How digital advertising started vs. how it's going

DIGITAL MARKETING
Matt Weaver

This year, I have read countless articles about consumer privacy. I've watched our government bring big tech leaders like Mark Zuckerberg and Sundar Pichai in for hearings with questions centered around trust and privacy. Most digital ad industry news is dedicated to privacy issues.

It's not a surprise that the government and consumers in general do not trust our industry. In fact, a recent IBD/TIPP poll shows a majority are in favor of breaking up companies like Google and Facebook. There is a widespread perception that the entire industry subverts privacy while putting in place standards that say the opposite.

When you browse websites like CNN.com there are over 30 pieces of code tracking your behavior. They don't ask your permission, nor do they care. They place tracking cookies in your browser that are rarely cleared. This tracking extends across everything you do online and extensive profiles of your behavior, demographics and psychographics are compiled.

Digital marketers celebrate this. They say this is all for the end consumer; it's all for relevancy. The big trend now is "personalization," but not to worry, they also claim there's nothing personally identifiable in it. Not sure how that works.

All this information is then sent back to large ad tech firms who sell your data to advertising agencies and marketers. Your data is used to build digital advertising campaigns that can become as granular as targeting someone who is a mom with three children and is in the market for new yoga pants in a specific zip code or even standing in a specific store or other location.

This is done with "cookies." These cookies are what fuel the digital advertising industry. They allow buyers and sellers to trade on your data. Advanced data mining and predictive analytics allow the sellers to build profiles that try to closely match who you are. A lot of your data is then verified based on what you click. If you click a banner ad, that means the profile used to target you with a specific message worked. This is one of the main reasons clicks have become the ultimate way to determine success for digital campaigns. The click metric is ubiquitous in our industry and the largest companies, like Google, make billions in profit off the click. This has been decades in the making and will take years for publishers and advertisers to move away from. For the advertiser, unless a click actually helped someone buy something, it doesn't have much meaning at all. For the big tech companies profiting off your data, it means everything.

What's happening now is that these large ad tech firms do not want to be regulated, or worse, broken up. They risk losing billions of dollars in revenue if this happens. So, they are working proactively to show potential regulators that they now care about privacy and want to protect it. This is very difficult to do considering they have made billions off selling your data. They also understand that a growing consumer trend has been to block online ads and cookies from tracking consumers. The largest companies that own the browsers you most likely use, like Google and Apple, are axing this decades old technology. And now the digital ad industry is scrambling to figure out how to survive. Pretty much everything up until this point was based on cookies and clicks.

Internet advertising giants like Google and Facebook stand to benefit the most from this. In our industry, these companies are called 'walled gardens' in that they don't share consumer data with one another. Don't fret, Google, Facebook and Amazon have so much information on your personal browsing habits, they don't need to. In fact, these are the companies that are now anti-cookie, which makes them even more relevant since advertisers will shy away from neutral ad tech companies in favor of buying ad inventory from Google, Facebook and Amazon to target their audiences. Google has a wealth of your information through products like Android, Google Maps, Chrome and Gmail. They can track where you go, which stores you visit, products you buy and how you bought them. Same with Amazon. Facebook knows which brands you like and what content you interact with. This is why the ads you see on these properties are highly relevant. And they don't need to use cookies at all to do this.

In the next few years, the largest browsers on the market will be cookieless. This will have a detrimental effect on the digital advertising industry. Gone are the days of easily retargeting individuals and following them around the Internet. Companies built completely on third party audience data will go by the wayside. Demand side platforms claiming to be neutral players and evening the playing field in the digital ad market will most likely fail if they do not come up with a cookieless solution soon.

The winners will be digital marketers who aren't completely reliant on this decade's old technology. Context will matter more than ever, since we won't be able to target profiles, we will need to do the hard work of showing advertising where it actually makes sense. The industry will have to move to a consent model, which is happening currently, where people will need to opt in to being tracked. It's possible this option will give marketers realistic audience profiles built with real consumer information rather than machine learning algorithms. The shift from banner advertising to connected TV, for example, shows how much potential digital advertising has. Layering on real audience data to these campaigns can revolutionize the entire ad market, both traditional and digital. Marketers and agencies alike who understand this shift are in the best position to take advantage of it and make real gains for the brands, products, or services they represent.

Privacy needs to be front and center on the cookieless internet. It's not fair to monetize a person's actions on the web without them knowing. Their data is their currency. If anything, people should be paid to be tracked online, not the other way around. As we continue into 2021, the digital ad industry will need to focus on providing tangible outcomes tied to business goals, not glitzy targeting options and glamorous third party audience profiles. I like to think we are ahead of the curve on this. But as I continue to be pitched privacy invading tactics and new solutions dreamed up to bypass new restrictions by every digital ad sales organization in the country, I know we have a long way to go.

Matt Weaver is director of digital marketing for Mason Digital.

