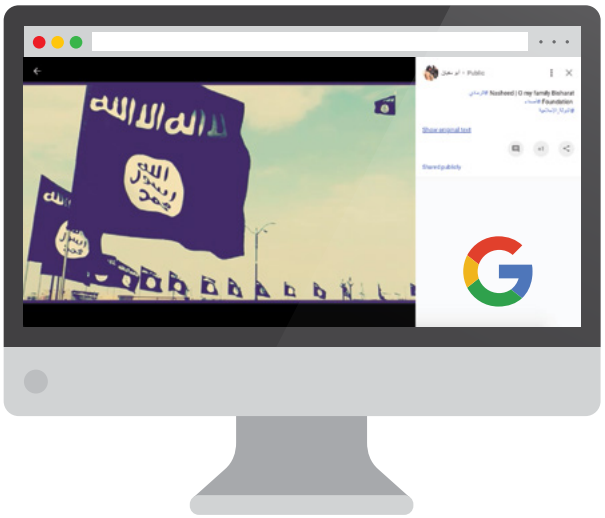
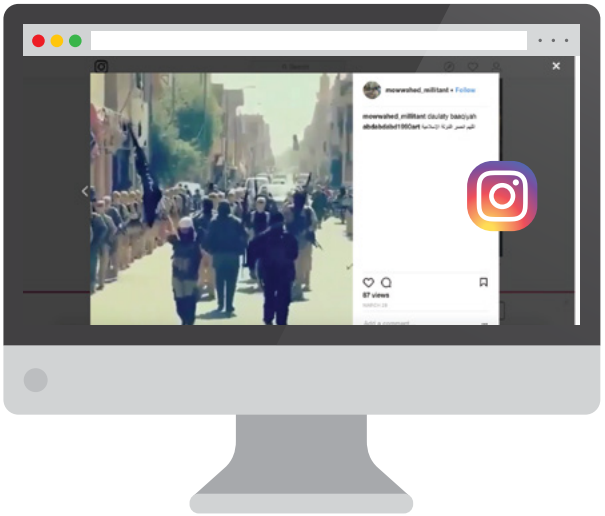
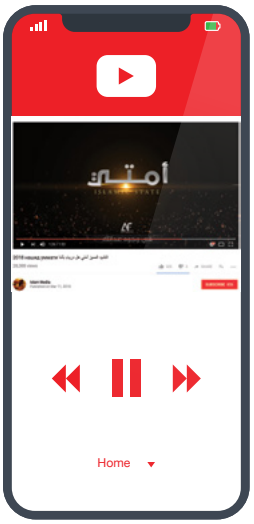


FOOL ME ONCE...

HOW TERRORISTS AND RELY UPON THE "SEE NO EVIL, HEAR NO EVIL" BUSINESS MODEL OF GOOGLE, FACEBOOK, AND INSTAGRAM





MAY 2018

digitalcitizens alliance

WARNING:

THIS REPORT CONTAINS DISTURBING IMAGES AND LINKS TO VIDEOS AND OTHER CONTENT THAT SHOW VIOLENT ACTIONS.

TABLE OF CONTENTS

TABLE OF CONTENTS I
INTRODUCTION 01
GOOGLE+: MAINSTREAM USERS MOVED OUT, JIHAD MOVED IN 04
JIHADIS FACEBOOK & INSTAGRAM 06
FINDING ANSWERS, CRAFTING SOLUTIONS 09
ENDNOTES 12
ABOUT DIGITAL CITIZENS 13

INTRODUCTION

Despite promises by digital platforms to curb material supporting terrorism, Jihadi groups such as ISIS and other terrorist organizations continue to rely upon Google, Facebook and Instagram to sow fear, spread hate and recruit members, according to a new Digital Citizens Alliance investigation.

Dozens of videos and posts appear on social platforms on accounts active at least since 2016—with some still available and others only recently deactivated. These include an April 2018 post that spotlights the teachings of ISIS leader Abu Bakr al Baghdadi, images of mass executions and a March 2018 YouTube video promoting the Islamic State (with over 34,000 views as of May 8, up from 15,000 views when the image was first discovered on April 26.).[1]

Social media is an important terrorist recruiting tool, so videos and posts utilize news such as recent bloodshed in Syria and even the recent mass shooting in Florida to promote their cause and attract members. Examples from dozens of screen shots and links are included in this report.

