JS|HELD

PERSPECTIVES

Reclaiming Your Privacy in the Digital Age

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

When you picture someone casing a house, a suspicious character in a white van parked down the street probably comes to mind. However, in today's increasingly online world, bad guys can also enjoy the perks of working from home, using social media to track their targets' movements, lifestyles, and habits. This was illustrated in a November 2018 *Los Angeles Times* report about a group of burglars who used celebrities' social media posts to determine when their homes would be empty.

In this article, we explain how these emerging digital threats can adversely affect personal privacy and detail some steps you can take to reduce online exposure and risk.

The Double-Edged Sword of Digitization

Love them or hate them, recent advancements in technology, online communication, and the way we access information pose a double-edged sword for personal security programs. While camera-enabled doorbells and real-time home monitoring products may deter porch pirates and allow for speedy responses in the event of an ongoing incident, the digitization of public records and exposure that comes from social media can present significant security challenges.

Publicly available property records, corporate registrations, and legal filings potentially allow anyone with an internet connection the ability to access information such as your address, date of birth, employer, and the identities of your family members. While this treasure trove of sensitive data has largely moved out of dusty filing cabinets and into cyberspace over the past two decades, it often remains hidden deep within antiquated county government websites that haven't been updated since the turn of the century. The information is there, but to the relief of many, it takes some amount of skill and know-how to access.

While the archaic nature of the public record provides a layer of protection from those who would seek to abuse our personal information, social media is a different story. More and more data is being shared across an increasingly large number of platforms, all of which were designed to facilitate the sharing of ideas and information with a mass audience. This information is being broadcast to a generation of digital natives who are skilled at piecing together bits of information from different corners of the web, potentially revealing much more than was originally intended.

Sensible Sharing or Excessive Exposure?

TikTok and Instagram Reels are full of videos posted by online "sleuths," gleefully describing how they determined where a photo was taken based on a road sign barely visible in the background or the corner of a partially obscured restaurant menu. X, the social media platform formerly known as Twitter, banned an account that used publicly available data to track the movements of owner Elon Musk's private plane. Illustrating the "Whack-a-Mole" nature of social media enforcement, the undeterred user simply re-started the account on Threads, the Twitter-clone recently introduced by Facebook parent company, Meta. While in some cases, the proliferation of this information may be born out of a desire for transparency rather than an intent to harm, it is all too easy to find examples of individuals who have been doxed or subjected to targeted harassment campaigns on platforms ranging from YouTube to Reddit, despite these actions being in violation of the platforms' rules.

With the rapid proliferation of social media websites and the ever-changing nature of the social media landscape, it can be difficult to know just how exposed you and your family are. Too often, we speak with clients who incorrectly assume that, because they are not on social media themselves, they have nothing to worry about. One of our primary goals is to help them understand that social networks are wide-reaching webs, consisting of family members, business associates, school friends, golfing buddies, and a myriad of other acquaintances. Like it or not, your social media presence is only as secure as the weakest strand in that web.

While more established social media platforms have taken steps to provide increased security and privacy options, if those options aren't utilized by everyone in your network, they aren't doing you much good. You may have taken great pains to lock down your profiles, but if your children and parents are constantly posting geotagged photos of you on their own profiles, your diligent privacy efforts are for naught. And this is all to say nothing of the upstart platforms where privacy settings are generally much looser, amounting to a Wild West of posting and sharing. We've seen the

cycle before: a new social media platform bursts onto the scene with little-to-no privacy protections, is pressured to institute tighter controls as increased popularity leads to increased scrutiny, only to be overtaken by a new upstart platform where anything goes. Lather, rinse, repeat. The question is not whether this cycle will continue, but who the upstarts will be and how we will adapt to the new challenges they pose.

An Ounce of Prevention is Worth a Pound of Cure

Ultimately, when it comes to protecting personal information, our message is simple: an ounce of prevention is worth a pound of cure. Executives and other high-profile or high-net-worth individuals need to understand where their data is exposed and how it can be accessed, while working with them to keep new information from ever making it online in the first place. Skilled consultants will pair preventative measures with step-by-step instructions on how the risks associated with existing exposure points can be mitigated.

Some of the steps that can be taken include:

- Following social media best practices, including regularly reviewing privacy settings to ensure proper usage;
- Deleting unused social media accounts to reduce exposure;
- Familiarizing oneself with personal data that is exposed in public records and taking steps to reduce the resharing of this information where possible.

CONCLUSION

In this digital age, where the websites people use to stay in touch with friends and business associates can be weaponized against them, even the laziest of criminals can find your home without ever leaving the comfort of theirs. Taking proactive steps to reduce and remove your data before an issue arises is key.

Acknowledgments

We would like to thank Michelle Willoughby and Ryan Murphy for providing insight and expertise that greatly assisted this research.

More About J.S. Held's Contributor

Michelle Willoughby is a Senior Managing Consultant in J.S. Held's Financial Investigations / Global Investigations Practice. She has experience in the United States and Canada leading and conducting complex due diligence, business intelligence, threat assessment, asset tracing, and litigation support projects. She has supported clients in a wide range of industries including the financial, pharmaceutical, media, technology, and legal sectors.

Michelle can be reached at michelle.willoughby@jsheld.com or +1 817 678 1940.