

# BLF

## BIGGER LAW FIRM

A magazine for attorneys

### MESSAGING

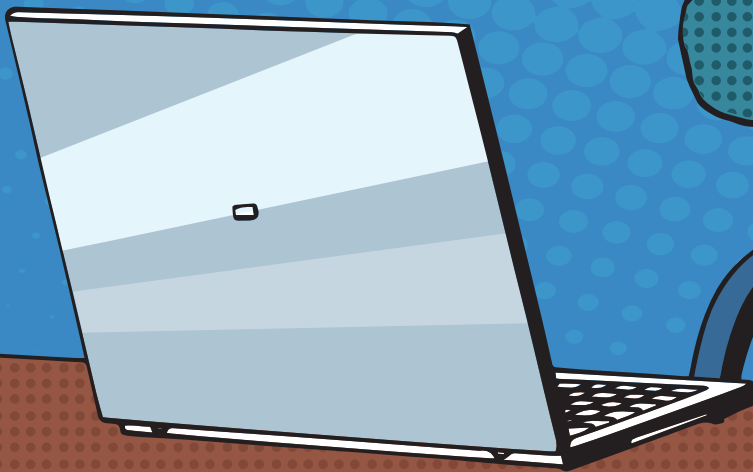
Neighborhood networking: how your firm can benefit from community involvement

### VIRTUAL IMPRESSION

Conversion tactics that improve the open and click-through rates of your emails

# IS ADVERTISING **BREAKING** — THE INTERNET —

?



*Poorly designed ads invade our privacy and clutter websites and apps, without any respect for user experience. Can a broken ad model be fixed?*



### LAW + TECH

The Supreme Court will decide how easy it will be for police to follow your phone

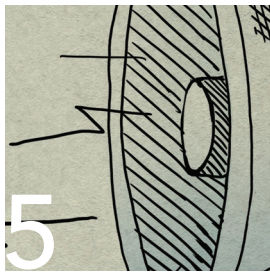




## Is advertising breaking the internet?

Online advertising is often criticized for failing to serve the needs of consumers. Articles, videos, banners and other ad content are designed to advance the objectives of the corporations that finance them, without respect for user experience.

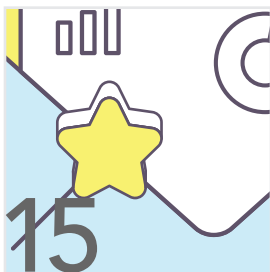
11



## POLICY

### Can we stop the spread of propaganda online?

As details continue to emerge about how foreign powers are using social media to manipulate voters, governments are beginning to try and fight back.



## VIRTUAL IMPRESSION

### Boost email conversion rates

Email marketing is a great way to build a relationship with your target audience. Ensure your emails do not get lost among the loud marketing messages and competitive subject lines bombarding recipients daily.

**SEO OBITER DICTA** 2  
Help stop Google Maps spam

**MESSAGING** 3  
How your firm can benefit from community involvement

**SECURITY** 8  
Make sure you are protected from the KRACK attack

**LAW + TECH** 17  
The Supreme Court will decide how easy it will be for police to follow your phone

**SEO IN DEPTH** 20  
Understanding featured snippets



*Bigger Law Firm™* was founded to introduce lawyers to new marketing and firm management ideas. Advancing technology is helping law firms cover more territory, expand with less overhead and advertise with smaller budgets. So many tools exist, but if attorneys are not aware of these resources, they cannot integrate them into their practice. The *Bigger Law Firm* magazine is written by experienced legal marketing professionals who work with lawyers every day. This publication is just one more way Custom Legal Marketing™ is helping attorneys Build a Bigger Law Firm™.

The *Bigger Law Firm™* magazine is part of the Adviatech™ family of companies and operates under Adviatech's legal marketing company, Custom Legal Marketing™. No part of this publication may be copied or reproduced. Converting any article in this magazine to digital format or sharing online is strictly prohibited. The content of this magazine, the magazine design, art, graphics and BLF logo are property of Adviatech Corp. All rights reserved.

To send mail to this publication, write to Adviatech Corp., BLF magazine, 4023 Kennett Pike Suite 57516 Wilmington, DE 19807, or email [editor@biggerlawfirm.com](mailto:editor@biggerlawfirm.com).

**Editor** Danuta Mazurek  
**Art Director** Kristen Friend

**Staff Contributors** Jason Bland, Ryan Conley, Hannah Felfe, Kristen Friend, Roxanne Minott, Dipal Parmar, Kerrie Spencer, Justin Torres

**Subscriptions** Thomas Johnson, [tjohnson@biggerlawfirm.com](mailto:tjohnson@biggerlawfirm.com)

**Founder** Jason Bland

**Website Offers** [www.biggerlawfirm.com](http://www.biggerlawfirm.com)  
**Single Issue** \$6.95

## I've Stopped Over 100 Google Maps Spammers. You Can Too.

I do not have special powers or privileged access to Google listings, just a commitment to ensure that spammers cannot rank higher than their honest competitors in local results.

If you have searched in your local market to see your ranking, you have probably come across a competitor stuffing keywords into its title and being rewarded for it. For example, in September, the top 3 local listings for a DUI lawyer in New York were:

### NYC DWI Lawyer - DWI / DUI Attorney - 24/7 on Broadway

### The New York DUI Experts on Park Ave

### New York DWI Attorneys on 3rd Ave

The problem with these listings is that the title of each business is not its legal name. Google's Guidelines for representing your business on Google<sup>1</sup> state, "Including unnecessary information in your business name is not permitted, and could result in your listing being suspended." The primary reason those three listings were at the top of the page was because they published "unnecessary information" in their business name.

This is more obvious in some states than others. In New York, the State Bar prohibits<sup>2</sup> the use of "trade names." Therefore, the "New York DWI Attorneys" could not be using their legal business name as that name runs afoul of local attorney advertising rules.

The listing titled "New York DUI Experts" gets two strikes against it. Rule 7.4 of the N.Y. Rules of Professional Conduct prohibits the use of words like "specialist" unless the attorney has completed a certification. In Opinion 1021, when responding to a request to use "expert" in a domain name, the New York State Bar Association's Committee on Professional Ethics declared that "expert" was a synonym for "specialist" and is equally prohibited without a board certification.

I had to do some digging to find out who the attorney was behind "New York DUI Experts." No attorney is listed on the website that links to that listing. But when I did locate him, I found no evidence that he was a Board Certified DWI Specialist, and therefore he could not use "expert" while complying with the N.Y. Rules of Professional Conduct.

Other states have different rules, which would allow someone to legally have a keyword heavy name like the Missouri firm

## ADDITIONAL READING

1) *Google Guidelines*: [blfmag.com/unnecessary-business-info](http://blfmag.com/unnecessary-business-info)

2) *New York State Bar rules*: [blfmag.com/NY-bar-expertise](http://blfmag.com/NY-bar-expertise)

3) *Tired of Law Firms Spamming Google Maps? You Can Fight Back*: [blfmag.com/google-maps-fight-back](http://blfmag.com/google-maps-fight-back)

that operates under Kansas City Accident Injury Attorneys, PC. But you do not need to be a connoisseur of lawyer advertising guidelines to know spam when you see it.