Terrorist groups and sympathizers have an acute understanding of how valuable digital platforms are to their cause. They share advice on how to use these platforms with posts such as: "A Guide to Social Media Platforms and how to manipulate each Social Media Platform."

It does not appear that the leaders of the digital platforms have a grasp on how often their systems fail to remove problematic content. During his recent testimony to Congress, Mark Zuckerberg said "99 percent of the ISIS and Al Qaida content that we take down on Facebook, our A.I. systems flag before any human sees it."[2] However, a January 2018 report from Just Security, found dozens of pro-ISIS pages on Facebook. In only slightly more than half of the cases did Facebook remove the content. And, now, this Digital Citizens investigation found new examples just weeks after Mr. Zuckerberg made that statement.

What makes these revelations especially troubling is they come to light after the companies vowed to clean up the hate speech and other offensive content on their platforms. These new examples of hate speech, for example, come a full two years after digital platforms were warned about terrorist content on their sites, including a March 2016 report in which Digital Citizens detailed how political ads for presidential candidates were appearing next to Jihadi videos.[3]

The inability to prevent terrorist organizations from utilizing these platforms raises questions and skepticism about whether the companies' business models—based on collecting user personal information and enabling anyone to post content—can effectively address the issues of hate speech and illegal and illicit content that regularly surfaces.

For the past five years, Digital Citizens has raised alarms, pointing out how painkillers such as oxycodone, stolen credit cards, pirated content, malware and counterfeits such as fake passports have proliferated on digital platforms.

2018 was supposed to be different. Chastened by how Russians used them to meddle in the 2016 U.S. presidential election and an advertiser backlash against inappropriate content, digital platforms were supposed to spend the year earning back our trust.[4] The platforms promised users and government officials that they would clean up the inappropriate, illegal and illicit content that blurred the lines between mainstream digital platforms and the so-called Dark Web where anything and anybody is for sale.

Instead, 2018 has been a year of revelations of how digital platforms such as Facebook, Google and Twitter mistreated the personal information of its users and gave criminals and bad actors a run of their platform.

The latest Digital Citizens Alliance investigation exposes the fallacy that much, if anything, has changed. Partnering with the Global Intellectual Property Enforcement Center (GIPEC), Digital Citizens has reviewed dozens of examples of how terrorist organizations continue to rely on digital platforms such as Google, Facebook, YouTube and Instagram to promote hate speech and recruit.

What it underscores is that the problem is not a surface issue that can be solved simply through greater vigilance or the hiring of more content monitors. The true cause of these troubling issues is the business model of these platforms. When Cambridge Analytica inappropriately received the personal information of at least 87 million Americans harvested by Facebook there was no breach—Facebook turned that information over to the company because its business model is to monetize users' personal information with advertisers and third parties.

And the Russians weren't able to try to influence the 2016 election due to digital platforms being asleep at the switch—it was because their business model was set up to enable nearly anyone to post content with essentially no ramifications. For years, Google's response to criticism about illegal and inappropriate content on its sites is that it will take it down if notified—but in 2018 that seems woefully short given the collapse of Internet user trust.[5]

Research surveys by Digital Citizens and other organizations found that a majority of Americans now view these digital platforms as irresponsible companies that should be regulated. Seventy-one percent of Americans said their trust in these platforms had dropped in the last year. Asked to think of Facebook as a neighborhood, 57 percent labeled it an "unsafe neighborhood."[6]

Moreover, the platforms are in no rush to change their business model—unless advertisers, lawmakers or regulators call them on it. The platforms prefer to treat the proliferation of illegal and illicit activities on their sites as a PR problem to be crisis managed instead of as Internet safety and national security concerns that require a fundamental re-consideration of their business model. And—as you will see—if there is no advertiser concern, forget about it—it's every man, woman and child for themselves. We can't be sure the platforms are even bothering to look and see the same things we're finding—pictures and posts glorifying murder, mayhem and attacks against innocents.

For their reliance on this "anything goes" business model, the digital platforms came under enormous scrutiny and criticism in 2017. They were blamed for their laxity. In other words, fool us once, shame on you. Now, in 2018, we face the realization that when it comes to taking Google, Facebook, Instagram, YouTube, Twitter and other platforms at their collective word that they will solve this problem on their own—fool us twice, shame on us.

