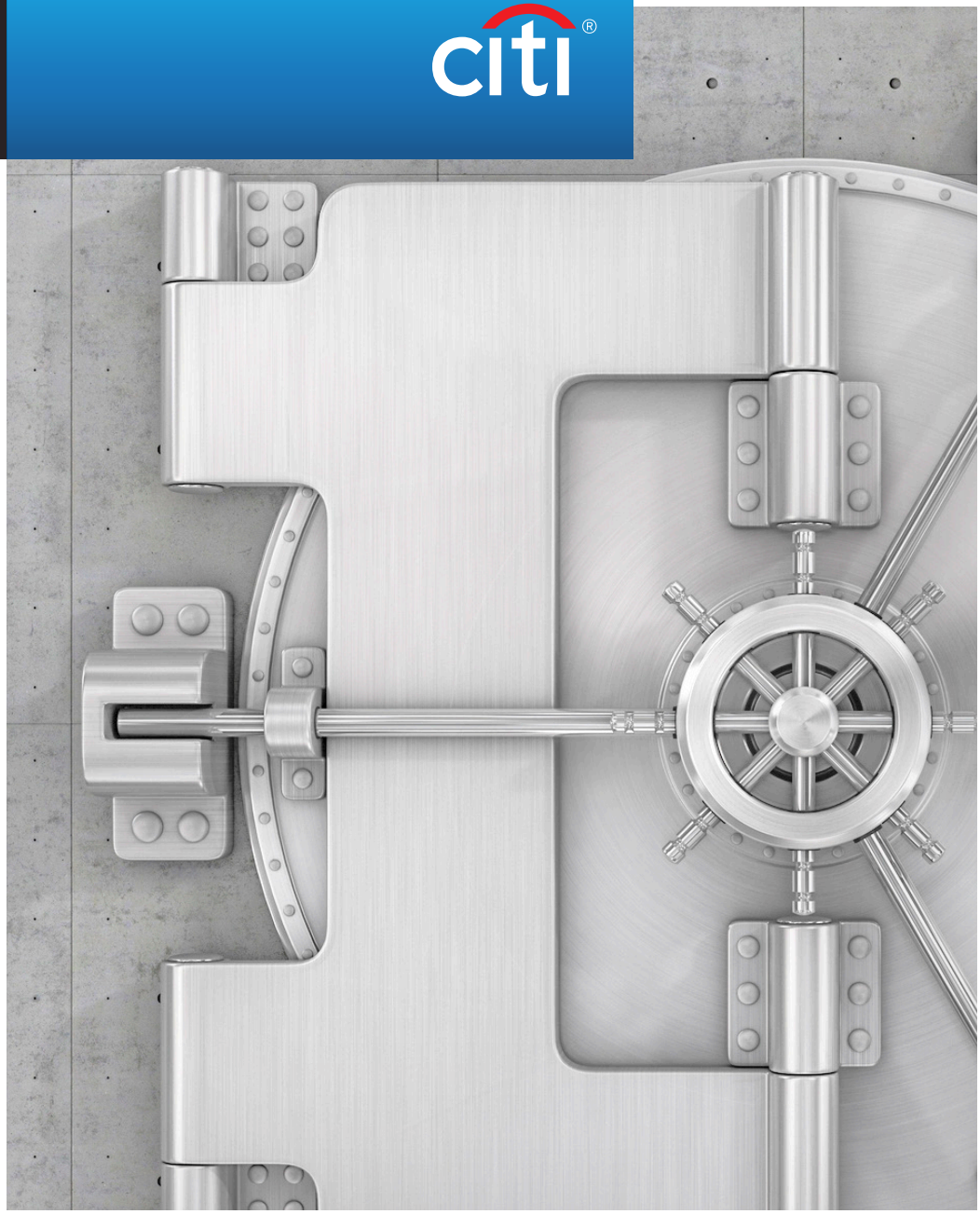
Private Bank

citi



Protecting the privacy of the world's wealthiest families

Citi Private Capital Group

Contents

Introduction

Family offices feel a strong sense of duty to protect the privacy of the ultra-high net worth families they serve. Regardless of whether family members are celebrities, high-profile business owners and executives, or famous philanthropists, there is an expectation that a family office will take effective measures to safeguard the privacy of a family's actions, assets, and personal affairs.

