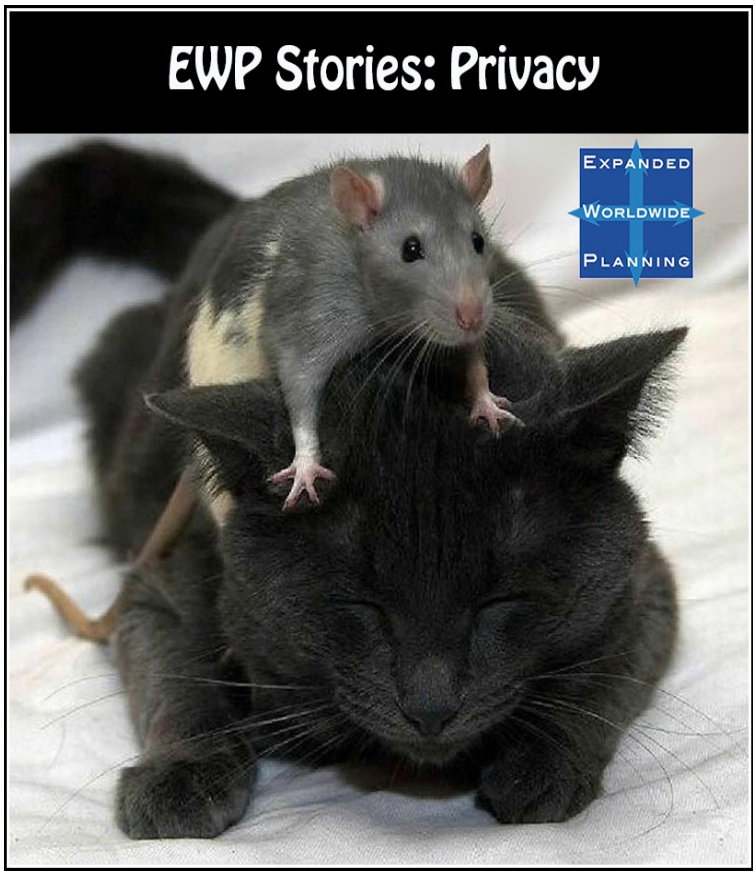
EWP Stories-1



Expanded Worldwide Planning
International Tax Planning

Stories

Part 1: Privacy

Privacy is a key element. Wealthy families are looking for ways to keep their affairs private, and still be compliant with tax authorities worldwide.

What was once private and personal becomes public and accessible to all. Computers and other electronic devices are part of our lives, whatever our opinion of them. These devices can add convenience and efficiency to our lives, but at a cost.

At ***EWP Financial*** we embrace the ***Privacy Principle*****.** The **Privacy Principle** is unique as it simply and legally shields wealthy families from unwished intrusions into their financial affairs. At the same time, the **Privacy Principle** is fully transparent and gives wealthy families a bespoke, compliant asset structure for all their holdings, wherever they might be throughout the world.

Electronic Privacy?

Andrew Grove, co-founder and former CEO of Intel Corporation, expressed the following thought:

> "Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age."

The ancient Greeks called man, "a political animal." In today's world almost all so-called facts are politicized. It is no different with privacy. Certain groups consider the journalistic authors of the **Panama Papers** and the **Paradise Papers** heros of a free press. Others say that these same journalists were thieves, who unlawfully stole private financial data. Whatever your opinion, these events did happen, and the targets were most decidedly wealthy families throughout the world.

How does the privacy afforded by a properly structured Private Placement Life Insurance (PPLI) policy protect the families whose financial information was published for the entire world to see?

The **Privacy Principle** of EWP accomplishes its objective in several key ways:

- Upon transfer into the PPLI policy, the insurance company becomes the beneficial owner of all the assets in the policy;
- If there is reporting to a tax authority for the asset structure, only one number is reported. This is the total cash value of all the assets in the PPLI policy. The individual assets are not reported;
- The bank account that is usually opened in connection with a PPLI policy is opened in the name of the insurance company, not the policyowner. The policyowner has full access to the funds in the bank account in accordance with the assets inside the policy.

