Washington Journal of Law, Technology & Arts

Volume 18 | Issue 2 Article 1

2-6-2023

GOOGLE DORKING OR LEGAL HACKING: FROM THE CIA COMPROMISE TO YOUR CAMERAS AT HOME, WE ARE NOT AS SAFE AS WE THINK

Star Kashman
Brooklyn Law School

Recommended Citation
Star Kashman, *GOOGLE DORKING OR LEGAL HACKING: FROM THE CIA COMPROMISE TO YOUR CAMERAS AT HOME, WE ARE NOT AS SAFE AS WE THINK*, 18 WASH. J. L. TECH. & ARTS 1 (2023).
Available at: https://digitalcommons.law.uw.edu/wjlta/vol18/iss2/1

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 18, ISSUE 2 — SPECIAL ISSUE WINTER 2023

GOOGLE DORKING OR LEGAL HACKING: FROM THE CIA COMPROMISE TO YOUR CAMERAS AT HOME, WE ARE NOT AS SAFE AS WE THINK

Star Kashman

ABSTRACT

This article addresses the issue of Google Dorking ("Dorking"): an underestimated, overlooked computer-crime technique utilized by hackers, cyberstalkers, and cybercriminals alike. Google Dorking is the specialized use of the Google Search engine which can be used to uncover sensitive data unintentionally exposed to the public online. Dorking can be beneficial and harmless when used by innocent researchers, journalists, and curious users. But it can be incredibly harmful if utilized by malicious actors. Dorking is behind notorious and infamous computer crimes that appear vastly different on the surface, such as a sextortion case involving over a hundred women including Miss Teen USA, an infamous hack of the Bowman Avenue Dam in New York, an intelligence failure that killed over 30 CIA assets and compromised around 70% of CIA operations internationally, and countless cases where legal officials, celebrities, politicians, families, and the average person alike have fallen victim. Anyone with access to the internet can "Google Dork"; the law currently fails to address the legality of this act or recognize it in the justice system. No one is nearly as safe as they think they are.

TABLE OF CONTENTS

INTRODUCTION

Although over half of the world has been utilizing the Google Search engine since 2019,[1] hardly any of these individuals have ever even heard of the term "Google Dorking". There is a vast difference between conducting a regular Google Search and a Google Dork. An average Google search does not yield the most accurate, unbiased, or useful results. Results are organized within a "filter bubble" based on Google's determination[2] of how relevant each result is based on an algorithm of over 210 miscellaneous factors,[3] our computer data, and paid sponsored content pushing products and political ideologies. Internet users are often oblivious to the power that search engines hold with the distribution of knowledge and sole discretion on what is made available to its users.

Thankfully, there is a method of searching and bypassing these filters to receive" untainted, unedited, and unbiased

[1] Danny Sullivan, *Google now handles at least 2 trillion searches per year*, SEARCH ENGINE LAND (May 24, 2016, 12:00 PM), https://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247.

[2] Robert Irvine, *6 Ways To Get Unfiltered Google Search Results*, MAKE USE OF (Nov. 21, 2020), https://www.makeuseof.com/google-unfiltered-search-results.

[3] *Google Rankings Explained – How Does Google Decide Which Websites To Rank When Searching?*, MORNINGSCORE (Sep. 27, 2021), https://morningscore.io/how-does-google-rank-websites.

> results called "Google Dorking"[4] (A/k/a "Google Hacking"[5], "Search Engine Hacking", or "Google Scanning")[6], which is the act of utilizing advanced search queries ("Google Dorks") to specify the exact results one is seeking while avoiding Google's filters.

Google Dorking can be a benefit to Google Users for numerous reasons. Aside from the perks of avoiding propaganda, advertisements, and search engine optimization ("SEO"), Google Dorking has been used to protect against cyber theft and data security breaches. In addition, Dorking is a common tool utilized by "White Hat Hackers" who are ethical legal hackers hired to seek out vulnerabilities in computer systems for the purpose of mending gaps in security before malicious hackers exploit them. Journalists and good faith researchers also utilize Google Dorks to obtain more accurate search results, and average Google users can make use of Dorking to yield enhanced results.