### Fighting Back

Keyword spam in Google Maps gives honest marketers a disadvantage. However, you can fight back. In September, I published an article<sup>3</sup> titled "Tired of Law Firms Spamming Google Maps? You Can Fight Back." Then, I sent the instructions to law firms I work with that are in heavily spammed markets and instructed all of my team members to follow those guidelines anytime they see spam anywhere in Google Maps. Whether we represent a law firm in that market or not, the spam has to stop. The procedure is simple:


- 1) Login to a Google account and do a search. Start with a keyword that relates to your city and practice area like "Phoenix car accident lawyer."
- 2) See a name that looks suspicious, like "Best Car Accident Lawyer in Phoenix – John Doe?" Click on its Maps listing.
- 3) Visit the website and find the legal firm name, usually located in the footer. Then return to the Google listing.
- 4) Right below the phone number in the Maps listing, you will see a link that says "Suggest an edit."
- 5) Click the edit icon next to the business name. Type in the correct name (an example from our fictional Phoenix firm may be "The Law Office of John Doe").
- 6) Click "Send," and you are done.

Your suggestion is reviewed by one of Google's quality control specialists. If they can confirm your change, it will be published. Sometimes, the change is not confirmed. If that happens, get your friends, staff and colleagues to join in and suggest edits. Eventually, a thorough quality controller at Google will do the right thing and verify the firm's correct business name.

If you are tired of being outranked by cheating competitors, Google's "suggest an edit" feature is a powerful tool for fighting back.

- Jason Bland





Community involvement is an overlooked tactic that can enhance your firm's marketing efforts while benefiting neighbors, strengthening bonds between co-workers and creating a positive image of your firm.

# Neighborhood networking

How law firms can benefit from community involvement

---

**T**o many firms, marketing is daunting, and understandably so. There are a lot of ways to spend marketing dollars. Some firms choose to engage in billboard promotion or create advertisements that air during popular television shows seen by thousands. Still others may choose to advertise on the radio.

These tactics can serve to introduce a firm to a community or to reinforce the existence of a firm in people's memories, if there is enough media saturation. However, if ads are not well coordinated, the audience may not get the right message. This can leave prospective clients with only vague thoughts of the firm: "Do I need this firm's services?"

---

Creating bonds through traditional advertising channels, while possible, can be expensive. What if there was a way to generate close connections with leads while making a positive impact on the community?

## Get your firm involved

An easy way to get involved quickly is to connect with an established organization. Yani Smith of Steinberg Law Firm is proud of Steinberg's Community Outreach Program, which supports the employees getting involved in the community. Members of the firm only need to commit a few hours a month to volunteering, an amount Smith says "is very doable." According to Smith, Steinberg Law Firm sponsors "a couple dozen local organizations each year that are equally dedicated to improving the lives of others."

Disaster relief is another impactful way to give back. People notice a firm that is willing to help those who are in need, whether through holding fundraiser events or offering pro bono services. Rob Nestico of Kisling, Nestico, and Redick (KNR) recalls his firm supporting hurricane relief this past fall. Nestico explains that watching firm members "step up and try to help communities that they've probably never even been to [gives him] a sense of pride in the people [he works] with." KNR also holds their own annual event called Coats & Cans for Kids Turkey Giveaway, and offers its offices as a drop-off location for Toys-for-Tots.



The options for getting involved first-hand are endless. There is never a bad time to start supporting your local community, whether it is to gain further leads or simply give back. Once you have started reaching out to provide your services to the community, the next step is to make sure your firm's actions are getting noticed.

### Use social media. Constantly

Once your firm has started getting directly involved in local organizations, you can begin promoting your involvement with a few simple steps. Where some firms attempt to publicize themselves through traditional media, your firm can gain a good name in the community while coming in direct contact with leads that are more likely to want your services.

Social media is one key to advertising your firm's name. Michael Liner of Liner Legal, LLC says, "when we sponsor events, we go all-in." Liner Legal posts on Facebook, includes events in its monthly newsletter and sends out weekly email blasts to spread the word. This leads more people to attend the event and strengthens the firm's public image on social media by increasing the amount of page likes and views.

### How real firms benefit

Liner tells his own firm's success story from a community-based standpoint, explaining that "the community approach to marketing has allowed us to easily reach our 'perfect client' without wasting our marketing message on people who don't want the product we sell." Liner found that giving back to the community with the help of his firm detracts from heavy monthly bills that he sees other firms paying to attract more leads. By direct interaction, the firm seems more human to potential clients, which establishes much-needed trust between the lead and the firm.

Steinberg's Yani Smith describes her firm's involvement as "a true testament for others, to see us practice our mission statement." According to Smith, the firm has "received more calls because people are moved by what SLF is doing in the community."

People notice what your firm does to make an impact. It moves them just as much as it moves volunteers to provide whatever help they can. Smith believes that volunteering adds a "higher sense of purpose" to workers' careers and lives.

### Look at the bigger picture

While there is a noticeable difference in community-based marketing compared to advertisements on television, Nestico keeps the true reason of giving back close to heart. He says, "we want our friends and neighbors to feel our presence, regardless of whether or not they ever need us for legal counsel."

Though earning a good name for your company is an obvious goal, it is important to remember that there is fundamentally no downside to volunteering. It strengthens the self, brings coworkers closer together and provides help to neighbors in need. As Smith puts it, "simply, the gift is in the giving."

### Now get started

It is important to not start with too many goals. The best approach is to set one objective and to give that your all, whether it is setting up a fundraising event or providing disaster relief. Liner explains that, "once you have found a way to monetize your efforts with one local organization, only then should you move on to opening doors with another."

Giving back allows you to be a positive example for your firm, strengthens your employees' enthusiasm and heightens neighborhood networking. Nestico points out that, "it doesn't matter if you can donate the most money, the most food, or the most toys, but if you can positively impact the community in any way at all then you should try."

Keep your firm's mission statement close to heart and acknowledge the personal meaning it has for you, remembering that the purpose of law practice is to protect the justice system and to give the best possible service to your clients. The results will have a positive impact on all fronts.

- Hannah Felfe



*Connect with an established organization or sponsor an event.*



*Organize a fundraiser for a cause that is close to your firm.*



*Raise money for disaster relief.*



*Get involved for the sake of making a positive impact.*



*Give in accordance with your firm's mission.*

# CAN WE STOP THE SPREAD OF PROPAGANDA ONLINE?



As details continue to emerge about how foreign powers use social media to manipulate voters, governments are trying to fight back. But whether governments can effectively regulate content on Facebook and Twitter is still an open question. In the United States, First Amendment law has not yet caught up to the challenges of quickly evolving technology. Can Congress come up with solutions that honor free speech and protect the integrity of elections?

The question of regulation is being raised again in light of Twitter's decision to ban all ads from Russian news agencies Sputnik and Russia Today (RT). Twitter co-founder and CEO Jack Dorsey explained, "This decision was based on the retrospective work we've been doing around the 2016 U.S. election and the U.S. intelligence community's conclusion that both RT and Sputnik attempted to interfere with the election on behalf of the Russian government."

As revelations have surfaced about the depth of foreign interference in the 2016 elections, U.S. lawmakers have introduced the Honest Ads Act, an attempt to govern political advertising on radio, television, in print and on social media platforms.

The Honest Ads Act has been touted as one of the strongest responses by Congress to address Russian meddling in campaigns. The act was introduced by Republican Senator John McCain and Democratic Senators Amy Klobuchar and Mark Warner, a former technology executive and vice chairman of the Senate Intelligence Committee.

The Act aims to expand currently existing election laws, which cover radio and television outlets, and apply them to paid digital and online social media ads. The law has not kept up with the growth of technology. Current U.S. laws ban foreigners from spending money to attempt to influence American elections, but these laws were not effective.