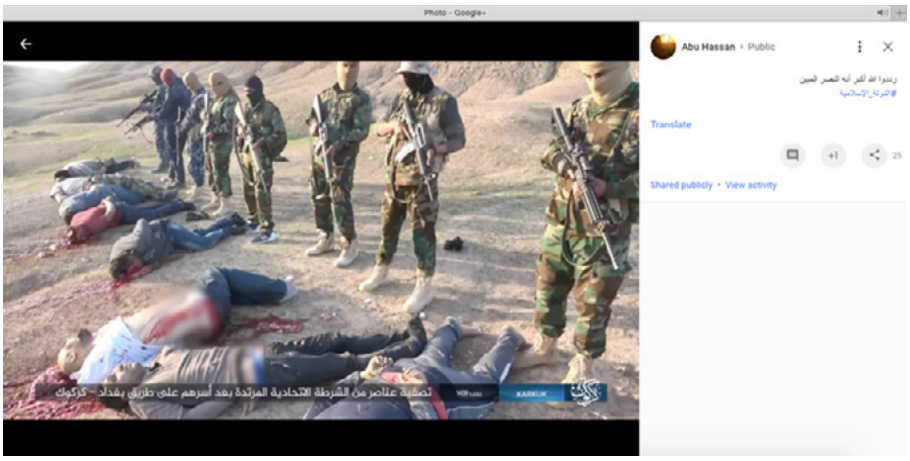
Digital Citizens would like to recognize and offer thanks to our research partner on this report, Eric Feinberg of GIPEC. Without Mr. Feinberg's diligence and technology this report would not exist. For more information on GIPEC, please visit: http://www.gipec.com.

GOOGLE+: MAINSTREAM USERS MOVED OUT, JIHAD MOVED IN

Google's efforts to combat Facebook's emergence included the launch of social media site Google+ in 2011. While it boasted of over hundreds of millions of users by 2014 it was labeled a "ghost town" by the New York Times.[7] In 2015, the company stopped requiring that users have a Google+ account and profile to access other Google sites—essentially a white flag moment.[8]

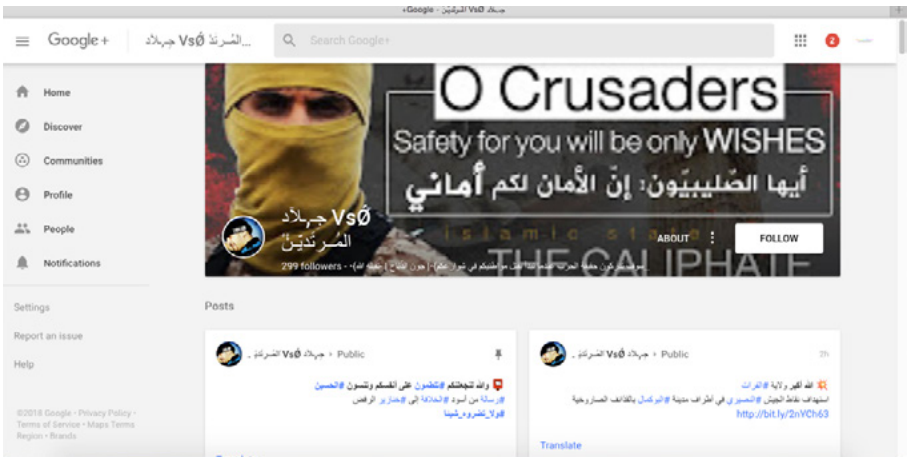
Enter the Islamic State. Today, dozens of videos populate Google+ to advance the Jihadi agenda and promote its activities. In the screen shot below, you see the aftermath of a mass execution of eight unidentified men and it depicts what appears to be the grisly deaths of numerous others. The accompanying video graphically shows the execution itself.[9] Note: If Google follows its crisis PR practice it will remove this content while explaining it does so upon being alerted. That in part is the very issue Google faces—why it takes the actions of others to get the company to police its own platform.

The disturbing videos, images and posts below were allowed to remain on digital platforms for weeks and months. Some have recently been removed; others remain active as of early May.