However, not all Google Dorking is conducted for legitimate reasons. Unfortunately, hackers and cybercriminals have also made use of Google Dorking to find sensitive personal information, and online vulnerabilities. Countless data, files, and webpage content that data owners do not intend to be displayed publicly can be found via Google Dorking. "That information can be used for any number of illegal activities, including cyberterrorism, industrial espionage, identity theft and cyberstalking."[7] There are countless incidents where individuals have their private data and files displayed online without even being aware of it. Additionally, Google Dorkers gaining more accurate search results may unintentionally stumble upon sensitive data, leaving them one click away from committing a cybercrime.

This research concentrates on educating the public about the dangers of Google Dorking and the lack of knowledge surrounding these dangers within the Justice System. The current statutory protections and efforts made by Google, the public, and the Cybersecurity community have been inadequate to protect victims from the evolving threat of hacking. Cybersecurity law must adapt in accordance with these modern cybercrime methods. Part I provides

[4] Ivy Wigmore, *Google Dork Query*, WHATIS.COM, (Sep. 2014), https://www.techtarget.com/whatis/definition/Google-dork-query.

[5] Julie Bort, *Term Of The Day: 'Google Dorking'*, INSIDER (Aug. 28, 2014), https://www.businessinsider.com/term-of-the-day-google-dorking-2014-8.

[6] JOHNNY LONG, GOOGLE HACKING FOR PENETRATION TESTERS 534 (2d ed. 2008).

[7] Wigmore, *supra*.

an overview of the current statutory protections against hacking, and their shortcomings. Part II analyzes the legality of Google Dorking. Part III evaluates whether Google Dorking should be legal, and Part IV advocates for change needed to resolve the issues surrounding Google Dorking.

What are Examples of Google Dorks?

Google states that "you can use symbols or words in your search to make your search results more precise." These functional symbols or words are called "operators." Use of these operators is typically harmless and useful. For example, one could search for specific websites by adding "site:" in front of the desired domain. Another commonly utilized operator is "filetype:" which limits search results to only display a specific file type such as documents, PowerPoints, excel sheets, and more. Google Dorks are search queries that use these advanced Google operators.

Google admits that one can easily access the cached (older) version of a website by placing "cache:" in front of the address.[8] If a website changes, the website owner expects the old version of the website to be replaced by the new version and rendered inaccessible. This is an inaccurate expectation if a searcher is using the above Google Dork. For example, if one's password is leaked and the webpage is edited to remove the password, Dorking can be used to pull up the old webpage to still access it. Other Google Dorks downright reveal lists of passwords, social security numbers, government information, sensitive documents, admin login pages, bank account details, phone numbers, and more. Some Google Dorks can be beneficial and seemingly innocuous when used for a good-faith purpose. However, the same operators can be exploited by malicious actors to commit cybercrimes.

More dangerous search operators reveal private and seemingly secure information, such as real-time feeds from security and personal cameras. Search "'Google — intitle:[….]' and you will find a list of webcams you can dive right into",[9] without the victims ever knowing. The article "Somebody's Watching: Hackers Breach Ring Home Security Cameras" reveals an authentic photo of a child's

[8] *Refine web searches, Google Search Help,* Google, https://support.google.com/websearch/answer/2466433?hl=en.

[9] Gourav Dhar, *Finding Vulnerable Info Using Google Dorking – Ethical Hacking*, Medium: INFOSEC WRITE-UPS (Apr. 3, 2022), https://infosecwriteups.com/finding-vulnerable-info-using-google-dorks-ethical-hacking-23f358117ceb.

bedroom as seen from a hacked ring camera[10]: "There have been at least three similar cases reported this month… Other breaches, involving … a baby monitor sold on Amazon, have also… prompted concerns about privacy." Id. The Ring hacks were among the countless webcam hacks conducted through Google Dorking. Ring's security team found "no evidence of an unauthorized intrusion or compromise of Ring's systems or network", stating the devices were hacked from malicious actors gaining log-in credentials. Id. These are clear instances of Google Dorking and how it could be used to access sensitive private information. Hackers likely found the exposed log-in credentials via Dorking and found the vulnerable servers in the same way. The article quotes Johnny Long, an early pioneer of Google Dorking: "In the years I've spent as a professional hacker, I've learned that the simplest approach is usually the best. As hackers, we tend to get down into the weeds, focusing on technology, not realizing there may be non-technical methods at our disposal that work as well or better than their high-tech counterparts. I always kept an eye out for the simplest solution to advanced challenges."[11] Devices are getting hacked with increasing frequency[12] as a result of hackers utilizing these non-technical methods. Innumerable advanced queries create the perfect playground for cyber criminals.

