SEPTEMBER
2021

INFOSEC

Solutions for a Changing World

There is an old saying: "*It's not the big that eat the small; It's the fast that east the slow.*" This has proven especially true for security with social media in ministry. The threat today is not only stemming from sophisticated state actors, or even well-coordinated non-state actors like cyber hacking group terrorist organizations. The threat also comes from ideologically driven individuals who troll the internet for Christian mission endeavor and "out" that ministry to a state actor. These individuals are doing as much or more damage to mission endeavor than state actors.

KNOW THE THREAT

The reality is the digital threat landscape is always changing. Gospel workers in restricted access settings in particular need to understand this fact as they communicate what the Lord is doing through their ministries on the field back home with their churches, supporters, and stakeholders.

INFOSEC and A Quick History of Social Media

The reality is that gospel workers and their organizations need to stay connected with their constituents. From financial donors to prayer support, Gospel advance does not happen in a vacuum. and we have been charged by Jesus to place our lights on a lampstand for others to see (Matthew 5:16). That being said, a balance needs to be struck between Jesus' words in Matthew 5:15-16 and Matthew 10:16 where he warns His disciples to be "shrewd as serpents and innocent as doves." This is quite a balancing act for those called to the nations; especially those called to restricted access locations.

The practice of protecting information by mitigating information risk is nothing new. Information security, or INFOSEC, has been around for decades and is practiced by the public sector and private sector alike. The government is constantly trying to develop new and better ways to protect its information. From the personal information of its employees to critical military secrets, governments work hard to protect their information from theft. Likewise, private sector companies are constantly updating their techniques and technologies to protect proprietary information. The private sector pays top dollar for well trained managers and technicians who understand the quickly changing

For more than twenty I have been dealing with the challenges of INFOSEC for gospel workers in restricted access locations. From launching a website for my first nonprofit ministry in 1998 (a student discipleship and mobilization ministry which served exclusively in the 10/40 Window), to starting larger ministries that interfaced with denominational sending agencies, managing information security has been a challenge.

What information to place, or not place, on websites was challenging, but with the advent of social media sites like Myspace (2003), Flickr (2004), YouTube (2005), and Facebook and Twitter in (2006) the struggle became especially real as gospel workers began placing sensitive information online about their ministries. Then in 2010, with the advent of Go Fund Me, the ability to not only know where missionaries were working, but also how they raised their support became even easier to track as they connected multiple social media accounts like Facebook, Twitter, and Go Fund Me together. Now, a decade later, the need for INFOSEC with social media has become even more necessary and challenging. I hope this resource helps you in this endeavor!

CONCILIUM

Be Careful with Your Email Updates!

In 2008, a missionary couple who had served for more than a decade in a Muslim nation were arrested for the crime of sedition. The couple were tried, found guilty, and each served one year of hard labor for having the "intent to bring hatred or contempt against the president or the government." Along with the prison sentence, the couple both received a fine of nearly $9000 each and were required to pay before release from jail.

What led up to their arrest? The government received copies of their prayer and support emails that the government felt damaged the president's reputation.

During an interview, the missionaries stated: "We simply wrote emails asking friends and family at home to pray for individuals here."

When initially asked after their arrest how authorities discovered their emails, they stated:

"We assume the authorities must have been monitoring them. We didn't circulate them, only sent them to friends and family."

It was later learned that the couple were the victims of good intentions by one of their supporters who was forwarding their updates to others to "pray." One of those on the forwarding list was national with whom the missionaries had a falling out. That person forwarded the emails to the government.

Remember, the while the streets of Heaven are paved with gold, the road to Hell is paved with good intentions… Be your own gatekeeper and do not connect the dots!

The Security/Engagement Balancing Act

Make your engagement "personal enough to connect yet general enough to protect."

There is a real balancing act between INFOSEC and engaging with donors and stakeholders. Because the digital security landscape is always shifting, this is NEVER a static endeavor where one can rest on their laurels.

The key principle I would mention here is do not connect the dots of the *Vulnerability Pentagon*. When bad actors (both state and non-state actors) connect the dots, they can victimize you, your local partners, and get your ministry shut down or ejected from the country. Sadly, this has happened to far too many organizations in restricted access locations over the years.