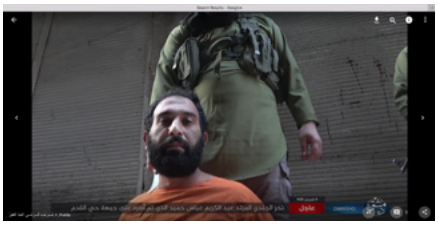
GIPEC researchers discovered this video on Google+ on April 4, 2018. As of May 1, it is still on Google+.

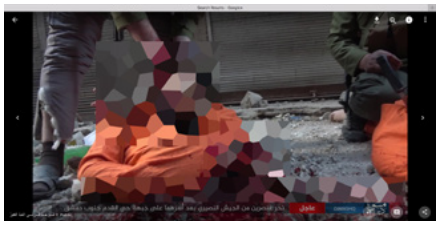
In this post, a group claiming to represent the Islamic Caliphate posts a threatening message (seemingly geared towards a Western audience) that "Safety for you will be only wishes."



GIPEC researchers discovered this video on April 9, 2018. It is no longer online.

The following images have been partially obscured because of their grisly and troubling nature. These and other the Google+ images show terrorists beheading at least two men. These images were captured on April 25, 2018. As of May 8, a link with still images from the beheading remains live on Google+.





There are, disturbingly, even more gruesome images on Google+ that Digital Citizens chose not to include in the report.

How these images remain on Google's platform is confounding. In 2017, Google—faced with an advertiser backlash that included well-known brands such as AT&T, Verizon, Pepsi, Walmart, Dish, Budweiser, Starbucks and General Motors—vowed to aggressively police "hateful, offensive and derogatory content."[10]

If that is the case, why are months-old Jihadi videos and content still proliferating on Google platforms? There seems to be only one possible answer: the business model enables it.

The investigation found that terrorist groups and sympathizers publish and share information on how to most effectively use digital platforms to advance their agenda. The shared posts found by GIPEC researchers included the previously mentioned, "A Guide to Social Media Platforms and how to manipulate each Social Media Platform."

GIPEC researchers found the Guide and other posts in which terrorists share strategic ideas about how to manage their social media accounts. Below is an example found on justpaste.it (a site that is known to be popular with jihadists[11]):

ما يحدث عند تعليق ملفك الشخصي أو صفحة على - JustPaste.it

. الان السؤال الذي يطرح نفسه كيف افك التعليق او بطريقة اخرى

تقديم التماس بشأن تعليق الملف الشخصي أو الصفحة على

Google+

لتقديم التماس بشأن تعليق ملفك الشخصي أو صفحتك على

Google+

استخدم جهاز كمبيوتر لتسجيل الدخول إلى حسابك المعلَّق واتبع التعليمات التي تظهر على الشاشة.

وربما يُطلب منك إزالة أو تغيير أي محتوى ينتهك سياساتهم أو يُطلب منك تقديم المزيد من المعلومات

وغالبا ما تحل المشكلة بتغير الخلفية والصورة ومرات يكون الاسم كذالك حسب التبليغ

فالمسالة ليست بتلك الصعوبة استرجع حسابك اخي المناصر ونشر اخبار دولتك وسد ثغرك الاعلامي

