



## COMMITTEE REPORT: HIGH-NET-WORTH FAMILIES & FAMILY OFFICES

By David S. Ascher & Patricia M. Soldano

# The Next Frontier in Internet Security

Proactively managing risks to privacy, prestige and profession

**H**igh-net-worth (HNW) individuals are in the crosshairs of a new generation of risks created by the proliferation of the Internet and its ability to undermine an individual's reputation.

Just a few years ago, a secure Internet presence meant firewalls, anti-virus programs, encrypted passwords and being savvy enough to protect yourself from the occasional off-shore scam artist. Today, a secure Internet presence is defined by an individual's ability to influence what the web says about him, his family and his business relationships. HNW individuals disproportionately face online reputation challenges because they're high profile and easy targets. In many ways, they have the most to lose, as they're tasked with protecting a hard-fought family legacy.

HNW individuals have always been the subject of unwanted press coverage and media attention, but the stakes are much higher now that anyone can play the part of publisher, instantaneously and costlessly broadcasting to thousands of sites and millions of people whatever pseudo-information, outright lies or (worse still) true private facts he wishes and achieving an unprecedented level of information permanence. Newspaper stories used to come and go, accessible only in musky archives or on microfiche; not so with Internet content, which has the uncanny ability to proliferate and then remain forever accessible.

As the web is our primary source for due diligence on friends, employees, business partners and romantic

partners, every HNW individual will be affected by these trends. HNW individuals will be defined online by the unfortunate things that happen to them—when they're named in a lawsuit simply because they have deep pockets, forced to deal with a disgruntled employee or caught off guard by their children's indiscretions. And, unless they manage these risks and reshape how they're defined on the web, they'll feel the impact on their family's friendships, employment prospects, business transactions and personal lives.

Online reputation risk must be managed proactively, not reactively, as it's very difficult to "unring the bell" once damage has been done. The building blocks of proactive online reputation management are: 1) ongoing risk evaluation, 2) targeted campaigns to remedy problems as they arise, 3) a family contract on privacy management, and 4) a pre-defined crisis response plan that can guide a family when a true crisis hits.

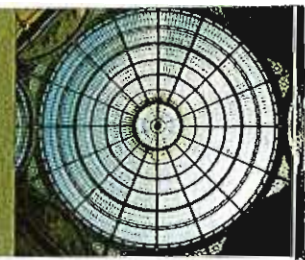
### Ongoing Risk Evaluation

HNW individuals and their families must contend with three categories of risk. We call them the three Ps: privacy, prestige and profession. Take a moment to evaluate your client's exposure to these risks on a scale of 1 (protected) to 10 (vulnerable) and see how he fares. As you do so, catalog the sources of vulnerability you find, so that you can evaluate which remedies (described later) are the most appropriate:

**Privacy risk.** Privacy risk entails the publication of information by others or by oneself that shouldn't be shared. There are several reasons HNW individuals wouldn't want such information online. Sometimes, HNW individuals just don't want anyone to know some details of their lives and activities for privacy's sake. For example, they may wish to keep their work and school

**David S. Ascher** is principal of ReputMinders, an online reputation management service. **Patricia M. Soldano** is chairman, Western Region, GenSpring Family Offices in Costa Mesa, Calif.





history, personal photos, sexual history or orientation, romantic relationships or political contributions, private. (Note that political contributions are public information by law, but this doesn't necessarily mean they have to appear at the top of the search engine listings.)

There's also information that, if acquired by the wrong person, could pose physical security risks for your client or his family members. This information includes your client's addresses, phone numbers, travel plans, school, exercise routines or children's photos—anything that could empower a stalker, kidnapper or thief. A HNW individual may sometimes provide this information unintentionally as a consequence of participating in social media sites with location-based features, such as Foursquare or Facebook Places. At other times, the information finds its way onto websites that share this information in the supposed interest of "transparency." Yet, the public's gain can often be the HNW individual's security risk.

Online access to other vital personal information—such as Social Security and driver's license numbers, place of birth or mother's maiden name—can make it easy for criminals to fraudulently access a person's bank accounts and wealth. It can also enable identity theft. Imagine your client trying to board an airline only to find that his driver's license has been flagged as a security risk or applying for a time-sensitive loan only to find out he has unexpectedly poor credit, because someone cobbled together enough information online to impersonate him financially. "Assessing Privacy Risk," p. 42, has questions to help your client determine what details of his life are on the Internet and may cause problems.