Part 1

The hot, dry night air seemed to smother the sleek, six passenger Cessna Citation XLS jet. The plane had just touched down on the tarmac of this isolated runway. Next to the gleaming white jet was a gigantic windowless warehouse. The eerie, yellow lights that protruded from the warehouse turned the body of the private jet the color of an overripe mango fruit.

As he emerged from the plane, Carlos Gutierrez felt the skin on his face tighten from the baking heat of the desert. He walked briskly to the newly completed

warehouse and his cell phone rang.

He usually did not answer calls from unrecognized numbers, but he was expecting a call from his daughter, Lucinda.

“Hello,” he said. The voice on the other end was strangely familiar.

“Juan, is that you?”

“Yes.” said the now unmistakable voice of his best university friend. The voice was indeed Juan’s, but it had none of the joy and conviviality that he associated with it from university days.

“Carlos, we have your daughter, Lucinda.”

“What? I don’t understand. What do you mean?”

“Carlos, I now do the finances for one of the cartels that Lucinda wrote about in her article. We want ten million dollars for her release. We will not compromise. We want the money now. We will give you 48 hours to deliver it, and, if we don’t receive it, we will be forced to do other things to your beautiful daughter. I will call you in three hours.”

The line went dead.

The Privacy Paradox

In connection to privacy, there is a concept called the privacy paradox that was first discussed by Bedrick, Lerner, and Whitehead, ***The privacy paradox: Introduction, News Media and the Law****:*

> “The privacy paradox is a phenomenon in which online users state that they are concerned about their privacy but behave as if they were not. While this term was coined as early as 1998, it wasn't used in its current popular sense until the year 2000.”

The authors go onto to explain this in more detail:

> “Some researchers believe that decision making takes place on an irrational level, especially when it comes to mobile computing. Mobile applications are built up in a way that decision making is fast. Restricting one’s profile on social networks is the easiest way to protect against privacy threats and security intrusions. However, such protection measures are not easily accessible while downloading and installing apps.”

Louis Menand excellently expresses the same thought in his *New Yorker* article, "**Nowhere To Hide**," of June 18, 2018:

> "How many of us are going to take the time to scroll through the new policies and change our data settings, though? We sign up to get the service, but we don't give much thought to who might be storing our clicks or what they're doing with our personal information. It is weird, at first, when our devices seem to "know" where we live or how old we are or what books we like or which brand of toothpaste we use. Then we grow to expect this familiarity, and even to like it. It makes the online world seem customized for us, and it cuts down on the time we need to map the route home or order something new to read. The machine anticipates what we want."

Legal Challenges

There is also another type of privacy paradox pertinent to EWP in the reporting of data breaches and news reporting on wealthy families. This is aptly put by **Filippo Noseda**, partner at the Mischon de Reya law firm in London:

> "It is somewhat curious that serious newspapers who have been covering both the private banking scandals and the erosion of privacy seem unable to make the connection between data protection on the one hand, and the Common Reporting Standard (CRS) and beneficial ownership registers on the other."

CRS was initiated in 2014 by the Organization for Economic Co-operation and Development (OECD) with the goal of creating financial transparency between countries that have agreed to implement its directives. Beneficial ownership registers collate information about the beneficial owner of a financial entity in a registry for storage and use by enforcement agencies.

Mr. Noseda also draws our attention to published material by The European Data Protection Supervisor (EDPS) where he questions the OECD's goal of total financial transparency.

> Mr. Noseda writes: "As if they were living on planet Europa rather than in Europe, the European Parliament, the OECD, and politicians show complete disregard for the warnings raised by their own data protection bodies and instead appear hell-bent on introducing a system of total transparency."

In October 2020, a client of the law firm **Mishcon de Reya** filed a claim with the district court in Luxembourg challenging beneficial ownership registers, and alleges that the 'indiscriminate and generalized' publication of personal details of individuals connected to family enterprises breaches their fundamental rights to data protection and privacy, and exposes them to 'unnecessary and disproportionate' risks.