The ordinary Google User merely accesses the tip of the iceberg. Google Dorking transformed the world of cybercrime by allowing the addition of punctuation marks and words to alter the information one receives from the same public tool accessible to everyone. The ease of Dorking provides any Google User with the capability to commit cybercrimes. "Hackers" no longer need technical experience or training. This accessibility has increased the quantity of cybercrimes enormously,[13] as Dorking allows the average person to access information that should be confidential. The act of hacking is now easier to commit, harder to prosecute, and no longer understood and covered by the law.

[10] Neil Vigdor, *Somebody's Watching: Hackers Breach Ring Home Security Cameras*, The New York Times (Dec. 15, 2019), https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html.

[11] *Id.*

[12] Rob Sobers, 166 cybersecurity statistics and trends Varonis (Jul. 8, 2022), https://www.varonis.com/blog/cybersecurity-statistics (last visited Jan 30, 2023).

[13] Beyond Identity Blog, *How has a decade of cybercrime impacted the United States? [study] The Rise of Cybercrime in the US [Study]* | Beyond Identity (Aug. 30, 2021), https://www.beyondidentity.com/blog/rise-cybercrime-study

The Evolution of Google Dorking

Johnny Long is a computer security expert known as the "Father" of Google Dorking.[14] While conducting research to protect servers against hacking while working with the CSC (Computer Sciences Corporation)'s strike force (the corporation's vulnerability assessment),[15] Johnny began to discover and compile Google Search queries capable of finding vulnerable servers.[16] Over time, he noticed these queries also found servers that post sensitive information publicly, such as credit card and social security numbers.[17] Word of these queries spread; others began utilizing them and discovering new ones. The collection of these specific queries became known as the Google Hacking Database,[18] where hundreds of queries were posted for the public around 2004.[19]

Individuals began exploiting other search engines such as Bing[20] and Shodan[21] similarly.[22] "Dorking, it is not something exclusive to Google. Other search engines like Bing or DuckDuckGo also work with this technique."[23] The use of advanced search operators on various engines is known as "Search Engine Hacking". Id. This is important because although Google Dorking is a massive problem that the law fails to address, it is part of a much larger issue. Search engines can be utilized maliciously, and there is a lack of regulation around this.

Dorking was the steppingstone of a transformation in cybercrime, creating large loopholes in cybersecurity and hacking laws. Updating the law to recognize and regulate Google Dorking

[14] Johnny Long, https://en.wikipedia.org/w/index.php?title= Johnny_Long&oldid=1095071400 (last visited Sept. 20, 2022).

[15] *First Hand Interview with Johnny Long,* CSC World, Sept. 2008, at 14.

[16] *See* Wikipedia, *Johnny Long*, https://en.wikipedia.org/wiki /Johnny_Long (last visited Sept. 20, 2022).

[17] *Id.*

[18] Johnny Long, *GHDB*, IHS, (Aug. 8, 2009, 11:57 AM), https://web.archive.org/web/20090808115759/http:/johnny.ihackstuff.com/ghdb/.

[19] *Id.*

[20] Paul Roberts, *Google, Bing: A hacker's best friends*, INFOWORLD (Aug. 2, 2010, 6:50AM), https://www.infoworld.com /article/2624407/google--bing--a-hacker-s-best-friends.html.

[21] Uladzislau Murashka, *Shodan – unique online search engine for vulnerable systems*, SCAN FOR SECURITY (Sep. 6, 2017), https://www.scanforsecurity.com/scanners/shodan.html.

[22] *Google Hacking*, WIKIPEDIA (Sep. 14, 2022), https://en.wikipedia.org /w/index.php?title=Google_hacking&oldid=1110261984.

[23] George Lanington, *What is Google Dorking*, DIGIS MAK (Sep. 10, 2022), https://digismak.com/what-is-google-dorking/.

will create a ripple effect in regulation, safety, and security. The increasing use of technology highlights the need to reevaluate the Computer Fraud and Abuse Act (CFAA), which criminalizes "hacking" and the unauthorized access to computers and computer systems. A more detailed examination of the CFAA will be discussed later in the paper.

Google Dorking in Case Law

Prior to this publication, just one case publicly noted a hacker's use of Google Dorking: the Bowman Avenue Dam Hack in New York. The scarcity of public discourse on Dorking belies how widespread this method is among cybercriminals. This one instance confirmed the hypothesis that hackers are using this method to commit major crimes without awareness from the justice system. Subsequent research uncovered a wide variety of seemingly unrelated cybercrimes with one thing in common: Google Dorking. The remaining cases cited in this publication were determined to involve Google Dorking through additional research and analysis.