To remedy this, Congress would like to require social media platforms that receive at least 50 million monthly views to keep public files of all ads bought by anyone spending over \$500, and have these platforms make "all reasonable efforts" to ascertain that foreign entities and individuals are not purchasing political ads to influence the United States. Such regulations could prove difficult to enforce as foreign actors become more savvy. Those seeking to buy such subversive ads will not always pay in a foreign currency and will go to greater efforts to hide the fact that they are foreign buyers. The proposed legislation





was not met with industry enthusiasm, but lawmakers hope social media companies will ultimately decide to work with them.

#### **Will the proposed act pass?**

The biggest players in Silicon Valley claim to be in favor of transparency, but do not appear ready to support the proposed regulations. The fight could be a test of the tech giants' lobbying abilities in the face of public disapproval over their handling of the controversy so far.

It is also not clear how much support the Act could garner in Congress, or whether Republican leadership would agree to bring it to the floor. Given the political unrest in the White House, it is possible the Act could be derailed through lack of cooperation.

Google is examining what steps it can take to control the spread of fake stories. Google wishes to reduce foreign abuse and improve transparency, but must balance this effort against its goal of protecting users' privacy. Facebook, for its part, did give congressional investigators thousands of Russian-linked ads that ran during the 2016 election.

The debate begs the question: Does the right to privacy of a foreign or domestic user justify the real-world results of interference? How can users' privacy be protected while actions are monitored for subversive activity?

Increasingly, political discourse is moving into the largely lawless world of cyberspace. And without new regulations, tech companies like Facebook and Twitter are left to decide what they will allow on their platforms.

While it may be illegal for foreigners to financially influence elections in the United States, no real way exists of enforcing this law. Furthermore, the fact that private companies are assuming this role is troubling to some. It makes a few large corporations the arbiters of speech.

According to the American Civil Liberties Union (ACLU), "Once companies go down the path of engaging in censorship, line-drawing decisions are often impossible, inconsistent, capricious or downright silly." The slippery slope argument possibly overlooks the rapidly evolving world of technology systems that can be hacked and manipulated, a point emphasized by Higher Ground Labs and its co-founder Andrew McLaughlin.

"Tech companies have built systems that are so open to manipulation by bots and trolls and other techniques that they effectively reward propaganda. Failing to tackle that problem means ceding the terrain to fraudsters, fake-news pushers and other kinds of propagandists, who easily gain the upper hand," said McLaughlin.

**\$400**  
THOUSAND

Russian agencies spent nearly \$400,000 advertising on Twitter and Facebook throughout 2015 and 2016

**15-25**  
MILLION

With an ad budget of \$100,000 on Facebook, propagandists could reach between 15 and 25 million Americans.

**201**  
ACCOUNTS

Twitter has uncovered 201 accounts linked to Russian activity

**20**  
PERCENT

Just 20 percent of links with election-related hashtags shared on Twitter in 2016 came from a professional news sources. People in swing states saw the most disinformation.



### The real effects of fake news

Bombarding people with deceptive information can inflict damage on the public discourse necessary to democracy. Facebook's current ad policy bans some messaging, like using socially or politically controversial material for commercial benefit. It also introduced new guidelines for monetized content, which are designed to verify buyer authenticity, a step that may deflect bots and trolls.

### Extending existing regulations

Mandated disclosure of online political ad sources seems like a natural extension of the law, which already applies to radio and television ads. The Director of research at the Oxford Internet Institute, Philip Howard, believes it should be possible for Facebook to archive a copy of an election ad with each applicable state or the Federal Election Commission (FEC).

As simple as this idea may sound, it too comes with pitfalls. For instance, most of the Russian ads Americans saw were aimed at dividing the country, not supporting or endorsing any candidate. Any new regulation would need to set parameters that define the extent social media platforms are mandated to investigate the identities of ad buyers.

Regulating political ads is complicated, but Washington University law professor Neil Richards believes the effort is necessary. "The way these advertising models subject all of us and our attention to advertising, a kind of mental pollution, is unprecedented in human history," said Richards. "The decisions we make regarding the way that tech companies are a market for advertising affect, in a very real sense, what kind of digital democracy we are going to build."

The First Amendment only protects speech directed at the government. As private companies, Twitter and Facebook have complete discretion over what speech they allow on their platforms.



Tech companies have built systems that are so open to manipulation by bots and trolls and other techniques that they effectively reward propaganda. Failing to tackle that problem means ceding the terrain to fraudsters, fake-news pushers and other kinds of propagandists.

### When is speech political?

It is tricky, and some say dangerous, for the government to intervene and censor content on social media in any manner other than requiring companies to ban illegal activity. But does forcing companies to clearly display purchaser information on political ads rise to the level of censorship?

That so much political speech takes place on digital platforms adds another dimension to the issue. The Knight First Amendment Institute (KFAI) has sued President Trump, to force him to unblock citizens whom he has blocked on Twitter. The KFAI argues that Trump violated users' rights to free speech because they were blocked over disagreement with their messages. Free speech law calls suppression of such voices "viewpoint discrimination." In his capacity as a government official, KFAI argues, Trump unlawfully suppressed opposing viewpoints, even though the blocking occurred on a private platform.

The president's attorneys claim he blocked the users in his capacity as a private citizen, and that his actions do not constitute government activity. In areas where the mandate of the First Amendment does apply, like public forums, neither the government or government officials can exercise bias. The president's Twitter account is not a traditional public forum, like a park or town hall, but could be considered a virtual public forum, in which ideas should be freely exchanged. In this scenario, the @realDonaldTrump account should be bound by the same rigorous standards as a traditional public forum.

The KFAI argues the danger of treating the @realDonaldTrump account as private is that it will create an echo chamber in which only favorable comments about the president are heard. That would fly in the face of the intent of the First Amendment. Justice William J. Brennan Jr., said the essence of the First Amendment is that "the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials."

Several constitutional scholars do not view the KFAI's argument as valid because @realDonaldTrump is a personal account and therefore not bound by the First Amendment.

"There's no right to free speech on Twitter," says Noah Feldman of Harvard Law School. "The only rule is that Twitter Inc. gets to decide who speaks and listens — which is its right under the First Amendment. If Twitter wants to block Trump, it can. If Trump wants to block followers, he can."

The underlying issue is that Facebook and Twitter's susceptibility to foreign manipulation does not fit easily into precedent governing free speech or privacy. The law has not evolved to adequately address commentary that appears on social media accounts, or the dispute over what is a private account versus what constitutes a public forum. If Congress does not act, the courts will be left to try to apply outdated precedent to contemporary issues.

- Kerrie Spencer



# wifi security check-up

**Millions of older devices remain vulnerable to a major wireless flaw**

A 13 year old vulnerability in the widely used Wireless Protected Access II (WPA2) security protocol has left millions of wireless clients vulnerable to snooping. The vulnerability, which was revealed publicly in mid-October, allows thieves to stand between you and your router and intercept your digital communications. Even with vendors quickly releasing patches, some simple data security practices can help mitigate this and future headaches.

Information security is a never ending game of cat and mouse: every safeguard to protect 1s and 0s will eventually be beat, and new safeguards will be needed to replace those that have been hacked. As time goes on, technology becomes more secure, and flaws that manage to persist through the fixes become more valuable to hackers and more destructive to users.