Cybersecurity predictions, lessons learned for 2021

VIEWPOINT
Michael Montagliano

I'm confident to say, and I'm sure everyone will agree with me, that the sooner we can put 2020 in the rearview mirror, the better.

While we've faced the pandemic, economy and election challenges, cybersecurity threats have also added to our angst.

With 2021 squarely in our headlights, here's a quick review of the security issues we've faced this year and the challenges that need to be addressed in the coming year.

Phishing frenzy

In April, I wrote an article about security at the beginning of the pandemic, including statistics about the rise of targeted phishing campaigns associated with COVID-19. Nine months later, that trend has not diminished. In fact, the threat has only grown more complex with the rise of COVID-19 themed attacks.

Phishing attacks are still the primary method hackers use to bypass corporate security safeguards. They're a low-cost, high-impact and risk-free method to simply ask a user to click on a link or enter credentials that grant the attacker a toehold on the network that they can then expand out from.

In the past, I'd say awareness training was the best line of defense. But while that is still critical, we must also be honest about training effectiveness and opt for better identity monitoring and detection tools.

Ransomware everywhere

A ransomware attack occurs every 21 seconds somewhere in the world. In 2020, attacks have been targeted at industries critical to COVID-19 relief and support, such as health care, manufacturing and supply chain. In other words, companies that are more willing to pay ransomware because downtime could affect lives, not just bottom lines. A recent conversation with the FBI revealed ransoms averaging over $1 million and as high as $40 million.

A company's best defense is reliable backups protected from malicious encryption. This allows companies to quickly restore systems and return to production.

A new ransomware element was introduced this year. Recent extortion success has been primarily driven by the initiation of a data exfiltration element that downloads data before encrypting systems. This involves demanding payment to provide a decryption key and, supposedly, prevent the publication of confidential data stolen during the attack. I say supposedly because security researchers say paying the ransom doesn't always mean the threat actors delete that data. Many victims have been double-extorted or have had data published after paying up.

The pressure to submit to extortion, targeting of vulnerable industries and methods that make it more challenging to recover encrypted data will keep ransomware the most profitable "line of business" for cybercriminals in 2021 — and the single biggest threat for all organizations. That makes it critical for organizations to ensure they follow best practices for mitigating ransomware risk in the coming year.

The new norm: remote workforce

Back in March, the pandemic forced companies to move to a work-from-home model, which included, in some cases, moving on-premises workloads to the cloud. The rush to regain productivity has left holes in many organizations' security postures, which hackers are now leveraging.

Cybercriminals always follow users and launch attacks that exploit their behaviors and habits. As employees suddenly became remote workers, cybercriminals took advantage of launching phishing, ransomware and many other targeted attacks. Many companies were unprepared to securely support a remote workforce.

Before the pandemic, most companies (82%) enabled bring your own device (BYOD) for employees, partners or other stakeholders. Because BYOD is outside of corporate support in most cases, basic malware protection tools were either lacking or absent. A lack of preparedness for how to provide BYOD security support is potentially disastrous.

Failure to understand how to support remote work without exposing sensitive information has led to nearly 25% of organizations paying unexpected costs to address cybersecurity breaches and malware infections. If organizations don't rethink their security approaches, cybercrime will continue to advance, with remote workers' exploitation being the ideal entry point into corporate IT networks.

Nations under attack

In 2021, there will be a significant increase in cyber espionage campaigns carried out by state-sponsored hackers due to the ongoing pandemic and escalating tensions between nation-states.

State-sponsored attackers strive to gather intelligence on strategic intellectual property, giving their governments a technological and economic advantage in the post-COVID-19 world.

Disinformation attacks have had severe consequences on our nation's confidence level on numerous fronts. Targeted attacks on critical infrastructure and attempts to steal defense contractors' regulated data place the country at risk. New regulatory and audit functions are being rolled out to increase contractors' ability to protect data. Those programs are still ramping up in 2021 and will take some time to be fully implemented.

Conclusion

The end of the pandemic is in sight, with vaccine delivery underway, and the economy will recover. Still, cybersecurity threats will continue, and it is our job to be ever vigilant in protecting our assets and information. 2020 placed us in the middle of a perfect storm. For cybersecurity, a multi-layered approach and the involvement of private and government stakeholders are necessary to prevent cyberattacks from having even more dramatic consequences next year.

2021 can't get here fast enough. Happy New Year!

As chief technology officer at iV4, a ProArch company, Michael Montagliano leads the technology strategy and execution for the firm he joined nearly 10 years ago. He is also a "Certified Ethical Hacker." Montagliano's love for music inspires him to bring creativity to the world of IT every day. Want to talk IT or music? He'd love to hear from you. Upcoming news: In 2021, iV4 will be rebranded as ProArch – more to come! To contact Montagliano, email him at mmontagliano@iv4.com.