behind anonymous accounts—such as numbered accounts and accounts held by offshore companies/trusts and foundations. In other words, the main focus of FATCA (and the CRS) is on 'empty'/'passive'/'secret' structures, which leaves out ordinary businesses such as an active enterprise.

9. One would expect the term 'Financial Institution' to comprise banks and the like, not charities. Again, the reason for the extension of the concept of 'Financial Institution' to charities (and other entities) stems from FATCA. FATCA sought to root out the connivance of private banks with US tax fraudsters by introducing a withholding tax of 30% on US investments, which a financial institution (such as a bank) investing on behalf of its clients, could only avoid by registering with the IRS. Under the registration system, the relevant financial institution undertakes to disclose any 'substantial US owner' who may owe US tax. Also, by showing its registration number ('Global Intermediary Identification Number' or GIIN) to paying agents, the relevant bank may receive payments of dividends, etc without the 30% withholding tax. As FATCA is about registration, certain companies/foundations/trusts, etc may avoid complex reporting by their bank(s) by registering directly with the IRS. In this case, the relevant structure is treated as akin to a financial institution, meaning that any reporting lies with the entity itself (rather than the 'real' financial institution, ie the bank). In other words, the entity becomes the relevant 'Financial Institution' replacing the 'ordinary' financial institutions (banks, etc) in the reporting chain. As FATCA seeks to stamp out secrecy, the system is relatively liberal when it comes to registration by foreign entities (as visibility is key).

Although the CRS system is not based on registration with the tax authorities it has maintained the distinctions introduced by FATCA. This means that certain structures qualify as 'Financial Institutions', thus relieving the relevant bank from reporting. Also, while a bank's reporting relates to its clients ('Controlling Persons' in the case of an entity), an entity that is treated as akin to a financial institution has to report on itself. This introduces a separate concept from 'Controlling Person', ie the entity has to report any person who has an 'Equity Interest' in the structure. The difference between 'Controlling Person' and 'Holder of an Equity Interest' has caused a lot of confusion, which has been partly fuelled by the OECD. Moreover, as the type of classification shifts the burden of reporting from the bank to the client (and vice versa), discussions with banks ahead of the implementation of the CRS have tended to be quite fractious and divisive (as well as expensive) This topic is addressed further later in this article, as the *lack of clarity* of the CRS affects its *proportionality*—a law must be adequately accessible and foreseeable, ie formulated with sufficient precision to enable the individual to regulate his or her conduct (see *Huvig v France,* Appl No 11105/84, ECtHR, 24 April 1990).

12. The use of concepts such as 'FI' (Financial Institution), 'active NFE' (active Non-Financial Entity), 'passive NFE' (passive Non-Financial Entity), 'Equity Interest', etc have been lifted directly from FATCA and have broadly the same meaning. Under FATCA, an FI (Financial Institution) is called an FFI (Foreign Financial Institution), an 'active NFE' is called 'active NFFE' ('active Non-Financial Foreign Entity', a 'passive NFI' is called a passive NFFI, etc.

13.

> FATCA is a Leviathan. And it breathes fire. Its size is monstrous (544 pages long). Moreover, the regulations are painstakingly detailed and excruciatingly technical, a bewildering maze of rules, sub-rules, sub-sub-rules, cross-references, exceptions, exceptions to exceptions and so on. They are daunting even to the most knowledgeable experts
>
> P Cotorceanu, 'FATCA and Offshore Trusts: The First Nibble' (2013) 139(4) Tax Notes 409.

structure and provisions of what is effectively a complex piece of US law transposed globally.

This raises the question as to whether the limitations to the right to privacy caused by the CRS are 'in accordance with the law', that is, whether the CRS is adequately accessible and foreseeable to enable the individual to regulate his or her conduct (as confirmed by case law from the European Court of Human Rights).

g. **The abstract nature of the CRS:** As a piece of US legislation, FATCA aims at ensuring that any tax liability arisen in accordance with the US tax rules is notified to the IRS. Accordingly, FATCA has been designed to comply with a specific domestic tax system (US tax law). By contrast, the CRS has not been designed with any particular tax system in mind, but broadly as a copycat of FATCA (with few alterations)

By applying a 'one-size-fits-all' approach that is independent of any domestic tax system, the CRS results in the exchange of excessive and often irrelevant information. Ultimately, this defeats the CRS's purpose of combating tax evasion, that is, the evasion of domestic tax laws in the country of residence of the account holder.

h. **The arbitrary nature of the CRS:** In many instances, the nature and level of reporting depends on the legal structure of the account holder, without any apparent reason for the difference of treatment.

One example: under the UK guidance, a charity may be required to exchange information in respect of people who receive a grant, but only if that charity is organized as a charitable trust (the common law equivalent of a charitable foundation)—and not if it is organized as a charitable company.

i. **The existence of a number of substantial contradictions:** The CRS contains contradictions in relation to a number of central concepts. In turn, this affects the amount and quality of information subject to information exchange. In particular, the OECD's *Commentary and Implementation Handbook* openly contradicts various definitions contained in the CRS (eg in relation to the concepts of 'Controlling Persons'/ holder of an 'Equity Interest').These contradictions have a direct effect on the DAC2, raising the question of whether the limitations to the right to privacy operated by the CRS are 'in accordance with the law'.[14]

Filippo Noseda *is a dual qualified English solicitor and Swiss lawyer, and joint head of the Private Client and Tax Department at Withers LLP in London. Email: filippo.noseda@withersworldwide.com.*

14.

In implementing this Directive, Member States should use the Commentaries on the Model Competent Authority Agreement and Common Reporting Standard, developed by the OECD, as a source of illustration or interpretation and in order to ensure consistency in application across Member States. Union action in this area should continue to take particular account of future developments at OECD level.