I. THE DANGERS OF GOOGLE DORKING ON PUBLIC SAFETY AND PRIVACY

The first case involving Google Dorking is the hack of the Bowman Avenue Dam in New York It is also the only instance when investigators have acknowledged the use of Google Dorking by name. From 2011 to 2013, a string of cybercrimes occurred on 46 major United States institutions; however, one stood out to the public and sparked further curiosity: "Hamid Firoozi was charged for 'obtaining unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam.'"[24] Investigators, the public, and United State officials were shocked to learn that Firoozi gained access "by scanning the internet", identifying vulnerable servers, and targeting the Bowman Avenue Dam. What appeared to be a technical and difficult hack was far simpler: Firoozi "googled it".[25] Former F.B.I. computer crime investigator Mike Bazzell said, "This stuff has been happening

[24] Press Release,, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*, UNITED STATES DEPARTMENT OF JUSTICE (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.

[25] Julie Bort, *Something called 'Google dorking' helps hackers find out stuff no one wants them to know*, YAHOO! SPORTS (Apr.1,2016) https://sports.yahoo.com/news/something-called-google-dorking-helps-183530092.html.

undetected for years, and now this is one of the first times that it's surfaced publicly."[26] Experts speculated that this would not be the last time we would hear of incidents with this hacking technique: "it's more likely than not that we'll see more cases like the hacker's exploit of the Bowman Avenue Dam in the years to come."[27] This was the first and the last case to reference Google Dorking. But that does not mean that this criminal method is obsolete. In fact, quite the opposite has occurred. Other cases of Google Dorking remain improperly identified and handled.

Perhaps the most shocking instance is the compromise of the CIA's worldwide secret communications network, which has been referred to as "one of the most catastrophic failures since Sept. 11."[28] This incident resulted in the execution of at least 60 assets and the compromise of 70% of CIA networks worldwide. Simple, unsophisticated Google Dorks were the root cause of what is known as one of the biggest intelligence failures of the United States[29]: "Iranian agents used simple Google searches to identify and then infiltrate the websites that the CIA was using to communicate with agents… The breach would reportedly lead to dozens of deaths around the globe."[30] Specifically, the compromise allowed Iranian intelligence to identify and execute 30 CIA spies in 2011,[31] and similarly allowed the Chinese government to arrest and execute another "30 people working on behalf of the US between 2011 and 2012."[32] If the CIA is not safe from Google Dorking, neither is any other technology user in the United States.

International malicious cyber-attackers are not the only malicious actors that use Google Dorks. Cyberstalkers also

[26] , *New report: Sabotaging America's power grid is far easier than we were told*, OFF THE GRID NEWS, https://www.offthegridnews.com/current-events/new-report-sabotaging-americas-power-grid-is-far-easier-than-we-were-told/amp/ (last visited Oct 1, 2022).

[27] Doug Bernard, *Hackers Pick Up Clues from Google's Internet Indexing*, VOA (Apr. 1, 2016), https://www.voanews.com/a/hackers-clues-serach-engines-dorking-technology-cybersecurity/3265245.html.

[28] *Report claims Iran Busted CIA's Secret Communication System Using Google Search*, Sputnik International (Mar. 11, 2018, 7:51 AM), https://sputniknews.com/20181103/iran-busted-cia-network-report-google-1069474391.html.

[29] *Id.*

[30] Benjamin Goggin, *Iran Reportedly Used Google to Crack a CIA Communications System, Leading to 'Dozens' of Deaths*, Task & Purpose(Nov. 3, 2018, 3:09 PM), https://taskandpurpose.com/news/iran-cia-communications/.

[31] Sean Gallagher, *How did Iran find Cia Spies? They googled it*, Ars Technica (Nov. 2, 2018, 11:26 AM), https://arstechnica.com/tech-policy/2018/11/how-did-iran-find-cia-spies-they-googled-it/.