Both proprietary and open source code is frequently taken apart and analyzed. When malicious actors discover a weakness, the knowledge usually makes it through a few hands before being exploited for profit. Once a vulnerability becomes known and the vendor issues a patch, the information is no longer as valuable. The public release starts the race to find unpatched victims.



The most recent Wi-Fi vulnerability has been dubbed the KRACK attack, short for Key Reinstallation Attack, and it affects any (unpatched) device connected to a Wi-Fi network.

### What is a KRACK?

When you connect any device to a secure Wi-Fi network, you must use an authenticator, or access point (AP), most commonly a router. In order to ensure a protected connection, your device (the client) and the authenticator (the router) send each other a series of messages that contain encryption keys and verification codes. This series of communications is the 4-way handshake.

## THE ATTACK EFFECTIVELY BREAKS THE 4-WAY HANDSHAKE OF THE WPA2 PROTOCOL, USED BY NEARLY EVERY WI-FI ENABLED DEVICE MANUFACTURED SINCE 2004. VENDORS HAVE BEEN NOTIFIED AND DEVICES ARE BEING SECURED AGAINST KRACKS.

During any secure connection, devices will perform the handshake and negotiate a new encryption key, which is used to protect all data during that connection. The handshake is essentially an agreement that transmissions are safe.

The vulnerability, which was discovered by Mathy Vanhoef, a network security and applied cryptographer, involves message three of the 4-way handshake. Vanhoef was finishing a paper on the OpenBSD Linux operating system, and was browsing code he has likely seen millions of times when he saw the flaw.

Sometimes, if a connection is unstable, one of the messages in the handshake may be dropped. In this case the AP (your router) will resend the third message because it has not gotten a confirmation from your device that it has received the key. Your device may receive message three multiple times, and each time it will install the same encryption key

and reset the incremental transmit packet number (nonce).

Vanhoef was reviewing the function that is called when your device processes message three of the 4-way handshake and installs the pairwise key (encryption code) to the driver.

“Staring at that line of code I thought, ‘Ha. I wonder what happens if that function is called twice.’ At the time I (correctly) guessed that calling it twice might reset the nonces associated to the key. And since message three can be retransmitted by the access point, in practice it might indeed be called twice,” writes Vanhoef.

Vanhoef had discovered that a hacker can force resets that sometimes occur naturally and establish new encryption keys that are known to the hacker. Essentially, the hacker sets up a dummy access point between you and your router and can interfere with any data transmissions. Your information is no longer encrypted.

### Proof of a long-available concept

In a proof of concept video of the attack, Vanhoef intercepts traffic by easily overpowering the signal between an Android client and the router, effectively breaking WPA2 encryption. Android and other Linux based operating systems are especially affected by this bug because it is possible to simply reset the key on these devices to all zeros. Once the actor is positioned between you and the internet, a number of things can happen from malware injection to the removing of HTTPS certificates that protect your communication.

This flaw does not show the password used to initially log into the network and requires someone with nefarious intentions to be in an optimal position, physically, between the client and the access point, which makes this an impractical attack to scale. Nevertheless, our phones and computers, updated or not, may use several different hotspots throughout the day and might be unlucky enough to be selected for snooping.

Thanks to the responsible disclosing by Vanhoef, many attacks can be prevented. Microsoft has already delivered a ninja update, Google released a patch for Android devices on November 7, and Apple included a fix in a late-October update. But older devices that no longer receive developer support, or systems that remain unpatched, will always be vulnerable. Both casual and professional users stand to benefit by catching up on the latest security measures.

### Encrypt everything in transit

As an end user, there is not a lot you need to do in order to stay safe when online. The Electronic Frontier Foundation has developed a simple browser plugin called HTTPS Everywhere, which helps you by automatically switching you to the secure version of a site. Secure Socket Layer or SSL certificates are easy to install. SSL certificates provide a secure and encrypted line of communication between a website and an internet browser. Any site without SSL should be browsed with discretion.

By funneling your online activities through a third-party, you ensure your communications are protected from snooping along every step of the way. Nearby key reinstallers, warrantless monitoring organizations, overzealous internet service providers and other digital eavesdroppers will only see an encrypted mess. It is highly recommended to add this additional layer of encryption, which encapsulates



all of your internet traffic, not just individual sites, using a virtual private network (VPN).

Several outfits have popped up in the VPN-as-a-service industry to empower small business and individuals to easily gain enhanced security. Private Internet Access is one of the more trusted providers, with strict customer-aligned privacy policies and over 30 clusters globally. Setting up an internal VPN server will require some moderate to advanced knowledge, depending on your set and size, but can be deployed quickly with a widely supported solution like OpenVPN.

### Update software and patch firmware

Our digital climate is as turbulent as ever, with attacks coming from foreign states, sophisticated crooks and bored neighbors. Unless you have explicit instructions to run older versions of programs or hardware, make sure your IT policy includes frequent updating. Updating the operating system and browser are always a top priority, but other software should receive the same level of attention.

Investigation into the Equifax data breaches revealed that an unpatched web server was the entry point for unveiling sensitive credit information on nearly 146 million Americans. Equifax has since patched the server, but our information is still out there. Anyone who has ever dealt with the American credit system should take steps to freeze their credit immediately to prevent that information from becoming ammunition.

Ninite is a tool that streamlines the process of installing updates to frequently used software such as web browsers, word processors and antivirus programs. Just visit the main page at [ninite.com](http://ninite.com), select which software to install, and a small executable will download. Run the program and the latest version of your selected software will be installed in the background. No need to hunt down downloads around the web or sit through endless prompts, Ninite makes it easy.

Software that is critical to the operation of electronic equipment like motherboards, smartwatches and TVs is called firmware.

Unfortunately, consumers are not always eager to update their firmware, which requires moderate technical knowhow and effort to track down and apply the latest updates. Even IT departments struggle with this decision, split between “if it isn’t broke don’t fix it” and “it’s fine until it’s not” philosophies.

### Audit passwords regularly

People have gotten really good at using bad passwords. The rise in two-factor authentication has helped reduce unauthorized access to our accounts, but has not helped us make better passwords in the first place. Arbitrary requirements like capitals, numbers and special characters can lead to overly complex passwords, which are forgotten almost immediately and can be trivial for computers to brute force. Even worse, passwords reused across services with varying degrees of security are like a series of dominoes lined up, just waiting for the first one to be toppled.

Password managers provide users with much needed security re-education. Utilities like LastPass (cloud based) and KeePass (locally managed) organize your login credentials and other sensitive information inside a vault. After installing the LastPass browser extension and creating a master passphrase, you can import your saved logins, see how secure your passwords are and replace weak ones.

Other features include a simple password generator, local encryption of your secrets to prevent unauthorized remote access and plans for teams that allow zero-knowledge sharing of passwords with co-workers.

The Identity Theft Resource Center tracked a record breaking 1,093 data breaches in 2016, up 40 percent from the previous year. The myth that hackers are just bored teenagers in their parents basement must be dispelled. In reality they are professionals in a global industry dedicated to stealing your information. Aggressive encryption, frequent updates and maximum strength passwords should be the bare minimum when using technology in any capacity.

- Justin Torres



## A LONG-STANDING VULNERABILITY

The code that makes a KRACK work was fully browsable on the online code repository, Github for almost a decade, but remained undetected by almost every major software and hardware manufacturer. “The fact is, open source has vulnerabilities,” says Greg Scott, an IT and security professional and author of Bullseye Breach, “just like its proprietary cousins.”