We have grown accustomed to the idea that transparency is a good thing, something that

supports the common good. Like many concepts, if taken to an extreme, it becomes its opposite—a weapon in the hands of governments hungry for wealthy citizens' tax dollars. **As proponents of EWP, we must question this overzealous approach to tax collection.**

Part 2

Carlos weaved to the door of the warehouse, followed closely by his pilot and co-pilot. Carlos fumbled with the key and finally opened the door to the office warehouse. His long-time pilot and co-pilot functioned also has confidants and body guards, so he told them in Spanish what just occurred.

Carlos was educated mostly in the United States, having received a masters degree in electrical engineering from Columbia University in New York, but English was his second language. Like all of us in times of emotional turmoil, he sought some comfort. Presently the only solace available was to speak his native language.

The plight of his daughter was beyond devastating, but the next step he knew was only a phone call away. He would call his insurance broker. Carlos had purchased Kidnap and Ransom insurance for his family, since the Mexican drug cartels had recently moved into his native Michoacan state, seeking to legitimize their sources of income by terrorizing the local avocado growers. By means of intimidation and violence, they sought access to this lucrative agricultural industry. His family were third generation avocado growers.

What put Carlos into emotional delirium was hearing the voice of Juan, his best friend at Columbia University. Juan had been a model student, an honor student like Carlos, and a kind and generous person. His involvement in his daughter's kidnapping seemed preposterous. He would not have believed it, if it weren't for hearing his voice.

Carlos was meticulous in his financial affairs. His company had the ability to assemble the most advanced and sophisticated electronic components. He had become a billionaire in his early 40s through his design of innovative electronics for medical devices. He abided by the law, both in Mexico and the U.S. Carlos was proud to be a citizen of both the U.S. and Mexico, even though it cost financially to do so.

The last time he had spent time with Juan was after college at the family farm outside the city of Uruapan. They had climbed onto one of the old avocado trees, and to drink beer together and eat avocados. They were looking forward to

launching their careers after college. He remembered the solid branches supporting them, the ripe avocados at their fingertips, with the dappled sunlight making the tree a private world of their own. He remembered the light being soft and multicolored like the light coming through stained glass in a church. They exuberantly discussed their prospects. Joining a drug cartel was definitely not on their list of future possibilities.

The Past Lacks Privacy

EWP and PPLI can further the aims of wealthy families seeking increased privacy, asset protection, and tax efficiency, but privacy, as we know it today, is a relatively recent phenomena.

We quote two eye-opening passages by Greg Ferenstein's "**The Birth and Death of Privacy: 3,000 Years of History**…," courtesy of *Medium:*

> "Privacy, as it is conventionally understood, is only 150 years old. Most humans living throughout history had little concept of privacy in their tiny communities. Sex, breastfeeding, and bathings were shamelessly performed in front of friends and families."
>
> "Privacy-conscious citizens did find more traction with what would become perhaps America's first privacy law, the 1710 Post Office Act, which banned sorting through the mail by postal employees."

This last quote seems quaint in light of the large-scale, present-day concerns of unauthorized data sharing by social media sites. The **Privacy Principle** was created to give wealthy families enhanced privacy. ***Our firm*** can be confident of our success, because EWP asset structuring greatly simplifies the process, and in addition, gives you the privacy that you seek.

The Dangerous Mouse Click

An adroit insider in the world of data breaches gives us frightening insights into how easily our personal data can be exposed and made public.

Lucia Vazquez,'s "**A Millionaire Hacker's Lessons for Corporate America**," for the *Wall Street Journal,* October 3, 2020 tells us:

> "Santiago Lopez started invading corporate computer systems at age 16, after he learned to hack from YouTube videos and like-minded friends.
>
> Now 21, he says he never wanted to commit crimes. Rather, he is a bounty hunter, invited by companies to find holes in their business networks and burrow into their vulnerable data. The idea is that a company will then fix what's wrong to harden itself against bad actors—"black-hat" hackers—

looking to steal data, conduct espionage and disrupt business operations. Like others in a stable of "white-hat" attack experts associated with bug-bounty firm HackerOne, Mr. Lopez gets paid commensurate with the severity of the weaknesses he identifies. He and other members swarm applications and websites to look for security holes missed by customers that contract with the San Francisco-based firm. Big problems pay big money."