**Prestige risk.** The dissemination of information that poses a threat to a HNW individual's reputation can be hard to prevent and difficult to remedy. Even a public image that's been cultivated over the course of many years remains tremendously fragile online. One negative posting can be enough to undo a carefully crafted image and rapidly deplete public goodwill.

Information on the Internet that poses prestige risk can range from public comments on a news article to photographs that portray an individual or family engaged in activities that are incongruous with

their desired reputation. Common sources of prestige risk include mentions of gambling, substance abuse or sexual dalliances and, in particular, those that have been documented in some manner. Prestige risk often furnishes a family's legacy and, for business leaders, can even impact stock prices and the willingness of business partners to continue their relationship.

Particularly troublesome are legal actions or cases linked to an individual or his family members. Regardless of the outcome and/or veracity of the claim, legal claims

HNW individuals are often named parties in business-related lawsuits, because they have deep pockets and can be casually connected with an alleged wrongdoer.

are public record and are often widely distributed by news aggregators and posted on court and governmental websites, making them nearly impossible to expunge from the web.

Michelle Jordan, a reputation management expert who works with HNW individuals, notes that:

In today's society, wealthy individuals take on a sort of celebrity status. They may wish to keep a low profile, but it is increasingly difficult to escape scrutiny. And once something negative hits the Internet—even if totally unfounded—it can be very hard to reverse its impact.<sup>1</sup>

For example, one of Jordan's clients was wrongly accused of fraud and subject to a lawsuit. Though the suit was ultimately dismissed, the word "swindler" still shows up in search results because a local newspaper picked up the story. Not surprisingly, that paper hardly acknowledged the suit's eventual dismissal. "Assessing





## COMMITTEE REPORT: HIGH-NET-WORTH FAMILIES & FAMILY OFFICES

Prestige Risk,” this page, offers some questions to help your client determine how his online presence may affect his reputation.

**Professional risk.** Professional risk entails negative Internet content arising from business dealings or any other content that could negatively impact an individual’s career or career potential. HNW

HNW individuals make easy targets for disgruntled employees and business acquaintances, who turn to the web to air dirty laundry.

### Assessing Privacy Risk

*Your client should evaluate the information about him on the Internet*

Assess your client’s privacy risk by checking:

- Is there private information about your client’s religious affiliation or sexuality?
- Are there sources with pictures of or information about your client’s family?
- Does your client participate in location-based social networking?
- Can people identify your client’s business contacts?
- Is there demographic or identifying information available online, such as in court documents or real estate listings?
- Is your client’s name connected to political interests, such as public donor lists or attendance at a political event?

— David S. Ascher & Patricia M. Soldano

### Assessing Prestige Risk

*Ask your client questions about his online presence*

Assess your client’s prestige risk by checking:

- Are there non-professional pictures that are accessible to the public?
- Is there any legal content linked to your client’s name, Social Security number or driver’s license? (Legal content can range from parking tickets to criminal cases.)
- What’s your client’s personal brand and does his online presence enhance or detract from it?

— David S. Ascher & Patricia M. Soldano

individuals are often named parties in business-related lawsuits simply because they have deep pockets and can be casually connected with an alleged wrongdoer, not because of any actual involvement in wrongdoing. These individuals also make easy targets for disgruntled employees and business acquaintances, who turn to the web to air dirty laundry. In one recent case, an unhappy former employee not only skewered a firm’s managing director, but also his wife and teenage children.

Negative postings along these lines can severely impact an individual or his company’s ability to work. They erode existing business relationships and interfere with new customer acquisition. Consider, for example, a dentist who looked online after his practice slowed by 30 percent. He discovered that a single posting on a dentist review website, alleging that he used substandard tools and that his office lacked hygiene, was turning off customers. He was able to trace this posting to a disgruntled former customer who had received excellent service, but, ultimately, refused to pay numerous bills and who had turned to the web to vent her frustration. Unfortunately, this is an increasingly common scenario across a broad array of professions. “Assessing Professional Risk,” p. 44, includes questions to ask regarding how your client’s business or business activities are portrayed on the Internet.