ولاتجعلهم يهنؤن او ويحسو انهم انتصرو بل اجعلهم يعتقدون انهم اما جيش وحدك

(الحوكم ابو سيف الله المسئول (الشيخ الاسود

Created: 20/03/2018

Visits: 79
Online: 1

Save as PDF

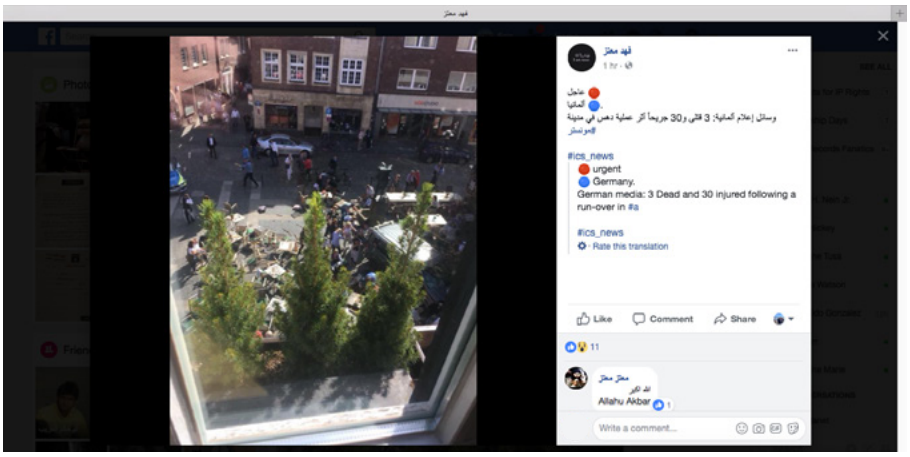
© 2018 justpaste.it

Premium Terms of service Blog About

JIHADIS FACEBOOK & INSTAGRAM

The real-time features of Facebook (and Twitter and Instagram as well) lend themselves to terrorists who rely on being nimble to get their message out. Here are examples where Facebook serves as the ideal platform.

In what German authorities labeled a terrorist attack, a van barreled into a crowd in Münster in early April, killing three people and injuring 30 more. The Jihad message was quickly spread on Facebook.



GIPEC researchers found this video April 7, 2018. This video is no longer online.

GIPEC researchers have found pro-ISIS content on Facebook for years and somehow it has stayed up on the platform all that time, including this image posted on July 7, 2016. GIPEC shared it with us on May 8, 2018.

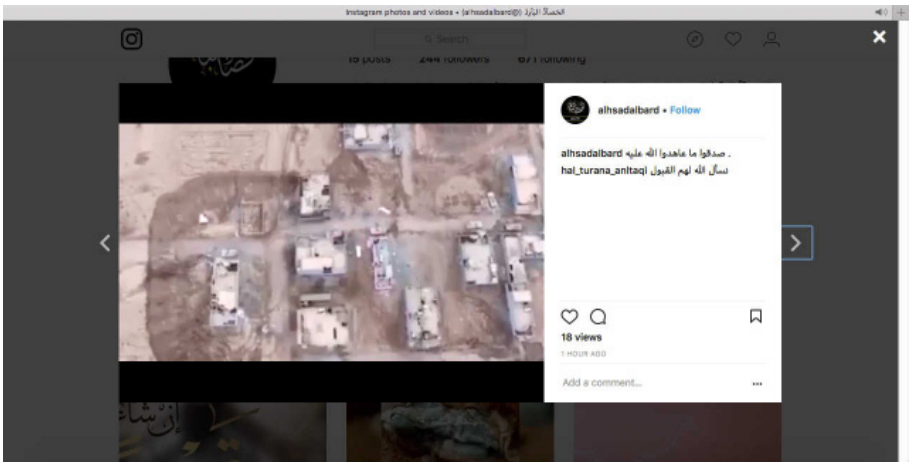
GIPEC researchers found this set of images at its current location on May 1, 2018. It is still online there. The GIPEC researchers have found this post several times and even reported it previously to Facebook, but it continues to reappear on the platform.

In its January 2018 report from Just Security, GIPEC reported dozens of pro-ISIS pages on Facebook. In 56 percent of those cases, Facebook removed the content. As the national security online forum Just Security pointed out: "this material had apparently escaped Facebook's own methods for identifying and removing malicious content."[12] Going further, Facebook decided not to remove pages that Just Security said, "clearly violated its standards, even after being directly informed of the malicious content." Just Security went on to say "it is difficult to discern any meaningful difference between the content that Facebook removed and the content it retained."[13]

Beyond Facebook proper, the Islamic State is also utilizing its hugely popular subsidiary platform, Instagram, which boasts a larger community of teens and younger adults than its parent company. While terrorist organizations, including ISIS, have been shown to use Instagram in the past, the nature of it has evolved.[14]

