DENTONS

The Erosion of the Right to Privacy Through Global Steps to Improve Tax Compliance and Prevent Money Laundering

Part 1: How privacy is being eroded

Grow | Protect | Operate | Finance

This is part one of a two-part series on the tension between the fundamental right to privacy and global improvements in tax compliance and the prevention of money laundering and terrorism financing.

This is a topic that is increasingly of interest, particularly to high net worth individuals (HNWIs) and the family offices that serve them. The more data that is provided to governments and exchanged, the greater the risk of unauthorized disclosure of that data. Unauthorized access to data held by HNWIs and family offices themselves is also increasingly an issue, with cyberattacks against individuals and organizations increasing.

HNWIs face particular risks when the confidentiality of their data is not maintained. Unauthorized disclosure of private information can lead to unwanted media, public scrutiny and reputational damage. It can also result in physical risk—in certain countries, sensitive information regarding HNWIs can be purchased by third parties, creating a risk of extortion and kidnapping.

The Dentons survey report on *The Evolving Risk Landscape for Family Offices* (issued May 2024) identified disclosure of sensitive information as being a major risk to family offices. That report found that one in five family offices have suffered a cyberattack in the past year and four in ten know a family office who has been the victim of a cyberattack. Yet, only 29 percent of family offices indicated that they are prepared to deal with risks to their organization, while a staggering 38 percent were not prepared.

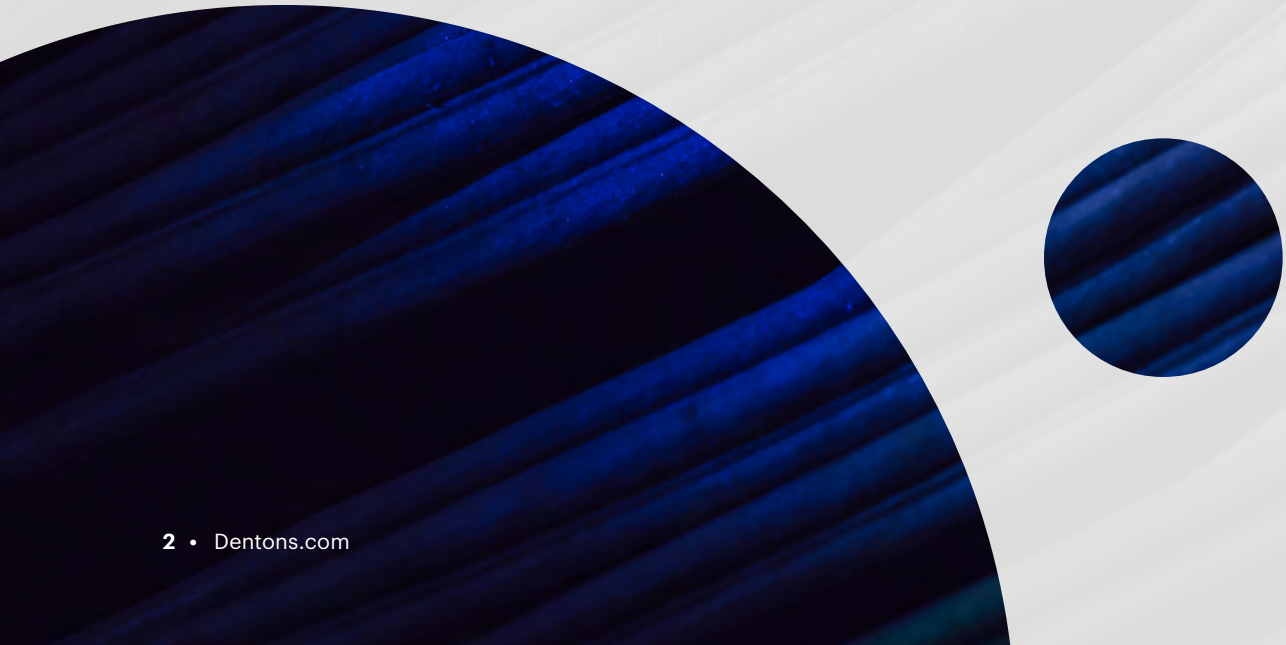
Setting the scene: privacy vs. transparency

The right to privacy is the freedom from intrusion by others in one's personal life or affairs. Privacy is protected by law and is a basic, but not absolute, human right. Total privacy does not exist as various laws, correctly, override the right.

Over the years, privacy rights have been abused by tax evaders and criminals. This mischief has arguably contributed to a proliferation in offshore wealth structuring, as wealthy people and multinational corporations set up bank accounts, companies and trusts in so-called tax havens.