In the same article, Ms. Vasquez asked these two important questions to Mr. Lopez:

"You're really effective at what you do. What does this say about corporate cybersecurity?

They're not investing money or time or work in trying to grow their cybersecurity team. A lot of companies, if you report bugs to them, they don't have the expertise to fix them. Software that they build themselves has more bugs but software generally is vulnerable, always. If software has access to important data, then encrypt it.

What kinds of technology changes are coming that will create cybersecurity problems?

Artificial intelligence has helped us a lot to optimize tasks, process data and make decisions much faster than a human being could. However, new technologies, including artificial intelligence, create big cybersecurity risks, as potential vulnerabilities are not fully understood when they are found. This means that with more organizations relying on machine learning to perform business-critical actions, AI systems are sure to become a major target for hackers."

Part 3

Diego wondered how he was to receive his bribe. He was told by his contact to buy a burner phone on Wednesday, and throw it away that evening after he received a text. His contact had booked him a table for 7pm at the Bellini Restaurant, atop the World Trade Center on the 45th floor in Mexico City.

"Good evening, sir," said the handsome young man in his well-tailored valet parking uniform.

His car door was politely closed, and Diego pulled away, feeling somewhat sheepish and out of place with his old Prius at this expensive restaurant in Mexico City. The Bellini was an uncomfortable experience for Diego. This

showed in the perspiration draining down his shirt from below his armpits. In his highly excited state, he had forgotten to put on deodorant this morning.

He had barely noticed the dazzling lights that lay below him, as he ate but did not taste the exquisite meal that was paid for by his contact. The restaurant magically revolved, but he might as well have been facing a blank wall. Diego only thought of one thing, and one thing only: “Will I get paid, or will they kill me instead.”

As he was traveling toward his small apartment, he received a text, *Look in the glove box, then destroy your phone. I mean destroy it completely.*

Diego opened the glove box to find a plain manilla envelope, which he tore open to find cash. Plenty of cash. 400,000 pesos, about $20,000U.S. The equivalent of his annual salary.

Why were 400,000 pesos put in his glove box? The reason was simple. Diego worked at the Servicio de Administración Tributaria (SAT). The SAT is the revenue service of the Mexican federal government. Diego had access to information that the cartel wanted to destroy Carlos Guittierez.

A new law had come into effect January 1, 2020, and stipulates that tax evasion will turn into a charge of organized crime if three or more people are aware of a scheme, which could result in companies being held criminally liable. Diego had access to salient information in Mexico’s Register of Beneficial Ownership. The cartel was going to use this information to charge Carlos under this new law.

How ironic that a successful businessman like Carlos could be discredited by an organized crime cartel when he went to great lengths to comply with all of Mexico’s laws. In a sinister way, the designs of Carlos’s intricate electronic components mirrored the devious, deceptive, and criminal practices of the cartel. One was used for good, and the other to destroy an innocent man.

Corporate Cybersecurity Amis

Large corporate data breaches have become almost commonplace in recent years. Here are a few courtesy of Dan Swinhoe from *CSO,* April 17, 2020:

Yahoo

Date: 2013-14

Impact: 3 billion user accounts

Details: Yahoo announced in September 2016 that in 2014 it had been the victim of what would be the biggest data breach in history. The attackers, which the company believed were "state-sponsored actors," compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. Yahoo claimed that most of the compromised passwords were hashed.

LinkedIn

Date: 2012 (and 2016)

Impact: 165 million user accounts

Details: As the major social network for business professionals, LinkedIn has become an attractive proposition for attackers looking to conduct social engineering attacks. However, it has also fallen victim to leaking user data in the past.

Equifax

Date: July 29, 2017

Impact: 147.9 million consumers

Details: Equifax, one of the largest credit bureaus in the US, said on Sept. 7, 2017 that an application vulnerability in one of their websites led to a data breach that exposed about 147.9 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May. The breach compromised the personal information (including Social Security numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed. That number was raised to 147.9 million in October 2017."