[32] *Id.*

commonly use this method. Celebrities are often targets of stalking, which is increasingly easier to do with Google Dorking. In 2013, an infamous 'sextortion' hack involving Miss Teen USA and approximately 150 other young females[33] utilized Google Dorking.[34] In August of 2013, Miss Teen USA Cassidy Wolf got an email of nude photographs taken from her own webcam by a hacker who had been watching her for over a year. He began to blackmail her and his other victims, attempting to force them to engage in Skype sessions with him to avoid their photographs being released publicly. Also in 2013, hackers stole and published social security numbers, phone numbers, and financial information of celebrities including Joe Biden, Michelle Obama, Hillary Clinton, Sarah Palin, Beyoncé, Kim Kardashian, Britney Spears, Donald Trump, and more.[35] The hack received significant publicity due to a disconcerting realization: if Presidents and first ladies of the United States and our most affluent celebrities can be hacked and exposed via Google Dorking, who among the rest of us is safe?

The Miss Teen USA sextortion hacks were not the only cases to involve webcam or security cam access through Google Dorking. In fact, webcams are some of the easiest targets to hack via Google Dorking, and countless institutions, buildings, and security systems have become compromised due to this. For example, more than 150,000 Verkada security cameras in Tesla factories, jails, medical centers and more were accessed through Google Dorking[36]: "The hackers' methods were unsophisticated: they gained access… through a 'Super Admin' account, allowing them to peer into the cameras of all its customers."[37] They found these log-in credentials

[33] Alyssa Newcomb, *FBI Investigating 'Sextortion' Case Involving Miss Teen USA Cassidy Wolf*, ABC NEWS (Aug. 15, 2013), https://abcnews.go.com/blogs/headlines/2013/08/fbi-investigating-sextortion-case-involving-miss-teen-usa-cassidy-wolf (last visited Oct 1, 2022).

[34] Kathakali Banerjee, *Google Hacking: How to save yourself from Google Dorking,* DIGIT (Apr. 12, 2016, 5:52 PM), https://www.digit.in/features/general/google-hacking-how-to-save-yourself-from-google-dorking-29755.html.

[35] Maria Puente, *Old crime of celeb-hacking reaches new level of spying*, USA TODAY (Mar. 12, 2013, 1:33 PM), https://www.usatoday.com/story/life/people/2013/03/12/old-crime-of-celeb-hacking-reaches-new-level-of-spying/1981949/.

[36] Andrea Vittorio & Jake Holland, *Surveillance Camera Hack Raises Legal Risk of Digital Device Use*, BLOOMBERG LAW (Mar. 15, 2021, 2:00 AM), https://news.bloomberglaw.com/privacy-and-data-security/surveillance-camera-hack-raises-legal-risk-of-digital-device-use.

[37] Nick Heer, *Surveillance and Facial Recognition Systems From Verkada Breached*, PIXEL ENVY (Mar. 9, 2021), (*quoting* William Turton, Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals, Bloomberg (Mar. 9, 2021, 1:32 PM)); (*quoting* Joseph Cox & Jason Koebler, Hacked Surveillance

publicly exposed on the internet.[38] Kottmann, the activist hacker (A/k/a "hacktivist") who hacked Verkada to raise awareness of the dangers of the vulnerabilities, credited Google Dorking for the hacks: "With just simple Google dorks, when I'm bored, and I keep being amazed by how little thought seems to go into the security settings."[39] This hacker's admission to using Google Dorking to perform his hacks, along with other security professionals' statements reiterating the need for change in legislative efforts due to these hacks,[40] highlight an opportunity to regulate.

Google Dorking is a tool that is also commonly used by criminals to commit identity theft given the ease of access of personal and private information online. One instance occurred in 2008, when Elmer Nanquilada was charged with aggravated identity theft because he knowingly used the identity of another person[41] with the help of Google Dorking. He used the identity in relation to committing bank fraud, a felony, and social security fraud. In his home, a detective located a notebook with "Google Hacking" written on top of one of the pages,[42] proving that the hacker studied Google Dorking techniques and used them to commit these crimes. Despite the notebook entry being noted in an official court document, Google Dorking was never mentioned again or scrutinized for how it played a role in those crimes.

Hackers further utilize Dorking to commit theft. Aside from the daily individual hacks of log-in credentials allowing hackers to access bank accounts, credit cards, and other sensitive financial data, there are large-scale hacks causing millions of dollars in damages to United States financial institutions. From 2005 through 2012, international hackers were responsible for several of the largest data breaches and exploits, hacking many of the largest retailers, financial

Camera Firm Shows Staggering Scale of Facial Recognition, VICE (Mar. 9, 2021, 3:45 PM)), https://pxlnv.com/linklog/verkada-breach/.