### Remedying Problems

Family offices and HNW individuals should begin to





address the issue of Internet risk by taking an inventory of existing or likely threats to privacy, prestige and profession. Using the assessment criteria above, they can get a good idea of where the greatest risks lie for their particular situation. Once this foundational understanding has been developed, it's time to consider three possible remedies: removal requests, optimization campaigns and decoy campaigns.

It's often wise to engage a professional firm to advise on which of these approaches would be the most appropriate and effective to pursue, but here are the highlights of each:

**1. Ask for removal.** The simplest approach may prove the most effective. A HNW individual can ask a poster, website or Internet service provider (ISP) to remove private, untrue or inappropriate information. This may be a sound strategy when the poster of the unwanted content published it inadvertently or is a

Even those who currently don't have negative content to contend with should consider an optimization campaign to help shape their story online.

friend or colleague who simply used poor judgment in sharing the information. It's also a good approach when the posting is in direct violation of an ISP's policies and the identity of the concerned party requesting removal can be obfuscated by constructing a request that's in the interest of multiple parties.

However, a removal request can backfire if not framed properly. It may draw the ire of the original poster, who may respond by posting even more damaging content in reaction to a perceived attempt to censor or bully. If the removal request itself is posted online by the receiving party, as often occurs, it may also serve

### Assessing Professional Risk

*Help your client determine how his business is portrayed on the Internet*

Assess your client's professional risk by checking:

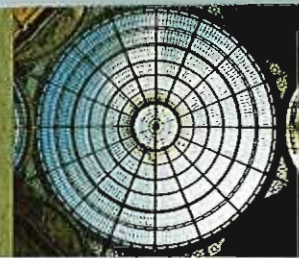
- Does any negative business content come up when searching your client's name or company name?
- Are there any mentions of your client's name or company name on unsanctioned websites, most commonly blogs, by current or former employees?
- Has your client's business been subject to any particularly negative events in the recent past?

— David S. Ascher & Patricia M. Soldano

to make the requesting party appear manipulative and overly concerned with his reputation. Online reputation management firms can serve as intermediaries to frame a removal request and to sidestep these pitfalls, yet, in most cases, we don't recommend this approach.

**2. Launch an optimization campaign.** Optimization campaigns aim to demote negative online content by promoting alternative content that presents a HNW individual or family in a positive light. The idea is to create new, positive content consistent with the desired story or brand positioning, post it on various websites that are designed to be picked up by search engines and enhance its position in search engine rankings through link building and other methods. The result is to make it easier for people who search for information about a HNW individual or his family to be presented with positive information, rather than the unwanted or negative content. Research has shown that the vast majority of web searchers don't look beyond the first three pages of search results.<sup>3</sup> Populating these first three pages with articles on business achievements and philanthropic works, for example, can serve to bury unflattering materials.

Individuals can impact their own online profiles by leveraging personal or business websites and social media profiles, but results will vary based on the



uniqueness of an individual's name and the amount of legacy content already online. For more complex cases, an online reputation management firm can help a HNW individual transform his online footprint and search engine listings.

Even individuals and families who currently don't have negative content to contend with should consider an optimization campaign to help shape their story online and to erect a defensive bulwark against negative postings that may arise in the future. Companies regularly seek to shape what the web says about them to protect their brands. Why shouldn't individuals do the same, especially those who may be forced to deal with unflattering content simply because of their wealth or family history?

**3. Manage a decoy campaign.** Decoy campaigns are a controversial but emerging trend in the online reputation management industry. They involve confusing the casual searcher by populating search engine results with competing and conflicting information to limit the impact of unwanted data that's reached the Internet. These campaigns may be appropriate when personal information such as Social Security numbers, home addresses or telephone numbers are exposed. Consider, for example, a high profile HNW individual with a unique home that receives extensive press coverage disclosing the address. One approach is to create a number of web articles and listings relating to the home that contain decoy addresses, so that a prospective kidnapper, thief or other bad actor would be hard pressed to know which address was real. While this approach may detract from the veracity and transparency of the Internet, it's, perhaps, a necessary evil for the sake of privacy and security.