The *Vulnerability Pentagon* is made of to two parts. The first part is the *Vulnerability Triangle* (in red), which deals with the issue of criminality and connecting the dots of Who, Where, and When. Bottom line, if bad actors can identify you, know your location, and when you will be there, they can target you for victimization. The dots are connected by both physical and electronic means, especially social media. From email prayer requests that get forwarded out of a secure circle, to paper itineraries that get printed and left lying around, it is very important to protect critical information from those who would that information against you.

The second part of the *Vulnerability Pentagon* involves the "What" and "How." Protecting the What and How is often most critical with state actors especially in restricted access areas as well as humanitarian environments. What you are doing and how you are doing it can be used to incriminate or exploit individuals and organizations.

So how do we avoid connecting the dots of the *Vulnerability Pentagon*? Practice this principle: Keep your engagement "*personal enough to connect, yet general enough to protect.*" Make your emails and posts personal by telling others about what God is doing in the lives of those you serve. Share of their hopes and their hurts, but DO NOT share ~~WHO~~ they are. Instead, use a pseudonym for that person with your audience.

Vulnerability Pentagon of Restricted Access

This includes sharing photographs of the person's face or head. Next, never share ~~WHERE~~ your ministry is located. Instead of sharing a city, province, or country name, share a regional geographic location such as "Middle East, North Africa, etc. This also includes **photos and videos** that could inadvertently identify where you are working. Be careful not to include popular geography, including panoramic shots of well-known buildings, cityscapes, or vehicles and their license plates that establish location.

Finally with the triangle, do not connect the ~~WHEN~~ of specific dates or times, either in the past or for the future. Instead, use terms like "recently," "last month," "the other day," etc. This also necessitates shutting off your phone or camera's location sharing that digitally embeds the date, time, AND LAT/LONG location of where the photo was taken. Lastly, be careful with the ~~WHAT~~ and ~~HOW~~ of the pentagon. While most of our organizations would never conceal the fact that they are overtly evangelical, connecting together ~~HOW~~ we are entering and staying in the country and ~~WHAT~~ we are doing (posting project specifics, and other information that could be used against the ministry) should be avoided.

DANGEROUS PHOTOS: UNDERSTANDING METADATA

It has been said, "If a picture is worth a thousand words, metadata is worth millions." So, what is photo metadata?

Simply put, photo metadata contains specific key information about a photo including (but not limited to): date the photo was taken, the camera owner, picture file name, photo content, location the photo was taken, etc.

To be clear, photo metadata is not a bad thing. Metadata helps to catalog, store, and locate an image among thousands of other images located on our phone, computer, peripheral, or stored in the cloud. Unfortunately, that data can also be used against us if we are not careful. Sadly, this has proven to be true for some gospel workers in restricted access locations.

Metadata is known by the technical term "Exchangeable Image File," or EXIF. EXIF metadata is embedded within a photograph taken by any digital camera, be it a small simple digital camera, a sophisticated SLR with telephoto lens, or even your smartphone.