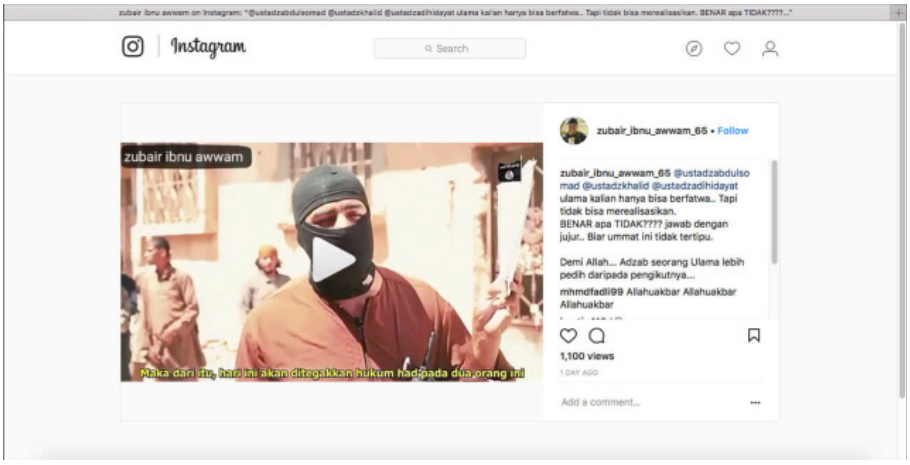
Previously, accounts linked to or supporting the Islamic State cause sought to normalize the behaviors of the terrorist group and depict the day-to-day life of participants in the Jihad. Today, the accounts and the materials they post have shifted more to the extreme with an increased focus on radicalizing those following their accounts on Instagram.

For example, the series of images below were taken from a video shared on Instagram of an alleged suicide bombing committed by terrorists.



Click the image at right to activate the series.

This particularly disturbing set of images was taken from a separate video shared on Instagram in which a terrorist is shown throwing his victim off of a building with his hands bound behind his back.



Click the image at right to activate the series. GIPEC researchers found this video from which these three screenshots came from on April 29, 2018 on Instagram. As of May 16, it is no longer online.

These images are, sadly, a mere sampling of those GIPEC found during the course of their research. GIPEC researchers used thousands of hashtags to find these posts, including (in Arabic) #khilafhfr, #broadcasting, #islamic_country, #Amaqagency, and #depthagency. The GIPEC researchers say the platforms will have more success pulling down terrorist content if they look for "problem hashtags or communications strings." If the platforms continue to simply look for the inflammatory content, they'll always be one step behind. The question is, with their current business model, with no economic incentive to search for terrorist content, will the platforms commit to pursuing threat actors and taking their content down?

For a full directory of Jihadi content found during this investigation please go to: http://www.digitalcitizensalliance.org/main/jihad-album

FINDING ANSWERS, CRAFTING SOLUTIONS

Digital Citizens has no doubt that within hours of the publication of this report all offending content that has yet to be removed will be. And Google, Facebook, YouTube, Instagram and others will hope that is the end of it.

It is clear, however, that there is no end as long as the business model of digital platforms is geared towards the flow of information that can be monetized. It is worth noting a memo from 2016 that recently surfaced in which a top Facebook executive said the company shouldn't let negative consequence get in the way of its mission. "Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools. And still we connect people," wrote Andrew "Boz" Bosworth, Facebook Vice President.[15]

That is the clearest reflection of the business model: nothing should stand in the way of our mission and progress. But we also know that short-sighted thinking based on legal exposure, growth and profits is what got us to a crisis in trust.

2018 has proven to be a watershed year. The core questions are no longer whether digital platforms violated our privacy by giving out and profiting off of the details of our personal lives. They did and do. Or whether these platforms were used by malicious actors seeking to undermine civil society and democracy. They were and are.

No, the core question now is what kind of change is coming to the digital platforms? The only uncertainty in that is whether it will be done by the platforms or dictated by policymakers in the United States or Europe or by federal and state regulators or law enforcement.

Digital Citizens has called on digital platforms—especially Facebook (which also owns Instagram) and Google—to come clean about what has happened on their platforms. The fact that Facebook knew about what occurred at Cambridge Analytica for two years but only took steps recently to change its business model explains why they have lost the public trust. The companies have to own up to the fact that the aggressively hands-off approach they took to policing content made it easy for criminals and other bad actors to exploit the platforms, which in turn has blurred the lines between mainstream sites and the "Dark Web." That would be a start.

For two years, Digital Citizens has proposed numerous steps digital platforms could take. They include using their vaunted algorithms and technology used to place relevant ads, even on inappropriate content, to flag suspicious content for inspection. For example, social media platforms should attack terror videos with the same vigor they've had going after pornographic and sex trafficking content. Specifically, any content advocating violence against any ethnic or religious group should come down in a day. If we run the same search six months from now, we should come back with nothing.