#### Family Contract on Privacy

The remedies described above are largely reactive, applying primarily when a problem already exists. As a proactive measure, HNW individuals and their families should consider establishing a social contract that governs what family members may reveal online about themselves and the family. HNW individuals and their families are often their own worst enemies in creating unflattering content online, particularly through their use of social media sites like Facebook.

Some of the elements that should be specified in the contract as inappropriate for sharing online are: birth year and place, vacation plans, home address, confessionals, password clues, real-time location and risqué or compromising photos. Moreover, HNW individuals should be counseled away from jumping into social media because "everyone is doing it." A family's web presence is simultaneously an opportunity to bolster or undermine a family's image. Those who don't have a full understanding of how to control it should refrain from engaging in it.

If family members are going to engage in social media sharing, they need to know how to configure their settings on every social media website (Facebook, LinkedIn,

Each family should codify in advance how it will handle an online public relations crisis should one arise.

Twitter, Tumblr, Flickr, etc.), blog or web forum they participate in to mitigate risks to privacy, prestige and profession. For example, they should adjust Facebook settings to share photos, videos, posts and personal information with friends only and uncheck the box that makes their personal profiles searchable by online search engines. In certain circumstances, individuals should consider using avatars or pseudonyms instead of their real identities in building a social media profile.

"Framework of Activities," p. 46, details our suggestions for how to use social media, or whether to use it at all, based on individual or family desires for Internet exposure.

#### Crisis Response Plan

In addition to creating a social contract, each family should codify in advance how it will handle an online public relations crisis should one arise. Best practice is to create a crisis response plan that specifies:

- Who, if anyone, in the family will talk to the media





## Framework of Activities

*The best way to use social media*

<b>Desired Positioning</b> (How high profile does your client wish to be?)	<b>High</b>	<ul style="list-style-type: none"> <li>• Facebook</li> <li>• Twitter</li> <li>• LinkedIn</li> </ul>	<ul style="list-style-type: none"> <li>• Increase activity on social media sites and lower privacy settings</li> </ul>	<ul style="list-style-type: none"> <li>• Facebook</li> <li>• Twitter</li> <li>• LinkedIn</li> <li>• Continue on current path</li> </ul>
	<b>Medium</b>	<ul style="list-style-type: none"> <li>• Join relevant social networks for career, social life, etc.</li> </ul>	<ul style="list-style-type: none"> <li>• Continue on current path</li> </ul>	<ul style="list-style-type: none"> <li>• Stricter privacy settings</li> <li>• Do not use Twitter</li> </ul>
	<b>Low</b>	<ul style="list-style-type: none"> <li>• Do nothing</li> </ul>	<ul style="list-style-type: none"> <li>• Don't use social media</li> <li>• Facebook only with stringent privacy settings</li> </ul>	<ul style="list-style-type: none"> <li>• Don't use social media</li> <li>• Have stringent privacy settings for friends only</li> <li>• Use pseudonym</li> </ul>
		<b>Low</b>	<b>Medium</b>	<b>High</b>
<b>Current Positioning</b> (How high profile is your client today?)				

— David S. Ascher & Patricia M. Soldano

or engage the threat online and, if appropriate, what external party will advise the family or even release statements on its behalf;

- What will be the family's standard talking points; and
- Which online venues will be used to counter the threat to the family's reputation.

Every HNW family should have such a plan in place. It's the best way to ensure a quick response while avoiding additional strife at what may be an incredibly sensitive time for the family.

### Take Control

HNW individuals and their families have much at stake when it comes to online reputation, but many are blazing the trail by successfully addressing risks to privacy, prestige and profession. They have done this by using social contracts to manage their behaviors online, establishing crisis response plans that prepare them to

react quickly to reputational threats and posting and optimizing positive content consistent with their story and core identity.

Family offices and their advisors should begin by assessing and cataloging their clients' risk profiles and areas of vulnerability. Based on what they find, they can reach out to specialized advisors, who can help craft a strategy to address areas of vulnerability and manage family behaviors on the Internet.

The task of managing an online reputation for a high profile, HNW individual or family is daunting, but worthwhile. Proactive management of their online presence is the foundation upon which the family's legacy may rest for generations to come.

### Endnotes

1. Phone interview on June 11, 2012 between David S. Ascher and Michelle Jordan.
2. iProspect/Jupiter Research/NBP Study, 2009.