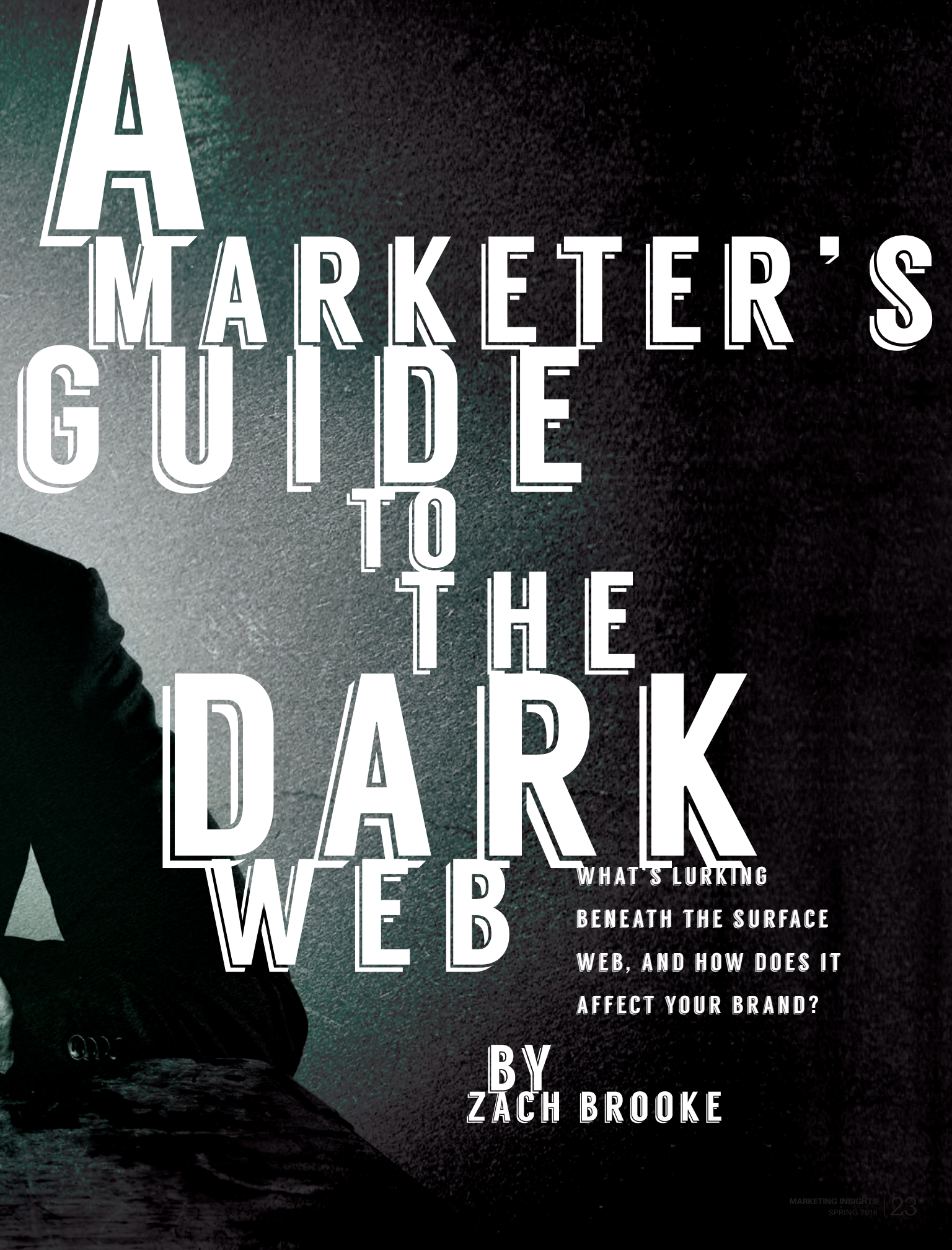

A MARKETER'S GUIDE TO THE DARK WEB

WHAT'S LURKING BENEATH THE SURFACE WEB, AND HOW DOES IT AFFECT YOUR BRAND?