# IS ADVERTISING ***BREAKING*** — THE INTERNET —

Online advertising is often criticized for failing to serve the needs of consumers. Articles, videos, banners and other ad content are designed to advance the objectives of the corporations that finance them, without any respect for user experience.



Users have started to abandon videos due to pre-roll ads that are excessively long and uninteresting. Visitors attempt to turn off autoplaying video ads on one of several open desktop browser tabs. At times, large ads drop down from the top of the screen, and content desired by readers is pushed far down.

Programmatic ads, which are automatically placed by Google and others, are particularly junky and repetitive. However, publishers have little control over them. There are sites on which native ads, in which articles or videos written by advertisers are mixed with standard content, are too difficult to distinguish from editorial content. And the “around the web” features at the conclusion of articles frequently use much lower standards than the site itself.

## **A broken ad supported online model**

The view that the ad supported online model is broken is shared by Evan Williams, CEO of the journalism site Medium. He condemned the ad-driven model, laid off the company’s

traditional ad sales team and promised to find a better alternative. He said that ad-driven media on the internet does not serve people, and is not intended to do so. Instead, the media serves the companies that fund it. And they are evaluated on the basis of their ability to do just that.

Williams indicated there would be a new business for Medium, but did not reveal what it would be. It is believed that the company is considering a subscription system that would consist of individual blogs appearing on Medium’s platform, or groups of blogs. That is the usual alternative or complement to ads. However, it has its own issues.

## **Ad blockers and subscriptions**

Ad blocking software, which can cause legitimate content sites to lose revenue, is becoming more popular among internet users. Some blockers allow certain ads through, thus functioning as gatekeepers and generating income for the ad blocking providers while



preventing websites from earning revenue. Subscriptions have been effective for certain publications, like *The New York Times*. The *Times* describes itself as a subscription-first business. Its focus on subscribers differentiates it from many other media organizations, which attempt to maximize clicks and sell low-margin advertising.

However, depending on how stringent they are, subscriptions can make it difficult to share articles and retain a site's content in the conversation. For instance, in trying to share a *Times* article with someone, that person may be unable to read it if they are not a subscriber. Some subscribers have also found that certain publications, such as *The Times* and *The Boston Globe*, forget who their subscribers are, and attempt to deny them

access. And the majority of subscription sites still contain ads.

One resolution is for publishers and platforms to impose rigorous advertising standards policies similar to those that print newspapers did many years ago. Such policies may prompt ad agencies to be less intrusive in the placement of their ads.

#### **Ad blockers to combat poor advertising**

Ad blocking software has become increasingly prevalent in response to the plethora of poor online advertising. Many internet users have welcomed the advent of ad blockers, which prevent the appearance of pop-ups, and stop promos from playing before videos. Blockers also alleviate qualms about inadvertent clicking on a virus.

Poorly designed ads invade our privacy and clutter websites and apps, particularly on mobile devices and in the Facebook News Feed, where content is consumed with no requirement that the reader or viewer visit the originating site.



Owners of sites that rely on ads are concerned that ad blockers will reduce their revenue. This is quickly becoming one of the most important disputes with respect to the internet. A rising number of nations are implementing measures in an effort to decrease ad blocking. For instance, the EU's European Commission went so far as to recommend a regulation that would permit media companies to ban consumers who use ad blockers.

According to PageFair, a leading company that handles advertising recovery, as of 2015, 500 million devices throughout the world had an ad blocking plugin or used a browser that automatically blocked ads. As a result, websites and online services that depend on advertisements for their principal source of revenue, suffered billions of dollars of losses.

#### How do anti-ad-blockers work?

Initially, companies run analytics to enable websites to comprehend the amount of revenue that is being lost to ad-blockers. Secondly, companies provide their customers with tools that can request that users accept advertisements, give online users an option regarding which ads are to be removed, or permit website users to have an ad-free experience provided they pay a fee. This will depend on which anti-ad-blocking service is used.

Evading ad blockers has the potential to prove lucrative, particularly for struggling industries like free training sites and gaming sites. Dan Rua, CEO of Admiral, which designs software to reduce the effect of ad blockers, says that providing users with options and explaining the necessity for ads prevents consumers from feeling as though they have been caught unaware. Rua states that in order to view the entire problem, you must look at ways in which the internet is impacted by ad blockers.



According to an analysis by PageFair, the decision by Facebook last year to create tamper-proof ads that are unable to be removed by ad blockers, is predicted to result in an extra \$720 million this year in revenue from advertisements.

The issue is whether the internet can remain free for all to use. He goes on to say that nine out of 10 sites that people visit are free, and that is due to advertisements. Ad blocking poses a threat to the continuity of the internet, says Matthew Courtland, spokesman for PageFair. He says that if publishers are not earning revenue from the internet, then the quality of the content on the internet will gradually deteriorate.

However, companies that engage in ad blocking claim they are safeguarding the spirit of the open web by allowing users to retain control. Adblock Plus spokesman Ben Williams says that when companies compel consumers to view ads, they are suspending the spirit of the free internet.

PageFair claims that some users are unaware that ad blockers are already installed on their devices. Browsers, such as UC Browser, which is widely used in China, is purchased with ad-blocking software installed. And others install ad-blocking software immediately in order to safeguard their devices from malware.

Essentially, ad-blocking has become the new firewall or anti-virus. According to Ben Williams, partial ad-blocking,

which is AdblockPlus' principal model, is a more plausible way for companies to recover revenue without usurping power from internet users. He believes there are better ways to help publishers recoup lost revenue, saying, "You can work with blocking companies" to display ads that users have approved. Working directly with consumers in this way is a more feasible means of resolving the issue of online advertising.

#### How ad tech is harming the web

There was a time when individuals who visited the same web page simultaneously using the same web browser would view the same thing. Currently, however, scripts, cookies, auctions use personal information to show brand messages and sales pitches designed especially for the user. This raises privacy issues. For instance, almost immediately after you view a website online, ads for that site begin to follow you on each website you visit subsequently. Such an invasion of privacy can persist for weeks.

In this way, your bandwidth is being used to display content you neither requested nor desired. As a result, your user experience is corrupted. In response to privacy concerns, Apple revealed a new iPhone operating system

that facilitates content blocking. An additional benefit is that it offers better performance on iPhones, and for those who have installed the correct plugins.

Ads' consumption of bandwidth is likely to increase unremittingly regardless of whether bandwidth itself increases sufficiently rapidly to meet that need. For example, several web publishers have begun to compel their viewers to sit through a video not only prior to watching video content, but even prior to reading a text story.

As mobile device use increases, it is likely that mobile ads will become more irritating over time. The shift to more privacy safeguards may aid in reducing the speed with which such technologies are adopted. But it is doubtful whether websites will show signs of improvement. If you wish to avoid having an unpleasant experience on the mobile web, you will have to begin reading your articles natively, in the Facebook or Apple News app.

### **The effect of advertising**

A major problem plaguing the web is the fact that network effects have a tendency to build online monopolies. While ad-blocking reflects consumers' increasing objection to an industry that has shown little regard for users' needs and desires, the ad industry has become reliant on two of the most influential companies on the web, namely, Google and Facebook. It is estimated that their combined percentage of online ad budgets ranges from a little under 60 percent to 75 percent. However, a monopoly, albeit a shared one, is not good for price competition, transparency or innovation.