However, globally, a paradigm shift is now happening as data about our everyday lives is increasingly available and valuable, meaning our privacy is not as protected as it once was. New compliance regimes now impose obligations on businesses and other third parties to disclose information to law enforcement and government agencies, which are cracking down on money laundering and tax evasion.

There are a plethora of human rights issues that arise from the latest approach to law and tax enforcement, from risks to open access to justice to existential threats to the very foundations of democracy. However, the reality is that these compliance regimes have been implemented and are here to stay. The Rubicon has been crossed, and now financial institutions and professionals must meet the challenge of compliance while protecting data as well as possible.



Privacy is a fundamental human right—with exceptions

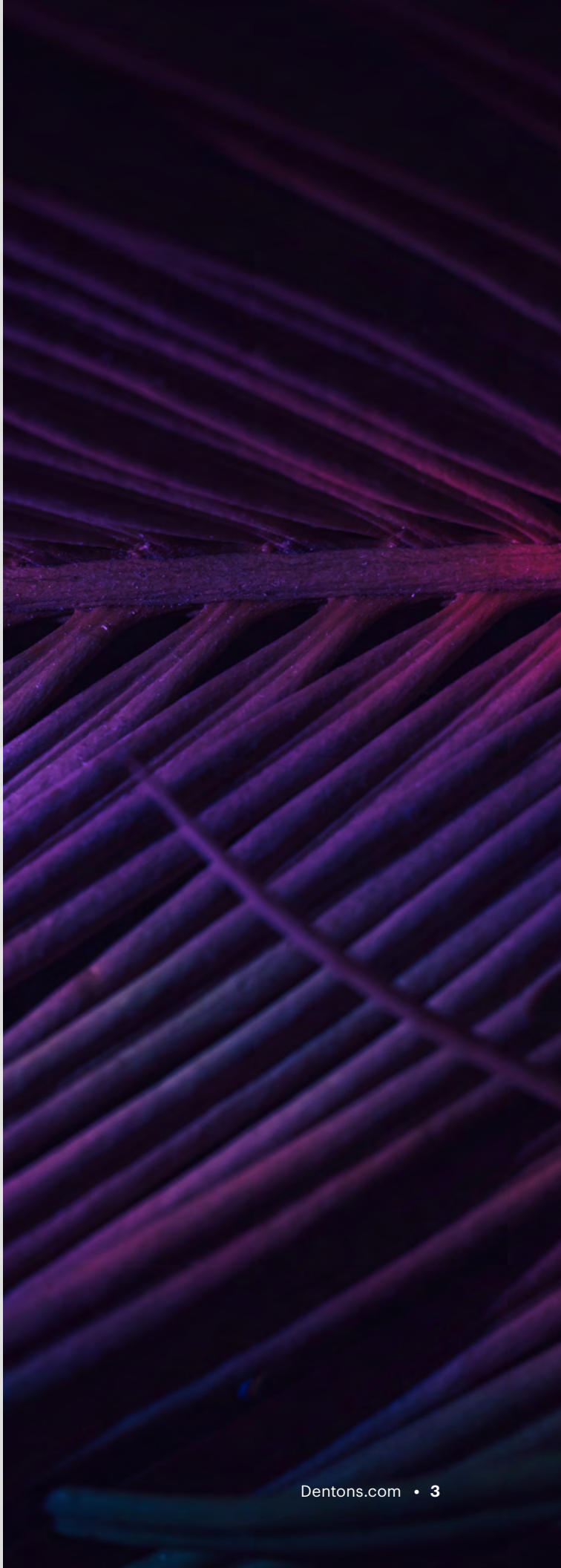
Article 12 of the Universal Declaration of Human Rights enshrines an individual's right to privacy. This is reflected in the domestic legislation of many countries, as well as in international instruments (such as the EU's General Data Protection Regulation 2016/679 (GDPR)), and even the law of equity (such as the equitable duty of confidentiality).

However, there are two main areas in which the right to privacy is overridden:

Tax evasion: This is the illegal failure to pay taxes. It involves deliberate misrepresentation to tax authorities of the true value of capital and/or income. By not declaring certain income, gains, profits or capital assets or by overstating deductions, a person (whether an individual or entity, such as a company) may reduce their tax liability. Tax evasion has historically been distinguished from tax avoidance, which is the legal structuring of affairs and use of tax laws to reduce the liability to pay tax.