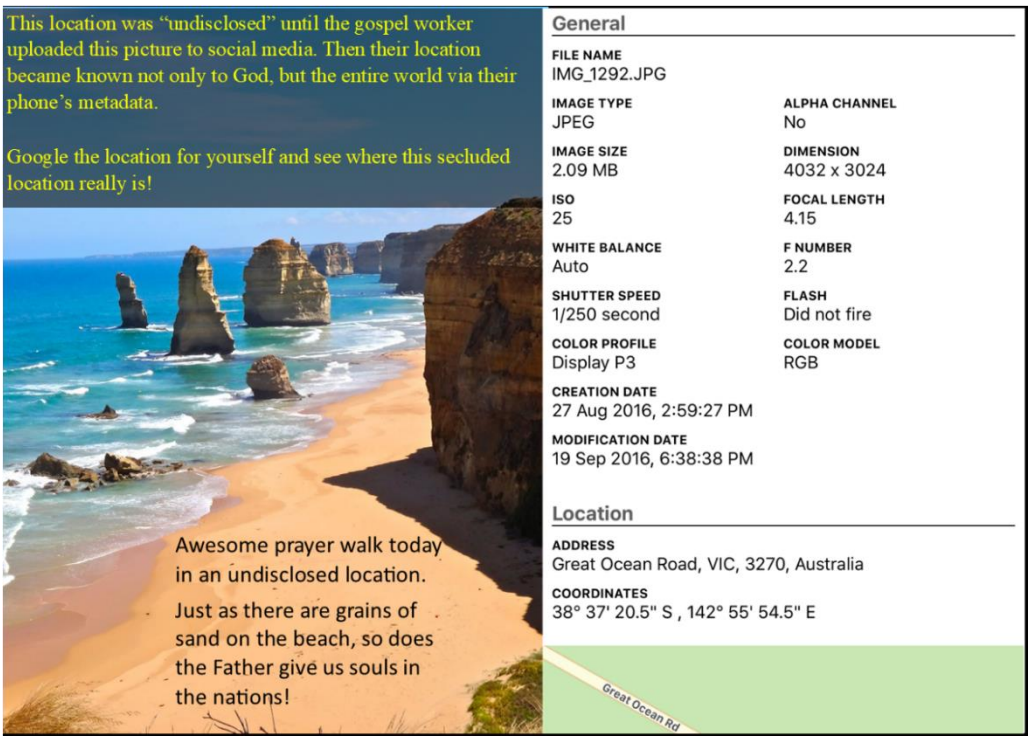
There is good news and bad news about metadata. First the bad news. The bad news is metadata cannot be shut off on a camera. It is necessary to identify, store, and catalog a photo in a folder. The good news is that you can limit the amount of information collected in metadata or delete compromising information later.

Here is how:

1. Start at the source. I always recommend that gospel workers turn off location sharing for photos on their smartphones, otherwise known as "geotagging." A simple Google search of "how to disable geotagging on iPhone, Samsung, LG, etc. will quickly yield results. While this will step will keep the location of your photos obscure. It will not obscure who took the photo.
2. Remove photo metadata via your laptop. Once you download a photo to your computer (laptop or desktop) you can go to the photo's properties and delete the name and date the photo was taken from the photo's metadata. Just google "Removing EXIF data from photos on Windows or Mac" for specifics. That said, you cannot necessarily delete geotags from photo metadata via your computer. So shut of geotagging on your camera or phone.

3. Use a dedicated EXIF editing program. There are several good EXIF editing programs on the market. Just Google and compare for an editing program that is best for you.

Remember, YOU are your own gatekeeper! That means you need you personally must take responsibility for the security of your personal and ministry information. To do otherwise not only places you at risk, but also your colleagues, family, and local partners. Be careful!



CONCILIUM

Final Thoughts On Photos and Engagement with Constituents

Pr@y and ask Father to give us more divine appointments in this amazing city. May Father's love be shown to all. Pr@y for Raj Agate who came to know Jesus and lives in a home beneath the trees on the right. May Father make Raj, his wife, and his three children Oaks of Righteousness!

In this prayer request example, the gospel worker connected the dots of WHO and WHERE. How exactly? By providing the name of the new believer, pointing out where he and his family live, AND using a very popular building/architecture in the photo. Apart from those who might know this building, the ability to place this photo into Google's photo search engine will quickly identify where Raj lives and the fact that he is a new believer in Jesus.

Here are some final unfortunate examples of photos that put Gospel workers and their local partners at risk. Remember: the biggest threat to information security is people who do not take security seriously.

As mentioned earlier, remember the *Vulnerability Pentagon of Restricted Access*, and avoid the mistakes made in these examples. This includes what we write and the photos we take. Never underestimate the enemy. He prowls around like a roaring lion looking for those he can devour. Therefore, be as shrewd as serpents yet gentle as doves as you glorify the Lord with your service in the Kingdom. Remember, security begins with YOU!

ABOUT SCOTT

Board and staff President, Scott Brawner, is Concilium's senior co-founder and provides direct leadership for Concilium Secure and Concilium Respond.

He accepted Jesus as his personal Savior in January of 1987 at the age of 16 and went on to serve with the US Army's First Ranger Battalion in Operation Desert Storm.

Scott was called to ministry on active duty and is a licensed and ordained pastor.

Scott has worked in mission sending and security endeavors for more than 20 years, including 7 years as Director of Risk Management for the International Mission Board, coordinating security for more than 5,000 Southern Baptist missionaries.

Scott has a BA in History and Masters Degree in Christian Education.

Scott lives in Missouri with his wife and three children.

CONCILIUM