According to Joe McCambley, who helped create the banner ad in 1994, brands are successful on the web because they ask "How can I help you?" rather than "What can I sell you?" He says, "Most advertisers and

their agencies do not know how to be helpful." He writes that once the web grew sufficiently large to capture the attention of big advertisers, it marked the end of the web's mission to provide beneficial or valuable information. Not long afterwards, the reach and frequency of large agencies were ruining content and utility.

However, it is arguable whether ads universally function well on the web. If they did, the ad blocker would not have been created. Nevertheless, with

will accomplish this goal via an ad marketplace, which will permit blogs and other website operators to choose acceptable ads and put them on their pages. If a consumer uses Adblock Plus, and visits the page, they will see those acceptable ads rather than whatever ads the site would usually run.

While the program is intended to be nice to publishers by allowing them to show some ads instead of none, publishers are not entirely pleased. In all likelihood, acceptable ads are less

**While ad-blocking reflects consumers' increasing objection to an industry that has shown little regard for their needs and desires, the ad industry has become reliant on two of the most influential companies on the web, namely, Google and Facebook. It is estimated that their combined percentage of online ad budgets ranges from a little under 60 percent to 75 percent.**

or without ads, all media is shifting to digital platforms, in which case, there will be no place for ads. And as digital takes over, it is unknown what will replace advertising.

Scott Cunningham, who previously worked for the Interactive Advertising Bureau (IAB), said that the key to much-needed change is convincing marketers to create ads that cooperate with the way digital media — and its users — functions. They must choose the sites on which a brand's ads will appear, and know that it is more advantageous to focus on quality instead of quantity.

### **The role of Adblock Plus in finding a solution**

Instead of removing all ads from the internet, Adblock Plus is trying to replace the negative ads, which it considers to be large, ugly or intrusive, with positive ads, which are smaller, subtler and much less irritating. It

profitable than the ads a publication could otherwise show, thereby restricting the site's revenue.

Publishers keep 80 percent of all ad revenue, and the remaining 20 percent is divided among other parties involved in placing the ad. Adblock Plus receives six percent of all revenue. According to Ben Williams, operations and communications director of Adblock Plus, the Acceptable Ads program is designed to reverse 100 percent of ad blocking.

Adblock Plus plans to establish a committee of publishers, privacy advocates and advertisers in order to determine the future of its Acceptable Ad standards program. This program may well provide the medium that can offer some relief to internet users who are bombarded with annoying ads, and publishers who are largely dependent on advertising to generate revenue.

- Roxanne Minott

*Email marketing is a great way to build a relationship with your target audience and convince prospective clients that you can be trusted.*



# Boost email conversions

The average person has countless emails jostling for attention in a crowded inbox each day. As a result, lawyers need to develop a strategy that ensures their emails do not get lost among the loud marketing messages and competitive subject lines bombarding them daily.

The good news is that attorneys can use a number of conversion tactics to improve the open and click-through rates of their emails. Using a targeted email marketing strategy that addresses everything from growing a list to implementing effective design elements can help yield higher conversion rates.

## Step 1: Building an email list

Email is a valuable tool because it provides direct entry into the inboxes of your target audience. However, one of the most challenging aspects of email marketing is gaining access to that coveted space. For law firms, the first step is to build a substantial list of email addresses that includes not only current clients but also prospective ones.

There are multiple ways to procure new email addresses. Attorneys can use their Facebook page and other social media to gather basic information like names and emails,

or they can extend offers on their law firm website. For example, people can sign up to receive an ebook in exchange for submitting their email.

While gathering email addresses is an ongoing process, simply having a large list is not enough. Email marketing firm Listrak estimates that around 63 percent of email lists consist of inactive subscribers. Successful email marketing campaigns are those that make periodic efforts to re-engage inactive groups of subscribers by perhaps creating separate lists and content for people moving through different phases of the conversion process.

## Step 2: Getting recipients to open emails

Landing in a prospect's inbox is half the battle. The next step is to get people to open your emails, read them and click through. To do that, your law firm's emails have to generate a connection with the target audience.

**Subject line:** Subject lines create the first impression for email recipients and play a vital role in helping your emails stand out from the competition in a crowded inbox. According to CMB Consumer Pulse, 47 percent of email recipients decide whether to open an email simply based on the subject line.



A subject line should be catchy, clear and brief. All keywords in it must be both descriptive and informative so that recipients know what to expect when they open the email. Avoid spam-like promotional language. Conversion rates will suffer if the message's actual contents diverge from reader expectations.

The length of the subject line is also important. Those that are too long risk getting cut off, especially when emails are viewed on mobile devices. HubSpot recommends keeping subject line length under 50 characters.

**Personal touch:** People receive so much spam that they may be reluctant to open emails from unknown senders. Sending emails from an actual person, rather than your firm, can boost email open rates. Recipients tend to trust personalized sender names and email addresses rather than general ones. An email from an attorney is likely to be more personal than one from "such and such law firm."

### **Step 3: Compelling people to take the desired action**

Email campaigns should be a continuation of the law firm's website in terms of color scheme and fonts, thereby building trust with email subscribers as an overall brand.

**Design elements:** Colors can evoke emotions and capture readers' attention. While emails can and should include images, graphics and colors to be visually appealing, avoid cluttering your messages with too many distracting elements that compete for attention. Anything too bright and garish may be a turnoff and come across as unprofessional. Images can improve reader engagement if they are chosen wisely. Instead of using cheesy stock photos, include graphics and images that are relatable and relevant to the content in the email.

Email still reigns supreme as one of the most cost-effective law firm marketing tools. Campaign Monitor reports email is 40 times more effective at attracting new customers than Facebook or Twitter. With the number of email users worldwide projected to surge to 2.9 billion in 2019, email clearly offers an efficient and direct line of communication to a large number of people.

---

The email's accompanying title and body text should use a combination of complementary fonts that enhance readability while creating interest.

Opting for a minimal design in your emails allows the reader to focus on key features. To that end, divide content into sections so readers can skim the content for an overview before deciding to delve deeper. Break up your email message with images, bullet points and lists for visual appeal and a concise layout.

Today, over 53 percent of emails are opened on mobile devices. Email designs must be responsive and appealing, whether they are opened on a smartphone, tablet, laptop or desktop computer. Emails should be optimized for mobile devices in every aspect including image size, text, format and layout. If your law firm's emails are not mobile friendly, subscribers are likely to delete them without a second thought.

**Call-to-action button:** When it comes to client conversion, emails should include a next step, or call to action (CTA). The majority of email recipients tend to scan emails in a matter of seconds in order to determine if they want to read it in detail. That is why it is essential for every email to have a prominent CTA button that even the speediest scanners will find hard to miss.

If you do not include a next step in every email, it will be difficult to get a return on your investment. The CTA should encourage your law firm's

target audience to click through to your website, contact your law office for a consultation, download an ebook or follow your Facebook page, thereby yielding conversions. Clicking on the button should take the individual to an on-brand landing page that matches the email. Whatever the desired action is, make sure it is clearly communicated through the CTA button.

The CTA should accompany interesting, compelling content that is written using action-oriented language. The more engaged email readers are, the more likely they are to click through the email and convert.

In addition, use a unique color for the CTA button so it stands out from the rest of the email content. Play around with sizing and the use of white space in order draw attention. Bold CTA buttons that are not dominated by overwhelming design have the power to boost click-through rates by 28 percent.

Email marketing is an effective tool for generating new leads and figuring out what works best for your firm is a process. Attorneys can benefit from A/B testing, which involves sending emails to different parts of your email list after changing one variable to compare how it performs. A wide range of elements can be tested, like colors, copy, subject lines, images, CTA buttons and email frequency. Once you determine a format that yields higher open rates and conversions, you can really begin honing your law firm's email marketing strategy.