These large corporate data breaches might seem impersonal and far off, unless you were one of the victims. We finish this section with a more sinister example, that highlights the vulnerable interfaces of our technologically dependent world. This example is again from Mr. Menand's thoughtful *New Yorker* article quoted from earlier:

> "An Oregon couple's domestic conversation (about hardwood floors, they said) was recorded by Echo, Amazon's "smart speaker" for the home, which sent it as an audio file to one of the husband's employees. Amazon called the event "an extremely rare occurrence"—that is, not a systemic security issue."

Part 4

One week later Carlos Gutierrez found it difficult to pursue life in his usual diligent and focused manner. His daughter Lucinda had been returned by the cartel, unharmed physically, but shaken to the core psychologically. Carlos was now flying back from San Jose to one of his homes near La Jolla in southern

California.

He requested that they take a route directly south from Santa Barbara, over the Channel Islands, only veering west after San Clemente Island. It was the most common route when he flew commercially before he could afford to keep two jets. Carlos was attempting to re-establish some order in his life.

Before the kidnapping and the lawsuit, he and his family inhabited a sane and orderly world, cut off from the concerns of those outside this thin bubble. When it burst more illusions escaped than he had ever thought possible. He could repair things with money, but money alone could not repair his family's current emotional devastation.

One of his business strengths was the ability to inspire those who could put his creative electrical engineering concepts into integrated circuits and the other components of his medical devices. In San Jose he had visited a shop owned by Koreans, who were excellent to work with, and could manage his sometimes maddening deadlines.

Carlos was spared the emotional distress of having to speak with Juan again. The insurance company that wrote his Kidnap and Ransom insurance took over the successful negotiations with the cartel so that his daughter could be freed. He still could not fathom how his best friend of twenty years ago could now be working for one of the most vicious and notorious drug cartels in Mexico.

Although not currently a churchgoer, he was raised a Roman Catholic. He reflected on the forbidden fruit of the Garden of Eden. Just one week ago, they had lived in a similar paradise. But like Adam and Eve, they could now not return to this peaceful and predictable world.

The moist, soft, delicious avocado fruit was his last link to Juan. After all, the fruit that Eve ate was called the fruit of good and evil. How strange it turned out to be good for Carlos and evil for Juan.

His jet gently sloped down to the runway. He promised himself to protect the privacy of his affairs ever more vigilantly. Yes, the former bubble had burst, but he could construct a more solid one going forward. All he could be sure of was that Juan had taken his path in life, and he had taken another. Carlos's new path would have to include a new, creative design, presently unknown, but one he vowed to find. After all, that is how he had amassed his billions.

Conclusion

As we are learning, the danger of data collection by online companies is not that they will use it to try to sell you stuff. The danger is that that information can so easily fall into the hands of parties whose motives are much less benign. A government, for example.

EWP and ***PPLI*** are employed by our firm to not only give you enhanced privacy, we also keep you compliant with tax authorities worldwide. This is something that other asset structures can't accomplish. The **Privacy Principle** is integral to our successful asset structures.

EWP has the six principles that matter most to wealthy families throughout the world today—no matter where they are located. They are the building blocks of any successful asset structure.

If an EWP Structure Had Been Used….

Can an EWP Structure prevent kidnapping and extortion? While an EWP Structure can't prevent the nefarious deeds of organized crime, it can go a long way in securing the privacy that can prevent these acts of physical and emotional violence. Had Carlos Gutierrez had a properly executed EWP Structure, it is doubtful that his story would have unfolded in such a painful way. Since an insurance company becomes the beneficial owner of the assets in an EWP Structure, the reporting requirements to government agencies are very limited.

If the drug cartel wished to secure details about the private financial matters of the Gutierrez family, they would be hard pressed to find them. As it was, the details that they needed to kidnap Lucinda and begin their frivolous lawsuit were readily available to them using the Gutierrez's present asset structure. The precise, pin-point accuracy of the planning that led to the kidnapping of Lucinda would not have been possible with an EWP Structure in place. The information that the cartel used would simply have not been available to them.

Please ***Contact Us*** for any questions you may have.

by Michael Malloy, CLU TEP RFC.
CEO, Founder @***EWP Financial***