[38] James Vincent, *'Anti-capitalist' Verkada Hacker charged by US government with attacks on dozens of companies,* THE VERGE (Mar. 19, 2021, 4:17 AM), https://www.theverge.com/2021/3/19/22339625/tillie-kottmann-swiss-hacker-verkada-charged-us-government-verkada.

[39] Catalin Cimpanu, *Mercedes-Benz onboard logic unit (OLU) source code leaks online*, ZDNET (May 18, 2020), https://www.zdnet.com/article /mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/.

[40] Andrea Vittorio & Jake Holland, *Surveillance Camera Hack Raises Legal Risk of Digital Device Use,* BLOOMBERG LAW (Mar. 15, 2021, 2:00 AM), https://news.bloomberglaw.com/privacy-and-data-security/surveillance-camera-hack-raises-legal-risk-of-digital-device-use.

[41] United States v. Nanquilada, No. CR08 0323TSZ, 2008 WL 6874717, at *3–4 (W.D. Wash. Sept. 24, 2008).

[42] *Id.*

intuitions, and payment processing companies in the United States. They stole personal information, passwords, and over 160 million credit card numbers. Corporate victims included NASDAQ, 7-Eleven, JCPenney, JetBlue, Visa, Discover, and more. Just three of the corporate victims suffered combined losses in excess of $300 million.[43] In the Second Superseding Indictment, Google Dorking is implicated multiple times. When discussing how the hackers scouted their victims, it is noted that they researched websites and publications "to find corporations that engaged in financial transactions",[44] and they further investigated vulnerabilities in the websites that they found through research. Google Dorking is what hackers use to find these types of vulnerabilities to exploit. Additionally, conversations between the hackers in the court documents referred to basic Google Dork operators: "'I have triggers set on Google news for… "data breach" "credit card fraud" "debit card fraud"'.[45] This mention of the exact text quote search on Google makes it clear that these hackers knew of and used Dorking for these major cyber-attacks. It is far too simple to conduct these hacks and gain access to credit cards and bank log-in information from millions across the world. These are no longer dangers we can protect ourselves from because technology is intertwined with every aspect of life, and the combination of increasing reliance on digital assets while legislation lags behind creates a major security concern.

Judges themselves have also been targets of crimes committed through Google Dorking. Ester Salas, a judge of the District Court of New Jersey, became a victim of this hacking technique in 2020 when a gunman who once appeared in Judge Salas' court disguised himself as a delivery driver and appeared at her home which he found via Google Dorking. He opened fire, murdering her son Daniel and wounding her husband. Judge Salas later began to advocate for increased privacy protections for judges.[46] Judge Salas was not the first or last judge to suffer the consequences of Google Dorking. In 2022, after public outrage over the decision that overturned Roe v.

[43] *See* Second Superseding Indictment at 1, United States v. Drinkman, (D.N.J. 2013) No. 09-626, 2013 WL 10196105.

[44] *Id.*

[45] Bob Sullivan, *160 million credit cards later, 'cutting edge' hacking ring cracked*, NBCNEWS.COM (Jul. 25, 2013), https://www.nbcnews.com/technolog/160-million-credit-cards-later-cutting-edge-hacking-ring-cracked-8c10751970 (last visited Oct. 3, 2022).

[46] *Booker, Menendez Applaud Senate Judiciary Committee passage of bipartisan bill to Protect Privacy, safety of federal judges and their families,* U.S. SENATOR CORY BOOKER OF NEW JERSEY: HOME (Oct. 3, 2022), https://www.booker.senate.gov/news/press/booker-menendez-applaud-senate-judiciary-committee-passage-of-bipartisan-bill-to-protect-privacy-safety-of-federal-judges-and-their-families.

Wade, many young people were angry with the Supreme Court Justices. Several young adults on Tik Tok[47] found and posted the personal information of the Supreme Court Justices online, a practice referred to as "doxing".[48] There were reports of Justice Clarence Thomas' credit card number being leaked,[49] and TikTok users were posting content containing home addresses of six Supreme Court Justices. Some of the addresses were confirmed to be accurate, leading to protests outside of the Justices' homes.[50] Many were concerned about how regular kids were able to easily find such private information so quickly, speculating different methods that may have exposed this data.[51] Google Dorking could easily have been the technique utilized in these incidents, given that it is accessible to individuals with non-technical backgrounds and so simple that children could do it. If Justices can fall victim to Google Dorking and children can do real damage with this method, then anyone can be a hacker, anyone can be a victim, and absolutely no one is safe.