To quickly weed out offensive, inappropriate, illicit and illegal content, Digital Citizens has called on the companies to create a cross-platform initiative to identify and share information, so they could ban bad actors. Yes, that will result

in a game of "whack a mole" whereby bad actors surface under new names, companies and web addresses. But research shows that having to continually change inhibits bad actors' ability to effectively operate.

Facebook CEO Mark Zuckerberg recently acknowledged that the company is "responsible for the content" on its platform.[16] Will Google make the same declaration? Acknowledging their role in 2016 political misinformation, Facebook and Twitter committed to supporting the Honest Ads Act that imposes new political ad disclosure requirements on tech companies. Will Google make the same commitment?

Digital Citizens is now skeptical that voluntary action by the digital platforms themselves will solve the crisis and satisfy a distrustful public. It seems the window for companies on their own to satisfy the public is closing.

That means government action may be necessary. But whoever takes that role should not start with the symptoms: inappropriate content such as Jihadi posts and videos, illegal and illicit content promoting dangerous painkillers, stolen credit cards, pirated content or counterfeits. They must start at the root: the lack of accountability exhibited by Google, Facebook, Instagram, YouTube, Twitter and others. Russian meddling and worrisome and offensive content are simply the inevitable outcome of that lack of accountability.

There are multiple avenues for the United States government to pursue. It could be a mix of federal and state actions. The United States Congress could revise privacy and other laws that govern how content is treated online to force platforms to take greater legal responsibility.

Regulators and watchdog agencies such as the Federal Trade Commission could investigate to understand just how much digital platforms know about this content. There is reason to wonder: in 2011 Google paid $500 million to close a U.S. investigation that the company knew that rogue online pharmacies were illegally marketing medications through Google AdWords as early as 2003.[17]

States could intervene as they have with big tobacco and other industries—especially as we learn the impact of digital platforms on young teens. For example, state attorneys general could work together to negotiate agreements in which digital platforms agree to take more steps to block illegal and offensive content. In Missouri, Attorney General Josh Hawley has already launched an investigation of Google's business practices.[18]

And in Europe new regulations are due to take effect in May to protect user privacy and other efforts are underway to force digital platforms to be more accountable for the content that appears on their sites.[19]

The British House of Commons, Home Affairs Committee may have provided a preview of what could come in future regulations in its report, "Hate crime: abuse, hate and extremism online."[20]

Based on their investigation, the MPs wrote about Google: "one of the world's largest companies has profited from hatred and has allowed itself to be a platform from which extremists have generated revenue."

Later in the report, the MPs wrote about the other major social media platforms: "Social media is too important to everyone—to communities, individuals, the economy and public life—to continue with such a lax approach to dangerous content that can wreck lives. And the major social media companies are big enough, rich enough and clever enough to sort this problem out—as they have proved they can do in relation to advertising or copyright. It is shameful that they have failed to use the same ingenuity to protect public safety and abide by the law as they have to protect their own income."

After everything that has happened in the last two years, the discovery of offensive and hateful Jihadi videos and posts on lading digital platforms is an indicator that perhaps the companies simply don't have the capability or the will to police themselves. In that case, someone will have to do it for them.

ENDNOTES

1 Islam Media. "2018 нашид уммати بأننا دريتِ هل أمتي المميز النشيد." YouTube, 11 Mar. 2018. Web. 26 Apr. 2018. https://www.youtube.com/watch?v=tzuL69z64QI

2 "Transcript of Mark Zuckerberg's Senate hearing." *Washington Post*. 10 Apr. 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.1c062cbd3906

3 Digital Citizens Alliance. "Fear, Loathing, and Jihad: How YouTube is Pairing the 2016 Candidates with the Creepy, the Corrupt, and the Criminal." Digital Citizens Alliance. Mar. 2016. http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/fear-loathing.pdf

4 Woo, Stu & Sam Schechner. "YouTube Faces Fresh Backlash After Ads Appear Near Pedophile Comments." *Wall Street Journal*. 27 Nov. 2017. https://www.wsj.com/articles/youtube-faces-fresh-backlash-after-ads-appear-near-pedophile-comments-1511532337

5 Galvin, Tom. "Facebook in Crisis: 10 Years in the Making." *Morning Consult*. 3 Apr. 2018. https://morningconsult.com/opinions/facebook-in-crisis-10-years-in-the-making/