However, this has become a bigger challenge as we have moved towards an increasingly digital world. The information revolution has not only changed the way we view privacy; it also has fundamentally changed our expectations of it. Smartphones are now ubiquitous, with nearly everyone in the developed world not only owning one, but also relying on it for many of their day-to-day activities. With most people always carrying their smartphones with them, there is also an expectation we are 'available' at all times.

Furthermore, people's willingness to share their information - whether knowingly or unknowingly - is staggering. For example, emails, phone numbers, social networking activities, search engine histories, contacts, friend lists, photos, locations, and device usage are all 'shared' in one form or another with third parties who can keep this information forever. In a world where we are all crunched for time and people want effective results instantly, many share personal data to ease a process without fully realizing the consequences of their actions.

Moreover, today's digital world has a long memory and even well-crafted attempts to delete information can fail to achieve the desired effect.

Privacy breaches are often the prelude to reputational damage to wealthy families and their family offices. For example, leaked emails could have detrimental effects on the professional reputation of a family business by revealing confidential proposed business transactions or family information that should remain private.

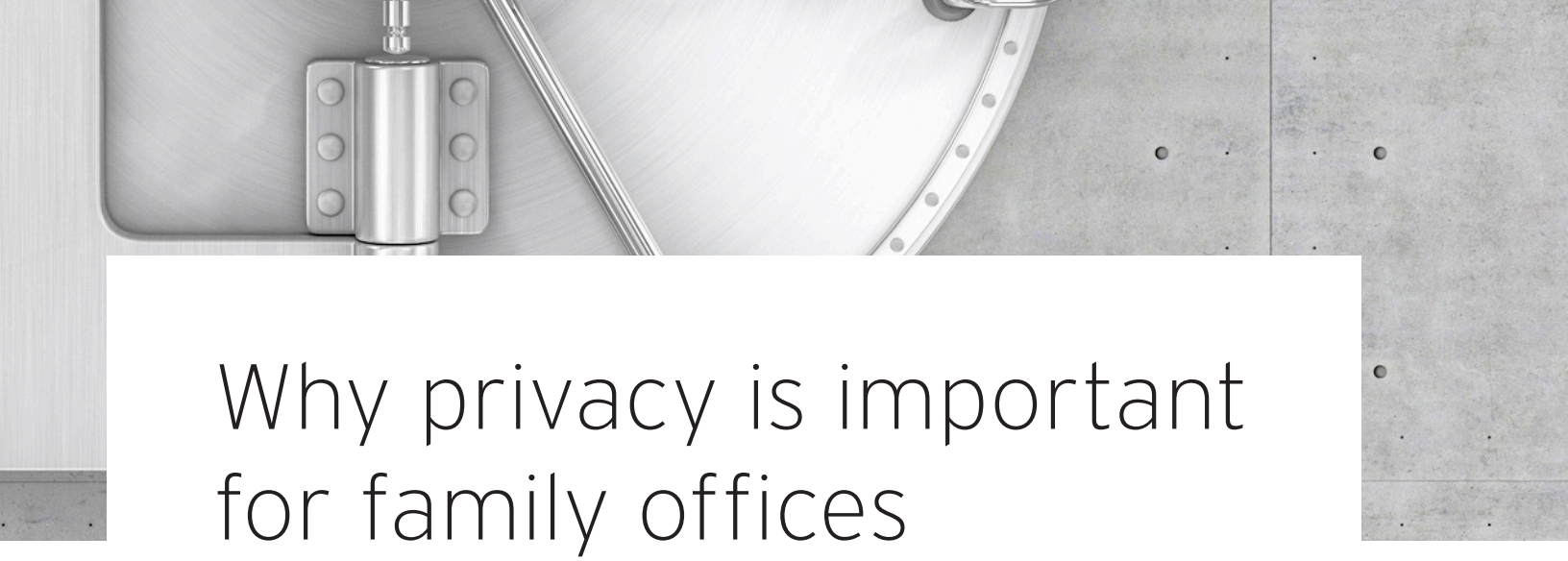
> "In a digitally-enabled world, wealth owners and international families have never found it harder to live their lives privately. Yes, the rules may have changed, but that just means your approach to privacy needs to stay one step ahead." [1]
>
> Magnus Boyd
> Partner, Schillings

Family offices face many challenges trying to achieve a myriad of goals set by their principals - investment returns, family harmony, philanthropy, perpetuating wealth across generations, wealth education, convenience - while maintaining a family's rightful desire for discretion and a private life.