- Dipal Parmar

# WARRANTLESS TRACKING

A case before the Supreme Court will affect countless criminal investigations in years to come, and it is arguably the most important privacy case in decades.

In *Carpenter v. United States*, nine justices will decide the extent to which cell phone users have a right to the privacy of the entire history of their physical whereabouts.

## Cell-site location information

When a cell phone sends or receives data, the service provider creates and maintains a record of the specific tower with which the phone communicates. This is called cell-site location information, or CSLI, and depending on the circumstances, it can be quite specific. The communications between towers and phones that generate CSLI do not occur solely during calls, or even active use of apps. Users tend to have a large number of apps that periodically issue data requests in the background throughout the day. Thus, service providers generally have detailed records of the location of any phone covering all times it was powered on and not in airplane mode.

Given that the majority of people in the developed world own cell phones and carry them virtually all the time, the aggregate of every service provider's CSLI data approximates a near-complete historical record of everyone's movements. In the United States, it is all available to law enforcement without a warrant.

*Carpenter v. United States* touches on many strong legal precedents, most of which work against any expectation of privacy over CSLI. The Fourth Amendment has long been considered to protect the content of communications, but not "non-content information," often called metadata. Thus, law enforcement needs a warrant to listen in on a phone call, but not to know the number called.

They need a warrant to read a letter, but not the outside of the envelope. CSLI could be seen as non-content information in that it does not contain the actual data communicated, only where and when the communication occurred.

Further, the “third-party doctrine” is a longstanding legal construct that holds people who knowingly and voluntarily give information to third parties, as with CSLI, give up any expectation of privacy relating to that data.

### No warrant required

From December 2010 to March 2011, a group of armed robbers held up a series of T-Mobile and RadioShack stores in Michigan and Ohio. Subsequent to the arrest of four suspects that April, one of the individuals confessed and gave his phone to the FBI. From that phone, the agency compiled a list of sixteen phone numbers with which the confessed had communicated near the times of the robberies. One of these numbers belonged to Timothy Ivory Carpenter.

The FBI then requested and was granted an order from a federal magistrate judge compelling wireless carriers to turn over information about the phones tied to those numbers, including the CSLI data at key times surrounding the robberies.

The request was made under the Stored Communications Act. The law, passed in 1986 as part of the Electronic Communications Privacy Act, defines the circumstances under which the government can compel an internet or cell phone service provider to turn over information.

The judge’s order was not a warrant and therefore did not require probable cause, which likely could not have been demonstrated from the list of phone numbers. Instead, the order stated the government needed only to show the information was “relevant and material to an ongoing criminal investigation,” per the Stored Communications Act.

With the help of CSLI data obtained from Carpenter’s phone, prosecutors were able to secure a conviction, which was later upheld on appeal in the Sixth Circuit.

### Special information

Government attorneys have the easier job in Carpenter. In addition to the precedents laid out above, they will also point to the Supreme Court’s own ruling in *Smith v. Maryland*. That 1979 case concerned the use of a “pen register” — a device installed at telephone company offices that records the phone numbers of calls to and from a suspect’s line. The Court ruled the device’s use is not a “search” per the Fourth Amendment, and does not require a warrant.

Carpenter will have to persuade the Justices to accept that CSLI is distinct from other non-content information in that it amounts to a perfect record of someone’s whereabouts. They will argue it deserves Fourth Amendment protection and requires a warrant to access, despite third-party doctrine and *Smith*.

They will likely refer the justices to *Riley v. California*. The case concerned whether police, upon arresting a suspect and rightfully searching the arrestee’s person and immediate vicinity, could also search the content of a mobile phone. The Supreme Court held that the nature of cell phones, with their tendency to contain vast amounts of detailed personal information, deserved special consideration; police could not search them without a warrant.

*United States v. Jones* presents another potential strategy for the defense. In that case, decided in 2012, police had received a warrant to attach a GPS tracking device to a suspect’s car, but exceeded the warrant’s permitted geographical area and length of time. The Justices ruled unanimously that this constituted a warrantless search and thus was in violation of the Fourth

## IS CELL-SITE LOCATION INFORMATION DISTINCT FROM NON-CONTENT INFORMATION?

*Carpenter’s attorneys will have to convince justices CSLI deserves Fourth Amendment protection despite third-party doctrine and precedent in Smith.*

Amendment, though they split as to the basis of this conclusion. Some held that it constituted a trespass against the defendant’s “personal effects” — in other words, his car — a conclusion unlikely to help Carpenter, who would be hard-pressed to claim a property right over his CSLI. Others held that the search violated Jones’ “reasonable expectation of privacy.”

Carpenter’s attorneys may lean on the latter argument, and in particular the words of Justice Sotomayor, who was alone in accepting both the property rights argument and the privacy argument: “It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.... This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”

Cell-site location information is an enormously powerful tool for law enforcement. If the Justices decide its use should require a warrant, this tool will not go away. But if they do not, then all Americans, law-abiding or not, may have to think twice about what their phones are telling the government about them.

- Ryan Conley





**BIGGER**LAW FIRM

# NOW AVAILABLE EVERYWHERE

Now you can read all the quality articles you have come to expect, anywhere you are, on any device.

**Available on Amazon, the App Store and Google Play**





*Google makes continuous adjustments to not only its search algorithm, but also its search results pages. It experiments with the position and number of ads, the display of local search results, social media posts and news items, among other features.*



# S

## INSIDE FEATURED SNIPPETS

Competition for coveted top spots in organic search results is increasing, and the number of results displayed on page one is decreasing. A 2016 Searchmetrics study found that the number of organic listings on the first page of Google's results has decreased from 10 to 8.5.

Google has added many new elements to its results pages that go beyond its original 10 blue links. Moreover, now different queries will return different versions of Google's results page. For many searches almost all of the real estate above the scroll is occupied by information that is not an organic result, like that displayed in direct answer boxes, featured snippets and related question boxes.

Your firm can take advantage of some of Google's search engine results page (SERP) features that are not organic results links. One of a firm's best opportunities to climb to the top of

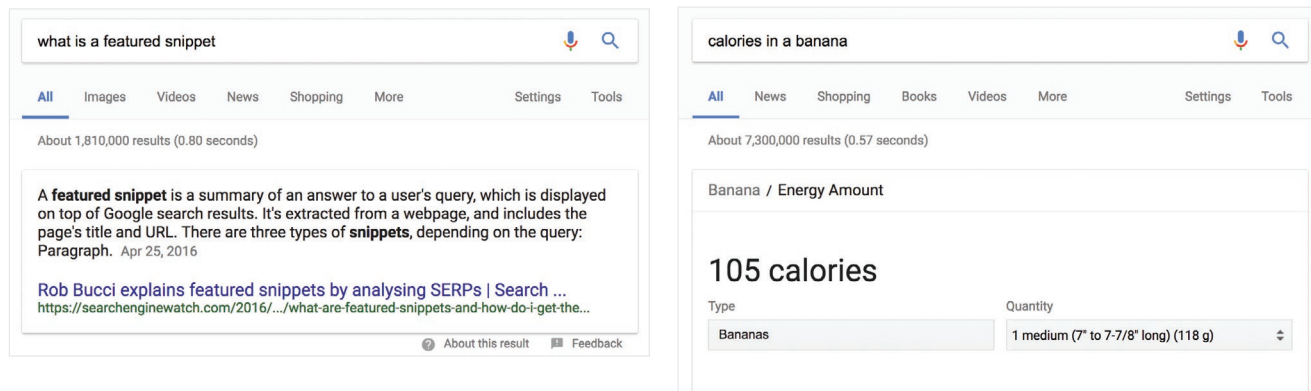
page one is to have a page chosen as a featured snippet. This article discusses statistics about featured snippets and ways your firm can tailor content for inclusion in a featured snippet.