Money laundering: This is the process by which criminals attempt to conceal the true origin of the proceeds of their criminal activities to make it appear as if they were obtained legitimately. This involves placing the proceeds of crime into the financial system, creating complex layers of financial transactions to disguise the origins of the funds, and then integrating the laundered funds into the legitimate economy. Money laundering is the lifeblood of a professional criminal enterprise because it can be used to advance other criminal objectives while reducing the risk of prosecution. The scale of money laundering ranges from crimes such as tax evasion to the financing of acts of terror, such as those that occurred in the US on September 11, 2001.

The extent to which the right to privacy has been overridden in these areas has accelerated in recent years, raising important legal and ethical questions about the increasing mass collection of taxpayer data and its disclosure.



How are governments responding to these crimes?

The terrorist attacks on 9/11 resulted in a new focus on the financing of terrorism, because it was clear that the terrorists were well-funded and supported by the global financial system. Accordingly, the Financial Action Task Force's remit was expanded to assist in fighting terrorist financing. Terrorist financing refers to activities that provide capital to fuel individual terrorists or terrorist groups. Terrorist financing involves processes similar to money laundering. Other developments introduced by governments to fight these crimes include:

AML/CFT legislation and regulations: Anti-money laundering and countering the financing of terrorism (AML/CFT) legislation criminalizes money laundering by making it a criminal offense for a person to inject the proceeds of their crime into the global financial system. More significantly, it also makes it a criminal offense for a financial institution to allow this to happen, thus imposing requirements on financial institutions to verify the identity of customers and the legitimacy of funds held in accounts. Money laundering has a material effect on developing countries in particular, because as capital is drained from their economies, development is inhibited through the perpetuation of poverty. In some cases, a small group of oligarchs entrench themselves in positions of power, authority and prosperity financed by the proceeds of crime. AML/CFT laws and regulations are aimed at detecting and preventing this type of activity.

Automatic exchange of information: In recent years, governments, led by the US, have joined in the global fight against tax evasion. The Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS) are the latest manifestations of their efforts. FATCA and CRS represent a generational shift in the way in which personal financial information is gathered, held and exchanged between financial institutions and governments. FATCA and CRS shift the burden of compliance away from taxpayers (after all, tax evaders could never be relied upon to report honestly) and instead impose that burden on the financial institutions (e.g., banks and trust companies) that serve them. If those financial institutions do not comply, withholding taxes and other penalties can then be applied by competent authorities and regulators.

EU's 4th AML Directive: In recent years, there has been a push towards collecting extensive information around beneficial ownership (BO). In many offshore jurisdictions there are, and have been for some time, requirements that trust and corporate services providers collect BO information. However, the new trend is focused on establishing centralized, national databases of BO information. The 4th Anti-Money Laundering Directive (4AMLD), which entered into force in June 2017, was the first practical measure implemented to achieve this goal. It requires EU member states to implement central BO registers (BORs) (referred to later in this paper) for trusts and trust-like entities. 4AMLD is primarily focused on tax concerns, rather than AML/CFT.

EU's 5th AML Directive: The 5th Anti-Money Laundering Directive (5AMLD) came into force in each member country by January 10, 2020. 5AMLD is essentially an extension of 4AMLD. The initial draft of 5AMLD provided for unfettered public access to the BORs of trusts maintained by each member state, which would remove the requirement to prove legitimate interest. In addition, the initial draft proposed to extend BO reporting to all trusts created, administered or operated in the EU, and not only those that have a tax consequence in a member state. The version

of 5AMLD that was ultimately adopted removed unfettered public access in relation to trusts and reintroduced the access rights for persons holding a "legitimate interest." However, 5AMLD also included a requirement for public access to BORs relating to companies, with no requirement to prove a "legitimate interest."

Beneficial ownership registers: A BOR is a centralized register that records the individuals who ultimately own or control a particular entity or asset. BORs are intended to increase the transparency of the ownership of entities and assets, in part to help prevent or investigate money laundering or other crimes. Due to the level of information that can potentially be included in BORs, the accessibility of the information is a material issue. At this stage, jurisdictions with functioning BORs generally restrict access to specific classes of people, such as law enforcement or tax agencies. Some jurisdictions have implemented the standard outlined in the EU directives (discussed earlier) of allowing access to individuals or groups that can evidence a "legitimate interest" in the information. This class is generally considered to include journalists.

EU mandatory disclosure rule: The European Council Directive 2011/16/EU on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC, known as DAC6, was created as a practical measure to strengthen tax transparency in the EU. DAC6 applies to any transaction between jurisdictions if at least one of them is an EU member state and the transaction qualifies as an "aggressive tax planning position." All jurisdictions in the EU were required to pass DAC6 into domestic law by July 1, 2020. The DAC6 amendment to include mandatory disclosure requirements was implemented in 2018 as a mechanism to aid tax authorities in the identification of potential money laundering or tax evasion practices and prevent non-compliance with the CRS. The measure requires anybody involved in an attempt to evade the CRS to disclose this to their local government.