Recent legislative, regulatory, and policy initiatives in various countries have attempted to establish norms in the name of privacy, however, a global standard remains elusive.

In this paper, we will look at the privacy threats that wealthy families and their family offices face and examine how family offices can look to identify, manage, and mitigate those dangers as part of a robust risk management program.

[1] A special thanks to Magnus Boyd of Schillings for his contributions to this paper. Schillings is an international law firm specializing in privacy and security consultancy. To assist their clients with these matters, they deploy teams comprised of intelligence experts, investigators, cyber specialists, risk consultants, lawyers and top people from the military, banking and government.



Why privacy is important for family offices

Privacy is a personal value that is unique to each individual. How much privacy a family needs should be an informed choice based on a discussion of each family member's expectations, the various family businesses and ventures, and the family's plans for the future.

There are several reasons why family offices should prioritize maintaining the privacy of the families they serve.

It does not matter if families have 'nothing to hide'

Family principals and their family offices tend to view privacy as a fundamental right intrinsically linked to personal autonomy and dignity that does not require any justification for protection.

There is an inherent link between privacy and reputation

Protecting reputation requires both a defense against falsehoods and the protection of private truths. Privacy enables people to manage how they are judged by others, including their professional contacts, friendships, and social circles. After all, if reputation can be simply described as what others think of you, then privacy is the extent of what they know about you. Family principals tend to seek places of privacy to withdraw to, free of public scrutiny. The preservation of privacy engenders trust which, in turn, promotes candor, interaction, and social cohesion between principals and their family offices.

The loss of privacy leads to a loss of freedom

The protection of privacy underpins freedom of expression which is vital to a free and democratic society. Many individuals would restrict what they share about themselves if they knew they were being surveilled and understood the volume of accessible information on them.

"The information you give to your phone is gathered to provide an incredibly intimate and personal picture of who you are and what you do to service providers so they can build products you want or even need. They know how old you are, how much money you have, who you talk to, what you like, what you don't like, who you don't like, where you live, where you travel, with whom you spend your time, who you are and who you hope to be. There are steps you can take to keep this information private."

Joel Wallenstrom
CEO, Wickr

Many families do have something they want to keep private

Everyone has something they would like to remain private and no-one should be made to feel self-conscious about it. While families might not harbor state secrets, they may well hold information that would cause shame or embarrassment if made public. Everyone has confidential knowledge that they may not want their friends or family to know, let alone business rivals. Furthermore, while families might not have something to hide now, they might in the future. Conversely, people should be able to change and grow without being shackled by their past. Privacy fosters the ability to reinvent, develop, and mature. Lastly, families should consider raising awareness on privacy by focusing on how it is a way to protect their children, rather than concentrating on the embarrassment that can occur from inadvertently sharing private information. Lessons on privacy management can help parents enable their children to live relatively 'normal' lives even if their parents and extended family live in the public eye.

Big data creates new privacy threats

In the era of 'big data', the vast amount of personal and business information that can be hacked and sold exposes wealthy families and their family offices to identity theft, fraud, and safety risks.

Once personal data is breached, there is an increased risk of a malicious actor attempting to log onto social media, banking, or corporate websites with these compromised credentials. This process could be automated and eventually result in unwanted texts, files, or pictures being shared.

Personal privacy planning is the only way to protect against such problems.

The dimensions of privacy

By making a few astute changes now, family offices can significantly reduce the possibility of a future privacy invasion and/or reputational damage.

Although modern society often focuses on digital privacy, there are actually five primary dimensions of privacy.

These dimensions are increasingly becoming more intertwined as our lives become more digitalized. Yet, each dimension requires dedicated attention and specific preventative measures to maintain privacy and safety, and manage reputations.

Family offices can play an important role by helping families address these issues with a three-step framework, which involves an audit, assessment, and action.