6 Digital Citizens Alliance. "Digital Platforms in Crisis: A Decade in the Making." Digital Citizens Alliance. Apr. 2018. http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Digital_Platforms_in_Crisis.pdf

7 Miller, Claire Cain. "The Plus in Google Plus? It's Mostly for Google." *New York Times*. 14 Feb. 2014. https://www.nytimes.com/2014/02/15/technology/the-plus-in-google-plus-its-mostly-for-google.html

8 Barr, Alistair. "Google Gives Up on Google+ as a Facebook Rival." *Wall Street Journal*. 27 July 2015. https://blogs.wsj.com/digits/2015/07/27/google-gives-up-on-google-as-a-facebook-rival/

9 Hassan, Abu. "المبين النصر أنه أكبر الله رددوا." GooglePlus. 3 Apr. 2018. https://plus.google.com/photos/photo/117354143024670565838/6540372238418529890

10 Chappell, Bill. "Google Promises To Keep Ads Off 'Hateful, Offensive' YouTube Content. *National Public Radio*. 21 Mar. 2017. https://www.npr.org/sections/thetwo-way/2017/03/21/520976552/google-promises-to-keep-ads-off-of-hateful-offensive-youtube-content

11 "JustPaste.it." *Wikipedia, The Free Encyclopedia*. Wikipedia. 2 Mar. 2018. Web. 1 May 2018. https://en.wikipedia.org/wiki/JustPaste.it

12 Goodman, Ryan. "Exclusive: New Evidence of Loopholes in Facebook's Regulation of Terrorism Content." *Just Security*. 16 Jan. 2018. https://www.justsecurity.org/51030/exclusive-evidence-loopholes-facebooks-regulation-terrorism-content/

13 Ibid.

14 Carman, Ashley. "Filtered extremism: how ISIS supporters use Instagram." *The Verge*. 9 Dec. 2015. https://www.theverge.com/2015/12/9/9879308/isis-instagram-islamic-state-social-media

15 Selk, Avi. "'Maybe someone dies': Facebook VP justified bullying, terrorism as costs of networks's 'growth.'" Washington Post. 30 Mar. 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/03/30/maybe-someone-dies-facebook-vp-justified-bullying-terrorism-as-costs-of-growth/?utm_term=.0b04d3642072

16 Weinberger, Matt. "Mark Zuckerberg just renounced a core piece of Silicon Valley wisdom—and it could come back to bite Facebook." *Business Insider*. 10 Apr. 2018. http://www.businessinsider.com/mark-zuckerberg-facebook-is-responsible-for-the-content-on-its-platform-2018-4

17 Pearson, Jake. "How A Career Con Man Led a Federal Sting that Cost Google $500 Million." *WIRED*. 14 May 2013. https://www.wired.com/2013/05/google-pharma-whitaker-sting/

18 Dave, Paresh. "Google faces antitrust investigation in Missouri."*Reuters*. 13 Nov. 2017. https://www.reuters.com/article/us-alphabet-antitrust/google-faces-antitrust-investigation-in-missouri-idUSKBN1DD2CE

19 Price, Rob. "Facebook may be underestimating the challenge it faces in Europe." *Business Insider*. 26 Apr. 2018. http://www.businessinsider.com/gdpr-facebook-legal-challenges-q1-2018-4

20 House of Commons Home Affairs Committee (2016-2017). *Hate crime: abuse, hate and extremism online* (Report No.14). London, UK: House of Commons. https://publications.parliament.uk/pa/cm201617/cmselect/cmhaff/609/609.pdf

ABOUT DIGITAL CITIZENS

This report was created by the Digital Citizens Alliance, a nonprofit 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet and the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place. While all Digital Citizens hold themselves personally responsible to do all they can to protect themselves and their families, we are also concerned that technologies, standards, and practices are in place that will help keep all of us safe as a community. The industry has a critical role to play in ensuring those safeguards are established and updated as needed to address the continually evolving challenges we face online. We have much work to do, but we can't do it effectively without understanding the problems we face. That is why the Digital Citizens Alliance investigates issues such as those detailed in this report. By sharing our findings with consumers, we hope all Digital Citizens will engage in discussions about these issues.

digitalcitizens alliance

@4saferinternet