BY ZACH BROOKE

THE DARK WEB. WHERE PRIVACY IS THE ULTIMATE PRIORITY. IS A MARKETER'S NIGHTMARE. AN OPAQUE OCEAN OF ROUTERS LINKING ROUTERS. FOR MARKETERS USED TO DEALING IN HARD DATA, THE DARK WEB PRESENTS A MONUMENTAL CHALLENGE: A NETWORK OF ANONYMOUS USERS WHO LEAVE ENTIRELY NO TRACE OF THEIR IDENTITIES, INTERESTS OR LOCATION. IN MANY RESPECTS, THE DARK WEB IS WHERE DATA GOES TO DIE. BUT IS IT DANGEROUS?

It's easy to think so. Headlines shout about digital drug bazaars like Silk Road and data dumps containing sensitive customer information, but the typical Dark Web experience is more vanilla than that, according to cybersecurity reporter Brian Krebs. While harnessing the Dark Web isn't a standard part of these brand conversations, that doesn't mean that marketers and researchers are off the hook. Who is writing the script about how the marketing industry approaches, talks about, learns from and uses the Dark Web?

"Plenty of would-be, legitimate consumers come from regions of the world where perhaps governments don't want their consumers visiting certain places or buying certain items. And for those consumers, [the Dark Web] can be a boon, and potential positive for retailers and marketers," Krebs writes in an e-mail.

Krebs goes on to say that much of the supposed danger posed by the Dark Web is nothing out of the ordinary when it comes to cybersecurity. "The darknet is a term—like many others before it—that gets bandied about by marketing people because it is a relatively new term that, for many, is filled with mystique. But there's really nothing special about the Dark Web, especially now that so many efforts are being made to index sites there."

Much of the confusion that comes from the Dark Web stems from its inaccessibility. If you could enter a Dark Web domain into an address bar of a commonly used browser it would be much less secretive. The terms are also confusing. Dark Web, dark net and darknet are interchangeable; Dark Web and Deep Web are not.

The Deep Web refers to any webpage that is not accessible through a search engine. The American Marketing Association homepage, for example, is easily found through a Google or Bing search, as are many of the links to other content pages. These are all part of the Surface Web or Clearnet (aka regular Internet). But, AMA members can also access their profile page and other gated content by entering their login information. Because none of these pages are accessible via a search engine, these pages are part of the Deep Web, as are all others that require keyed input to access.

Dark net websites, however, are inaccessible by standard search engines and browsers. To access the dark net, users need a special Web browser called Tor, short for The Onion Router. Tor masks where a user is originating by routing connectivity requests through multiple locations, like layers of an onion.

Developed by the Navy in the 1990s, Tor is now supported by a nonprofit called the Tor Project. The open source browser claims 2 million daily users. Tor users can still visit any surface website, such as AMA.org, but they can also access certain "hidden services." These are the websites that comprise the Dark Web, equipped with .onion domain suffix, many of which have become infamous. Yet despite their notoriety, the Tor Project estimates these sites make up only 1.5% of its total traffic.

These numbers underscore a fact often lost among dark net hype: While the Deep Web is several orders of magnitude larger than the searchable Web, the Dark Web is much, much smaller. According to *Wired*, the number of Tor "hidden services" sites is estimated to be between 7,000 and 30,000, or 0.03% of the normal Web.

Still, the Dark Web can pose a threat to some marketers. Just ask Ashley Madison.

On July 15, 2015, Ashley Madison, a dating service website targeting married men, was hacked. The hackers

sent owners AvidLife Media a moralizing message demanding the site be shut down immediately. When AvidLife refused, the hackers dumped stolen corporate data, including personal information about users, on the Dark Web. Fallout from the release prompted CEO Noel Biderman to step down later that month, and the company is now embroiled in a $576-million class action lawsuit.

Ashley Madison is just the latest prominent example of stolen corporate data turning up on the Dark Web. However, hacking sensitive information was still an issue prior to the emergence of the darknet, and would still be an online threat even if the Dark Web didn't exist. It just serves as a more desirable platform because of the anonymity.

"I've never considered the darknet to be much of a threat. Most of the crime forums and sites that I spend time on are on the regular Internet, but many also have darknet versions in case their normal URLs go down. I'm not aware of any unique threats that exist on the darknet that don't also exist on the regular Internet," Krebs says.

"From a fraud perspective, there are a lot of phishing sites and fraud activities happening at the Deep Web level [instead of the Dark Web]," adds Akino Chikada, senior product marketing manager at MarkMonitor.