This framework allows family offices to incorporate both an individual family member and overall family privacy plan into their risk management strategy. Doing so can prove to be incredibly helpful and allow families to identify the inter-connectedness of their personal affairs and assets, and the levels of power and influence that many actors and detractors can hold over a family's privacy.

PHYSICAL
- PROPERTIES
- FACILITIES

FINANCIAL
- ASSETS
- LIABILITIES
- INVESTMENTS

COMMERCIAL

OPERATING COMPANY INTERESTS

DIGITAL
- ONLINE ASSETS
- DIGITAL ACTIVITY

SOCIAL
- FAMILY
- FRIENDS
- ASSOCIATES

Privacy by design. Physical security is the protection of personnel and data against events that could cause serious loss or damage to an individual, business, or organization, including fires, burglary, and vandalism. It is a necessary consideration when designing any building or facility.

In the same vein, family offices should embed privacy security into their organizational design and strategy. This ensures that a family office has privacy and reputation responsibilities built into its DNA, and therefore has aligned its staff and procedures to these critical objectives.

The first step of the 'privacy by design' method is an understanding of a family's current privacy levels – and what they mean to a family - through an audit.

"At a time when anyone with a smart phone can become a roving reporter and anyone with basic investigation skills can correlate digital records, many are simply conceding defeat in the battle for privacy. But it doesn't have to be this way because fundamentally every individual and family has a right to a private life."

Keith Schilling
Chairman and Senior Partner, Schillings

"Governments and corporations invest millions in intelligence, trying to understand a numberless and emboldened enemy when frequently what they really need to understand is themselves. The best place to start your own intelligence journey is close to home: yourself, your family, your company. What does the enemy see when they search social media and the internet for you? Cyberthreat actors go for the easiest target first."

Jacob Norwood
Cyber Intelligence Center Director, Citibank

The audit

Personal privacy planning should be proactive and preventative. Families should not wait for risks to materialize before acting. The best way to prevent privacy invasions is to anticipate where such breaches may come from.

This is easier said than done, but a privacy audit enables family offices to map a family's potential risk areas. By mapping every person, asset, and activity that is connected to a family, family offices can identify private information that could be made public, and the means through which it could happen.

Within reason, this audit should also be extended to cover a principal's children as they are more likely to post pictures and information on social media channels with little or no regard for the potential privacy and security implications.

Any such risk assessment is complicated by the difficulty of aggregating this information. In this digital age, we are constantly mindlessly sharing our information across social media, geotags, app records, and behavioral trackers. This makes collecting and analyzing all this information challenging.

The process of aggregation should not be limited to what is available online. Several missing pieces of a person's private jigsaw can be filled in by cross-referencing public records and databases. The simple act of aggregating the disparate pieces of a private jigsaw can produce a very detailed, invasive, and valuable picture for those wishing to attack or exploit a family member or family office executive.

As a consequence, the most valuable proactive step in personal privacy planning is auditing the available information from an aggregation exercise. Family offices should take action by investigating publicly available data on themselves and the families they serve before someone else - with malign intentions - does.

An audit allows family principals to identify where privacy 'leaks' exist and the inferences that can be drawn about a family's private life. Only when this comprehensive overview has been completed is it possible to start anticipating the associated risks.

Families consistently underestimate how much information about them is publicly available and the level of intrusion that is possible from aggregating and cross-referencing that information. Moreover, there is a lot of public or government data that they may not be able to find themselves (e.g. restricted to in-person viewing or low demand and not digitized). Therefore, audits require expertise and experience to ensure that an exhaustive records and open source search is conducted.

Regardless of what is found, it is only after an audit that a family office can start to make informed decisions based on facts rather than fear of the unknown. Mitigating fears can involve reassuringly simple solutions such as:

- Deactivating or updating old profiles on social media
- Unsubscribing from mailing lists
- Removing address details and other personal information from the public domain
- Tightening security on social media profiles

The assessment

The next step is an assessment to evaluate the likelihood of a family's privacy being breached. It is important to understand that likelihood is not static, but will ebb and flow according to a family's profile, levels of activity, acquisitions of companies and assets, circle of friends and family, business relationships, and competitors.