Concerns with government responses

Many parties have raised concerns in relation to the privacy and data protection consequences of the 4AMLD and 5AMLD and other information disclosure regimes. The EU's own data protection regulator issued an opinion in 2017 criticizing the 5AMLD's introduction of public access elements. The opinion stated that this feature would infringe the privacy right under the European Convention on Human Rights (ECHR). Other privacy and data protection concerns and issues that have arisen in recent years include:

Legality: Article 8 of the ECHR and the Charter provide that "interference with an individual's right to privacy and data protection must be in accordance with the law." This principle requires that not only must there be a specific law that permits the interference in question, but also that it must be reasonably foreseeable and accessible to enable the individual to address their conduct before the interference occurs.

Proportionality: Proportionality is a bedrock principle of the EU legal system. This means that an action of the EU must be limited to what is necessary to ensure the functioning of the EU. In other words, are central registers proportionate or necessary in the fight against tax evasion and financial crime? Arguably the existing tools at the EU's disposal mean these measures are disproportionate, and it raises the question of what exactly the data is being collected for if existing automatic exchange of information and AML/CFT regulations are sufficient.

GDPR: The GDPR represents the most significant development in European privacy and data protection law in many years. The GDPR sets out a number of data protection principles that apply across the EU, including requirements to minimize the collection of data from individuals and to ensure that data is kept secure. Several aspects of the GDPR appear to be in plain conflict with 4AMLD/5AMLD, and the GDPR does not exclude public bodies from its scope. This particular aspect is the subject of litigation in the English courts.

***Re Helen S* decision:** Interestingly, the French government pre-empted the EU by introducing its own public register of trusts in 2016. The French Constitutional Court promptly struck the register down in the case of *Re Helen S*. In this case, an elderly woman challenged the legality of the register on the basis it would infringe her privacy and would require public disclosure of the bequests left in her will. The French Constitutional Court held that the public registry of trusts infringed the right to privacy in a disproportionate manner compared to the aim of fighting against tax fraud and evasion. The court declared the register illegal in its entirety.

Court of Justice of the EU decision: In one of the most significant recent decisions on this topic, the Court of Justice of the EU recently held that BORs of companies that are accessible to the public at large are invalid (CJEU Judgment). The court found this on the basis that public access infringes fundamental rights of respect for private life and of the protection of personal data. The decision followed a number of appeals in Luxembourg relating to that country's BOR, which provided public access to BO information regarding companies.

Data breaches: In April 2024, the US Internal Revenue Service (IRS) sent notifications to thousands of HNWIs that information from their tax returns had been publicly released by an independent contractor working for the IRS. From 2018 to 2020, this data breach resulted in the release of sensitive private financial information to several organizations, who then published articles about these HNWI that included the sensitive data.

Concluding comments

Privacy is a fundamental human right and one that is recognized in both international and domestic law.

It is accepted that there are some important exceptions to this right, particularly in order to combat money laundering, tax evasion and the financing of terrorism.

Concern about these crimes has increased in the past two or three decades, and privacy is increasingly being eroded by information-disclosure regimes aimed at preventing them.

The disclosure of information is becoming increasingly sophisticated and thorough. Governments—and potentially other entities—now have access to a significant volume of information about citizens. In addition to the incursions into privacy that these measures represent, there are risks of identity fraud or to the physical safety of HNWIs if information is stolen from the legitimate recipients by unauthorized users. At the same time, cyberattacks are increasing and bad actors are accessing information directly from and organizations.

Part two of this series will explore what we believe will be the future for transparency and privacy, and will suggest steps that HNWIs and family offices can take to reduce the risk of unauthorized dislosure.

Key contacts[1]

Henry Brandts-Giesen
Auckland
D +64 93 75 1109
henry.giesen@dentons.com

Linda Pfatteicher
San Francisco
D +1 415 267 4108
linda.pfatteicher@dentons.com

Daniel McLaughlin
Auckland
D +64 93 75 1131
daniel.mclaughlin@dentons.com

For more information on how Dentons works with family offices, please visit www.dentons.com/familyoffice

[1] With assistance from Jackson Tu'inukuafe, Solicitor, Dentons

ABOUT DENTONS

Across over 80 countries, Dentons helps you grow, protect, operate and finance your organization by providing uniquely global and deeply local legal solutions. Polycentric, purpose-driven and committed to inclusion, diversity, equity and sustainability, we focus on what matters most to you.

www.dentons.com

CSBrand-146565-DFO-whitepaper-Part 1-05 — 24/08/2024