### **What is a featured snippet?**

A featured snippet is a selected search result that appears in a box at the top of a results page with a link to the content's URL. Google populates the snippet by pulling content from selected web pages.

A featured snippet is promoted content from an organic result that may not be the top organic listing. Because of its coveted position above all other organic results, the featured snippet's placement is also referred to as position zero.

Featured snippets appear as paragraphs, lists or tables, with the most common format being the paragraph. The snippet may also contain an image.



*In the above screen shots, the image on the left is an example of a featured snippet and the example on the right is an answer box, which does not contain a link.*

For the purposes of this article, the defining characteristic of a featured snippet is the inclusion of a URL. Answer boxes, which also appear at the top of SERPs, do not contain a link.

Your content is less likely to be selected as a featured snippet for a query that has an established answer, a term that can be looked up in the dictionary, or for information Google considers to be common knowledge or public domain.

## Featured snippets statistics

Recently, Ahrefs performed a study of 112 million keywords in its U.S. database and found that approximately 12 percent of those queries returned featured snippets. Other studies have found that up to 30 percent of queries produce featured snippets.

Ahrefs also uncovered interesting featured snippet click data. The link contained within the snippet does not receive the most clicks. For queries that returned a snippet, the result at position zero received 8.6 percent of clicks, and the first organic search result received 19.6 percent of clicks.

When a SERP does not contain a featured snippet, the top organic

result receives approximately 26 percent of all clicks. Additionally, Ahrefs found that the presence of a featured snippet reduces the overall number of clicks on all listings by about four percent. According to Rand Fishkin, founder of software company Moz, approximately 40 percent of all searches result in no clicks.

## Organic click-through rates

Sometimes a snippet will increase clicks to your site, particularly if your page ranks lower for the query but you have the featured snippet. But, a snippet can also decrease clicks to your site because the user get an answer and has no reason to read more.

These findings do not necessarily indicate that you should stop pursuing position zero. Any page ranking within the top 10 search results can be promoted as a snippet. If, for example, you have a page that ranks naturally at position eight, and you can optimize its content so that it is promoted, the resulting jump in traffic could be substantial.

The featured snippet offers a chance to get more traffic to a page that is having difficulty reaching the number one spot.

The effort required to get to position zero can be less than that required for you to climb to position one.

Additionally, a single page can rank for thousands of snippets. Ahrefs found one top-performing page in its database was chosen as a featured snippet for 4,658 queries.

## How does content get chosen as a featured snippet?

This is a question that is still hotly under debate — and something of a mystery. Google's algorithm determines which pages best answer certain queries, and that there is no concrete list of steps you can take to ensure placement in a featured snippet. However, research does offer some insights into the answer.

**Engagement metrics:** Google's choice of featured snippet content is not based entirely on traditional SEO metrics. This is apparent from the fact that approximately 70 percent of all pages that earn a featured snippet rank below position one. While most (over 90 percent) of the featured snippets are picked from the first page of results, it is not impossible for content on a page in the second or third set of results to be featured.

Larry Kim of WordStream dug into some of the data on lower ranking pages with content that Google promotes to a featured snippet. He found that engagement metrics like click-through rate (CTR) and time on site appear to be important.

Kim looked specifically at a page with an average position of 10 in Google's results with a featured snippet for a particular key phrase. He found the average click-through rate for that result was 21.43 percent, which is roughly 10 times the rate he would expect for a page in position ten.

He also found that average time on page was 14 minutes and 30 seconds — an amount of time virtually unheard of in the online world.

While anecdotal, this data implies that metrics like click-through rate and time on page may be more important to choice of featured snippet than traditional metrics like links.

**Search query:** The majority of featured snippets are the result of long-tail key phrases. Google does not necessarily provide a box answer for the most commonly searched keywords.

This provides a unique opportunity for attorneys, many of whom are already optimizing for high-value long-tail key phrases. Frequently asked questions fit nicely into this box. When you ask a question and provide an answer on the same page, it is easy for Google to recognize your page as the best answer for a specific question.

Questions that employ the five Ws (Who, What, When, Where, Why) + How are good candidates for featured snippets. However, Ahrefs found that 70 percent of the queries that produced featured snippets were not questions, or even sentences. Some examples include,

## WHAT CAN YOU DO?

**1. Write content that keeps readers on your pages.** This means your page must address visitor concerns, not just spam them with location and practice area keywords.

**2. Write in-depth descriptions** for any media content, like videos.

**3. Format your pages in a way that encourages snipping.** Write short, direct sentences and paragraphs. Place headers above your paragraphs that highlight the information contained within the paragraph copy.

Even if you do not place content in a list format, using `<ol>` or `<ul>` tags, Google may still display that content in a featured snippet list if you clearly delineate items with numbers or bolded header text.

**4. Look for featured snippet pick-up opportunities.** If a competing law firm has landed a snippet for a specific key phrase, look for ways you can replace it. Find pages on your own site that answer the query, and create headers, paragraphs or lists on that page that directly address the query. If you can provide a better answer, Google may replace the snippet with yours.

“windows 10 compatibility,” “primary taste sensations,” and any key phrase containing the word “recipe.”

While focusing on a question can produce results for high-performing key phrases, it is not the only tactic for acquiring a featured snippet.

**Formatting:** Snippets are generally formatted in three ways: paragraph, list and table. The paragraph is the most common format.

Pages that receive featured snippets tend to arrange content into easily consumed pieces. The average snippet length is between 40 and 60 words. While unconfirmed by Google, it follows that pages with content distributed throughout the page in smaller, easily sampled chunks are more likely to receive snippets.

**Media descriptions:** Google will feature YouTube video descriptions in a snippet if you tell its algorithm enough about the video. When a video is featured, Google pulls paragraph text from the video's description. Google is unlikely to feature videos with spammy, keyword stuffed descriptions. However, if your description clearly states what the video is about, or what question it answers, the related video can be a candidate for a featured snippet.

Do not chase featured snippets because you think having a snippet will drive more traffic. Experiment with snippets. Some snippets will drastically increase clicks, while others may work against you. Be sure to look at your own analytics and referral data to understand which key phrases you should target for snippets and which are doing fine organically.

- Kristen Friend



A photograph of two men in business suits standing on a rooftop. The man on the left is wearing a grey plaid suit and holding a silver laptop, looking up and to the right with a smile. The man on the right is wearing a dark pinstripe suit and holding a yellow folder, looking towards the first man. In the background is a multi-story brick building with many windows.

# Are you competing against your marketing company?

---

## BRILL LEGAL GROUP ISN'T

---



**CUSTOM**  
LEGAL MARKETING

If your marketing company isn't exclusively working for you, they're helping your competitors. That's why Brill Legal Group trusts Custom Legal Marketing. They know Custom Legal Marketing won't work with any competing firms in their No Competition™ Zone.

**Secure your law firm's No Competition™ Zone at  
[customlegalmarketing.com/exclusive](http://customlegalmarketing.com/exclusive)**

---

**No Competition™**