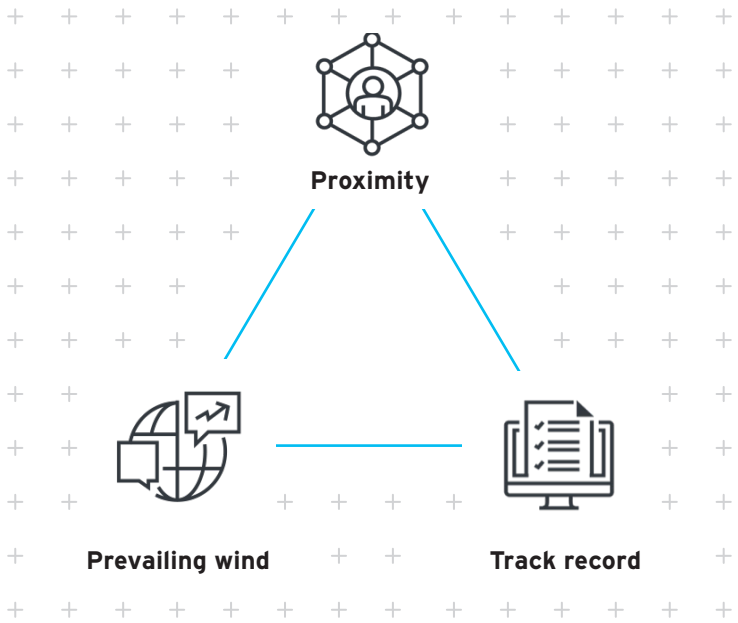
There are three principle considerations when evaluating a potential threat:

Proximity. How close is a family and its family office to the potential risk? For example, is it something that directly involves a particular family member – or is it something that relates to a third party?

Track record. What are the potential risks of a particular family member or family office employee involved in the threat given their track record/history? For example, previous nefarious or illegal activity

Prevailing wind. How sensitive is the threat topic and what is the general societal mood and wider context? For example, potential accusations of discrimination based on leaked emails

By establishing this assessment and updating it on a regular basis, family offices can make informed choices and identify where families may be vulnerable. This, in turn, will allow a more conscientious and less heavy-handed approach that may also be less intrusive and more cost-effective.



The action

The final step is to act on the results of the assessment. Mitigating privacy risks can often be achieved through simple measures, such as pre-emptive briefings with family office staff and the use of non-disclosure agreements.

Younger generations of a family will require information presented in an age-appropriate manner to ensure they can fully appreciate any required changes in behavior and follow through on recommended best practices.

Other privacy risks will require a much deeper set of interventions. The following are some examples of how and when to take action to protect and defend a family's privacy.

1. SPECIAL OCCASIONS

Social events such as weddings and birthday parties can represent a significant risk for privacy as guests can compound the risk of media intrusion.

Possible actions:

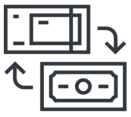
- Guest briefings
- Use of secure messaging platforms especially those with enterprise management capabilities
- Supplier risk assessments and non-disclosure agreements
- Location planning and preliminary surveying/research
- Decoy deployment
- Security perimeters and no-fly areas
- Image rights
- Social media monitoring and gatekeeping of all guests
- Anti-drone measures

2. PROPERTY

The purchase, sale, and renovation of property provide ample opportunities for the details of these assets to leak into the public domain.

Possible actions:

- Contracts in third party names
- Buy-out image rights
- Contractors under non-disclosure agreements
- Technical surveillance countermeasure (TSCM) analyses aka 'bug sweeps'
- Banning cell phones and all electronics from meeting rooms where sensitive information is discussed
- Staff training
- Take down of photos of the property from the internet
- Social media monitoring of staff



3. COMMERCIAL DEALS

There is always heightened interest in an individual when financial information about them is disclosed. While the purchase or sale of a venture, a tax investigation, or an offshore investment might raise eyebrows, the below actions can help lower the risk that shared information is used inappropriately.