There's even reason to believe the sinister uses of the dark net have already peaked. Law enforcement monitoring of the dark net is at an all-time high. Ross Ulbricht, founder of Silk Road and poster child of Dark Web, is currently in a federal prison appealing a life sentence for money laundering, computer hacking and conspiracy to traffic narcotics.

THE MAINSTREAM GOES DARK

Just as the more problematic dark net sites are exiting the scene, some prominent mainstream services are entering. In October 2014, Facebook announced it had added a Dark Web version of its social network in order to circumvent problems caused when Tor users accessed their accounts through Facebook's regular site. A spokesperson for Facebook said the company was still in the process of evaluating dark net metrics and is not ready to publicize them.

More recently, ProPublica made headlines when it announced in January that it would host a version of its news site on the dark net. Several reporters and news organizations already have a limited dark net presence—a smart move for organizations wanting to connect with whistle-blowers and political dissidents. But ProPublica's announcement that it would host a .onion site is a step beyond what everyone else has done.

Well, almost everyone. A few hours after ProPublica's Dark Web announcement on Jan. 6, Adland, an advertising news and curation site, announced it had launched its own hidden service site, as well. "Adland's target cares about privacy. We have two different types of readers. There are people who work in advertising, and then there are a lot of technical people like gamers who already have adblock installed," says Adland founder Åsk Wäppling, when explaining why she decided to set up a .onion version of her site.

In fact, Wäppling portrays the Surface Web as the more dangerous place to surf. "The way ad networks are today are basically indistinguishable from malware. There's a lot of third-party calls going on between the publication that you're reading and the [tracker] on the publication," she says.

Wäppling cares deeply about protecting her readers from malicious advertising and metadata collection. She notes that when Apple products made adblockers available, the number of Adland readers using those services skyrocketed 55%. Since tracking data via cookies or other metadata is hidden on the dark net, Wäppling sees the dark net as a turbocharged adblocker.

FOUR THINGS MARKETERS SHOULD KNOW ABOUT THE DARK WEB

1. Legitimate organizations such as Facebook, ProPublica and Adland are expanding into the Dark Web to reach users with privacy concerns.
2. Many of the fears marketers have about the Dark Web are mirrored in consumers' fear of data collection. Marketers should counter the appeal of the darknet by starting a dialogue about data collection and why it can be beneficial.
3. The Deep Web is not the Dark Web. If your company site requires keyed input to access certain pages, those pages are part of the Deep Web. To get to the Dark Web, you need a separate browser.
4. The majority of Dark Web browsing is not centered on illegal activity. "Hidden services" sites comprise only about 1.5% of traffic on the Dark Web, according to the Tor Project.

These sentiments were echoed by ProPublica news applications developer Mike Tigas, who said on a recent ProPublica podcast, "I think it's a public service to give your readers these kinds of choices. It's a very conscious decision that we have to make as an organization to decide that we want to do this. I think we all agree that letting our users choose what types of metadata they leave behind is positive for us."

Wäppling says the .onion version of Adland contains the same content that the Surface Web does, and that there are no extra costs to hosting a site on the Dark Web.

Adland is also in the unique position of being able to generate revenue off of the Dark Web. Having switched over from an advertising-based business model to one based on donations, Adland can receive contributions on the Dark Web using PayPal. The site also accepts Bitcoins, a virtual currency that is the most popular form of payment on hidden services sites.

Wäppling predicts that more organizations with particularly privacy-attuned users will join Adland and ProPublica in offering .onion versions their sites on the Dark Web. She also feels that she isn't giving anything up by encouraging anonymous traffic.

"I've never really collected data from my users anyway," she says. "That's the thing, if you're using somebody else's ad network, the data collected doesn't go to you as the site presenter, it goes to the ad network. So the data collected, which is infringing on my users' privacy, isn't giving me any knowledge …. But [a site's presenters] carry the weight of all the hatred when a malware banner ad disrupts their readers."

SALES AND THE DARK WEB

Soliciting Bitcoin donations is one thing, but is it possible to sell on the Dark Web? We know from stories about drug marketplaces that it is, but what about legitimate services? For three artists, the answer is yes.

Gabriella Hileman, May Waver and Violet Forest form cybertwee, a collective that explores ways of combining femininity and cuteness with technology in traditionally male-dominated spaces. Last year, they set up a Kickstarter to fund a Dark Web bake sale.