Possible actions:

- Pre-emptive disclosure strategies
- Assessment of inner circle personnel
- Digital privacy checks
- Encryption of files and digital watermarking
- Vetting and due diligence
- TSCM analyses aka 'bug sweeps'
- Use of secure messaging platforms especially those with enterprise management capabilities
- Banning cell phones and all electronics from meeting rooms where sensitive information is discussed
- Information security assessments

4. PERSONAL ADVERSARIES

A relationship break-up could be the fuel for an estranged party to take 'revenge' and cause damage to their former partner.

Possible actions:

- Network analysis of the estranged party to understand their connections and ability to influence
- Serving of obligation agreements
- Contingency claims for misuse of private information
- Development of counter evidence
- Physical and digital security checks on schools
- Protection of children
- Family law advice: divorce and pre- and postnuptial
- Security detail briefings
- Secure communications

Practical privacy top tips

Family offices can consider and implement the practical tips below to protect principals, extended family members, and family office executives from often avoidable privacy intrusions and reputational damage.

Internet usage

Public Wi-Fi. Where possible, always avoid making online purchases when connected to a public Wi-Fi network as it is difficult to guarantee that the network is secure. This is the case even if a password is required - e.g. in hotels or restaurants. If mobile data usage permits, it is preferable to use mobile applications or tether a computer using a phone as a personal hot spot. When and where public Wi-Fi use is required, the use of a Virtual Private Network (VPN) is highly recommended in order to ensure data is encrypted and secure. That said, for VPNs to be effective, they must be set up properly.

Search engine suggested searches. Whenever terms are first entered into internet search engines, the website will usually suggest a series of more complete search options. These suggested searches – which constantly change and vary by location – are generated by these companies' proprietary algorithm 'learning' about search subjects based on previous searches. If using the internet to find media coverage of a sensitive or confidential issue, take care not to inadvertently teach the algorithm a negative search string about the subject (e.g. '[Company X] scandal') or revealing confidential information (e.g. '[Person X] owner [Property Y]'). A number of people searching a term, or set of terms, could inadvertently create a new but unwelcome suggested search. Family offices should also consider anonymization browsers and integrated service providers to protect their searches and online activities.

Data breaches and breach lists. Online platforms are hacked or otherwise compromised with increasing frequency resulting in data breaches. Some data breaches compromise extensive amounts of personal information including phone numbers, driver's license numbers, email addresses and passwords, financial information, and card payment data. An email address and password are the most commonly compromised pieces of personal data. It is for this reason that family offices should use unique passwords for different accounts and use password managers to aid in this effort. Moreover, to minimize connectivity between user IDs and specific individuals, family offices should consider using different user IDs for different sites - e.g. BaseballFan22 for Instagram and Slugger81 for online shopping sites. Family offices should also consider employing two factor authentication devices that can be tied to accounts and use manual keys to gain access to sites. Family offices might also want to use websites that allow users to check if their personal data has been compromised.

Online shopping

Privacy policies. Most online retailers require the user to click 'agree' or check a box to indicate that they have read and understand the company's privacy policy. It may not be possible to use the site without accepting this, however, it is helpful to be aware that some websites may share personal information with a third party, track personal data, and collect personally identifiable information. Some websites are more private than others in this regard, and there are several websites that provide helpful summaries of key conditions for some popular retailers so that family offices can avoid or use sparingly those that leverage personal data the most.

Amazon Wish List. Unless otherwise specified, Amazon Wish Lists are publicly searchable. The items on a Wish List may provide a journalist and other third parties with insights into personal interests, and other aspects of personal lives. Family offices should bear this in mind and alert family members about the risk of adding items to a Wish List. A safer option may be to add items to their 'basket' but 'save for later.'

Operating a website

When setting up a website – either for business or as part of an interest or hobby – individuals must provide their name and contact details to purchase and register the domain name. Unless specific security measures are taken, users should note that the ownership of the domain can be searched using domain name directories and that the search will reveal information including the name of the registrant, their address, and the date of registration.

Buying a property

It is a common misconception that owning a property through a company can provide an individual anonymity from the process. Journalists and other third parties are able to 'reverse search' public databases using a company name, though not the name of an individual. Therefore, if a principal or family office executive can be linked to the corporate entity in any way – including through media reports or other documents naming family lawyers or other advisors – principal ownership may be identifiable. If families own properties in multiple jurisdictions, family offices should be well versed in the country-specific laws on property ownership privacy as they vary greatly. It is likely that the transparency of property ownership will increase over time in most countries, therefore family offices should be prepared.

Unwanted photography and surveillance

Long-lens photography. Long-lens and covert photography have become an increasing threat of privacy for the wealthy or famous, especially as media interest of these individuals' private lives has intensified. Exercising caution where there is reason to suspect press intrusion is recommended, although the nature of technology means that family offices and principals may not be aware that the intrusion is taking place. If privacy has been violated by covert photography, a legal remedy may be available to remove the images or to seek to obtain the copyright for them depending on the jurisdiction in which this occurred.

Drone footage. As an extension of long-lens photography, drone videos and photographs are becoming increasingly popular. While a common sense approach is recommended - e.g. if surveilled by a drone, go indoors if possible - it is notable that governments worldwide are seeking to regulate drones more comprehensively. For example, in July 2017 the UK government announced that drones would need to be registered and that drone users would need to take safety awareness tests. Additionally, the UK government has collaborated with the Civil Aviation Authority (CAA) to develop a code of conduct for drones, which includes points such as staying below 400ft (120m), keeping an appropriate distance from people and private property, and staying away from aircraft, airports, and airfields.

Conclusion

Associate Justice of the US Supreme Court, William Orville Douglas wrote: "the right to be let alone is indeed the beginning of all freedom." There is an intrinsic link between freedom and privacy. Such lofty concepts can seem almost irrelevant when downloading an app to control your heating. However, it is important to understand these abstract concepts and their concrete consequences.

Rod Christie-Miller, Chief Executive and Partner of Schillings - a law firm specializing in privacy and security consultancy - believes that family office privacy planning is the key to securing the right for wealthy families to "lead a life on their terms - a life where they are in control of their affairs."

Everyone can remember being initially impressed when our electronic devices 'learned' from our usage and built knowledge of our preferences in music, books, and clothes. This is something we got used to and now largely accept and expect. We want our devices to refine and anticipate our choices - from exercise routes to passwords and payment details - without acknowledging the vast amount of personal data that is required for such customization.

Trying to comprehend and control the amount of personal information people share so readily can make family offices and the families they serve feel powerless.

Although cybersecurity awareness and preventative measures have increased, willingness to modify behavior patterns for digital safety has not grown in parallel. This privacy paradox leaves many family offices exposed.

The answers to privacy issues tend to be less complex than expected, and minor but meaningful tweaks in process and training can mean all the difference. Regular education of family members and family office personnel on prevalent privacy risks and preventative measures that individuals can make will go a long way.

Lots of seemingly insignificant actions – from strengthening privacy settings to monitoring image rights - are small steps that allow family offices to protect their principals' and the family's privacy in this information age.

Small steps to protecting privacy

- Strengthen privacy settings
- Utilize password managers
- Update/deactivate social media profiles
- Unsubscribe from mailing lists
- Remove details from public domain
- Monitor image rights
- Remove electronic devices from sensitive meetings
- Make shopping wishlists private

About Schillings

Schillings is an international law firm specializing in privacy and security consultancy focused on helping ultra-wealthy families, their businesses, and family offices around the world.

The firm employs a broad range of specialists including intelligence experts, investigators, cyber experts, risk consultants, lawyers, and senior people from the military, banking, and government to identify and stop potential privacy or security threats faced by their clients.

By working as a single team, Schillings believes it can solve problems quicker and more comprehensively than its rivals.

Founded in 1984 in London, Schillings has extensive experience working with family offices, on issues such as privacy threats, cyber-attacks, family conflict and divorce, data theft, and media intrusion.

Disclosures

Citi Private Bank is a business of Citigroup Inc. ("Citigroup"), which provides its clients access to a broad array of products and services available through bank and non-bank affiliates of Citigroup. Not all products and services are provided by all affiliates or are available at all locations. The views or opinions expressed herein in this white paper are those of the author and do not necessarily reflect the views of Citigroup Inc. or its affiliates.

This document is for informational purposes only. All opinions are subject to change without notice. Opinions expressed herein may differ from the opinions expressed by other businesses of Citigroup Inc., are not intended to be a forecast of future events or a guarantee of future results. Although information in this document has been obtained from sources believed to be reliable, Citigroup Inc. and its affiliates do not guarantee its accuracy or completeness and accept no liability for any direct or consequential losses arising from its use.