"We wanted to make the Dark Web more accessible to ourselves and others. We felt like it was made out to be this difficult and dangerous thing, but we thought it was a really valuable tool. We were really inspired by whistle-blowers, and wanted to make it easier to understand for others like us who may have felt alienated or intimidated by the process," Hileman writes in an e-mail.

Participants who donated to the Kickstarter were given instructions on how to access a .onion site set up for the bake sale. There, users would navigate to a form that allowed them to place their orders.

"We then sent them a unique Bitcoin wallet address to send the funds to. We kept track of who was sent which wallet address in a spreadsheet so we knew who had sent funds when we received them. Many participants used encryption when sending their sensitive information for added security," Hileman says.

The group raised just short of $300, which they donated to charity.

"We definitely didn't do it as a way to turn a large profit. For us, it was more about understanding how these tools worked and subverting the culture it is notorious for by offering a product that we had envisioned as the least threatening possible object." Hileman says.

While cybertwee is considering another fundraiser, Hileman says that she's not sure a Dark Web market exists for large scale commercial interests at this time. She, Waver and Forest all invested a tremendous amount of effort into walking users through accessing and ordering on a .onion site, and she's not sure it's worth it. Plus, she says, there is still a lot of anxiety over processing payments through the Dark Web.

But, she adds, "I feel like accessing the Dark Web is easy enough for almost anyone to learn. It just in-volves downloading a different browser …. I think as new, simpler interfaces develop, and they will, .onion sites using Bitcoin will become more viable marketplace for casual vendors. I think that in the past, the motivation around learning these skills had to do with evading prosecution. Now I think more people are interested in avoiding having their data mined."

THE VALUE OF CLEAR DATA COLLECTION

For most marketers, experiments like Adland's and cybertwee's are interesting to contemplate, but ultimately unrealistic. This makes the darknet a threat, but not in the traditional, hack-and-leak way. Rather, marketers' real vulnerability is the complete lack of a data trail the Dark Web offers to users increasingly jittery with the perceived pitfalls of data sharing.

Successful marketers, who are unable to utilize the dark web for their own ends, will negate the attraction the darknet has for tech-savvy but otherwise typical consumers by creating an open dialogue about data. Many of the fears marketers have about the Dark Web are mirrored in consumers' fear of data collection. Discussing in detail what information marketers collect and what value it provides to consumers addresses these fears head on. It may not convince the privacy die-hards, but it will go a long way in assuaging the fears of the typical Web consumer.

"THAT'S THE THING. IF YOU'RE USING SOMEBODY ELSE'S AD NETWORK. THE DATA COLLECTED DOESN'T GO TO YOU AS THE SITE PRESENTER. IT GOES TO THE AD NETWORK. SO THE DATA COLLECTED. WHICH IS INFRINGING ON MY USERS' PRIVACY. ISN'T GIVING ME ANY KNOWLEDGE."

- ÅSK WÄPPLING, FOUNDER OF ADLAND

Plus, data collection is not always a bogeyman for users, according to a study by global design and strategy firm frog. Writing in *Harvard Business Review*, frog executives Timothy Morey and Allison Schoop found that consumers are generally comfortable sharing data if they feel they are getting something useful in return. However, the utility threshold increases the as data collected becomes more personal and benefits grow less tangible.

"In other words, the value consumers place on their data rises as its sensitivity and breadth increase from basic information that is voluntarily shared to detailed information about the consumer that the firm derives through analytics, and as its uses go from principally benefiting the consumer (in the form of product improvements) to principally benefiting the firm (in the form of revenues from selling data)," they write.

Companies like Apple provide a useful template for conversations involving data collection. Following the high-profile hacks of celebrities' iPhoto accounts, Apple added a section to its website focusing on privacy. Morey and Schoop also explain that companies like Pandora offer a great example of the benefits consumers can gain by willingly participating in data exchange with advertisers. By imputing basic information about themselves, as well as providing feedback on music, they end up with a better user experience, while at the same time being exposed to relevant targeted advertisements in exchange for free use of the product.

Acknowledging consumers' nervousness with data collection, giving them some measure of control over the process and educating them about how data enhances user experiences all helps to ensure that the dark net remains a fringe experience, and may be the best way to establish the future of the Web is not darkness, but clarity. MI