Citibank N.A., London Branch (registered branch number BR001018), Citigroup Centre, Canada Square, Canary Wharf, London, E14 5LB, is authorised and regulated by the Office of the Comptroller of the Currency (USA) and authorised by the Prudential Regulation Authority. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation Authority. Details about the extent of our regulation by the Prudential Regulation Authority are available from us on request. The contact number for Citibank N.A., London Branch is +44 (0)20 7508 8000.

Citibank Europe plc is regulated by the Central Bank of Ireland. It is authorised by the Central Bank of Ireland and by the Prudential Regulation Authority. It is subject to supervision by the Central Bank of Ireland, and subject to limited regulation by the Financial Conduct Authority and the Prudential Regulation Authority. Details about the extent of our authorisation and regulation by the Prudential Regulation Authority, and regulation by the Financial Conduct Authority are available from us on request. Citibank Europe plc, UK Branch is registered as a branch in the register of companies for England and Wales with registered branch number BR017844. Its registered address is Citigroup Centre, Canada Square, Canary Wharf, London E14 5LB. VAT No.: GB 429 6256 29. Citibank Europe plc is registered in Ireland with number 132781, with its registered office at 1 North Wall Quay, Dublin 1. Citibank Europe plc is regulated by the Central Bank of Ireland. Ultimately owned by Citigroup Inc., New York, USA.

In Jersey, this document is communicated by Citibank N.A., Jersey Branch which has its registered address at PO Box 104, 38 Esplanade, St Helier, Jersey JE4 8QB. Citibank N.A., Jersey Branch is regulated by the Jersey Financial Services Commission. Citibank N.A. Jersey Branch is a participant in the Jersey Bank Depositors Compensation Scheme. The Scheme offers protection for eligible deposits of up to £50,000. The maximum total amount of compensation is capped at £100,000,000 in any 5 year period. Full details of the Scheme and banking groups covered are available on the States of Jersey website www.gov.je/dcs, or on request.

In Canada, Citi Private Bank is a division of Citibank Canada, a Schedule II Canadian chartered bank. Certain investment products are made available through Citibank Canada Investment Funds Limited ("CCIFL"), a wholly owned subsidiary of Citibank Canada.

Citibank, N.A., Hong Kong/ Singapore organised under the laws of U.S.A. with limited liability. In Hong Kong, this document is issued by Citi Private Bank ("CPB") operating through Citibank N.A., Hong Kong branch, which is regulated by the Hong Kong Monetary Authority. Any questions in connection with the contents in this document should be directed to registered or licensed representatives of the aforementioned entity. To the extent this document is provided to clients who are booked and/or managed in Hong Kong: No other statement(s) in this document shall operate to remove, exclude or restrict any of your rights or obligations of Citibank under applicable laws and regulations. Citibank, N.A., Hong Kong Branch does not intend to rely on any provisions herein which are inconsistent with its obligations under the Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission, or which mis-describes the actual services to be provided to you.

In Singapore, this document is issued by CPB operating through Citibank N.A., Singapore branch, which is regulated by the Monetary Authority of Singapore. Any questions in connection with the contents in this document should be directed to registered or licensed representatives of the aforementioned entity.

Citigroup Inc. and its affiliates do not provide tax or legal advice. You should seek advice based on your particular circumstances from an independent tax advisor. To the extent that this material or any attachment concerns tax matters, it is not intended to be used and cannot be used by a taxpayer for the purpose of avoiding penalties that may be imposed by law.

Citibank, N.A. is incorporated in the United States of America and its principal regulators are the US Office of the Comptroller of Currency and Federal Reserve under US laws, which differ from Australian laws. Citibank, N.A. does not hold an Australian Financial Services Licence under the Corporations Act 2001 as it enjoys the benefit of an exemption under ASIC Class Order CO 03/1101 (remade as ASIC Corporations (Repeal and Transitional) Instrument 2016/396 and extended by ASIC Corporations (Amendment) Instrument 2018/807).

Private Banking for Global Citizens

Private Bank

citi