II. IS GOOGLE DORKING LEGAL?

The main issue this article addresses is also the most searched question on Google regarding Google Dorking: "Is Google Dorking legal?" To find out, we must first discuss the most significant federal law in the war against hacking: the Computer Fraud and Abuse Act (CFAA).

The Computer Fraud and Abuse Act "CFAA"

The federal law that governs most computer crimes including hacking, is the CFAA. Title 18 § 1030 states that "whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any

[47] TikTok is a social media platform where users create and share short-form videos. It is known for its algorithmic recommendation system and the ability for users to create, discover, and engage with a diverse range of content. TikTok has become a popular platform, particularly among younger generations, and has been adopted worldwide.

[48] Jules Roscoe, *TikTok users are doxing the Supreme Court*, VICE (June 29, 2022, 11:39am), https://www.vice.com/en/article/v7vmpm/tiktok-users-are-doxing-the-supreme-court.

[49] Dan Evon, *Was Clarence Thomas' Credit Card Number Leaked on TikTok?,* SNOPES (Jun. 29, 2022), https://www.snopes.com/fact-check/clarence-thomas-credit-card-leaked/.

[50] *Id.*

[51] *Id.*

protected computer[52]... shall be punished"[53] §1030(a)(2)(C) by fine or imprisonment.[54, 55]

The CFAA was enacted in 1986 as an amendment to the first federal computer fraud law to address hacking.[56] Over time, this rule has expanded to encompass new technological advances and has redefined old terms stated within the statute to better fit evolving issues in cybercrime. The CFAA was originally intended to protect computers belonging to the United States Government and financial institutions.[57] However, the scope of the CFAA has expanded to shift the term of "protected computer" to effectively cover "any computer connected to the internet… including servers, computers that manage network resources and provide data to other computers."[58]

This statute remains a broad and vague provision that allows for an enormous amount of legal gray area, inconsistent application of the law, diminished understanding of what is legal , and lack of confidence from the public that justice will be served when they are victims of cybercrimes.[59] The CFAA states, "evidence mounts that existing criminal laws are insufficient to address the problem of computer crime."[60] This insufficiency remains true despite multiple revisions made on this vague, overbroad, and unclear statute. Technology is one of the most rapidly evolving fields, and the law is falling behind.

1. Google Dorking Under the Computer Fraud and Abuse Act

Upon reviewing the federal law that regulates hacking and computer crimes, the question arises of whether Google Dorking is legal. To analyze this, we must first define whether the activity of Google Dorking is considered hacking. The CFAA fails to directly address search Engine Hacking and falls short of properly regulating

[52] 18 U.S.C. § 1030(a)(2)(C)

[53] hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. 2017), *aff'd and remanded*, 938 F.3d 985 (9th Cir. 2019), *cert. granted, judgment vacated*, 210 L. Ed. 2d 902, 141 S. Ct. 2752 (2021), and *aff'd*, 31 F.4th 1180 (9th Cir. 2022).

[54] Order RE: Plaintiffs' Motion for Preliminary Injunction, Universal City Studios Prods. LLLP v. TickBox TV LLC, (C.D. Cal. Jan. 30, 2018) No. CV 17-7496-MWF (ASx), 2018 WL 1568698, at *9.

[55] 18 U.S.C. § 1030 (2013) (Proquest through Pub. L. No. 99-474).

[56] *Computer Fraud and Abuse Act (CFAA)*, NACDL - NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct (last visited Sept. 20, 2022).

[57] *Id.*

[58] hiQ Labs, Inc., 273 F. Supp. 3d at 1099.

[59] Universal City Studios Productions LLLP, 2018 WL 1568698, at *9.

[60] Computer Fraud and Abuse Act of 1986, S. Rep. No. 99-432, at 2, as reprinted in 1986 U.S.C.C.A.N. 2479, 2479.

all of the various issues in hacking. Today, along with technology becoming more prevalent, the methods of hacking are expanding as well[61]: "Although the CFAA states that hacking is intentionally accessing a computer without authorization or exceeding the authorization… there are now additional ways for individuals who are not trained hackers, to access and obtain information that they are not supposed to access."[62] This quote refers to acts like Google Dorking, which does not fit into the definition of "hacking" under the CFAA because accessing public information through Dorking does not require exceeding authorized access or accessing something without authorization.

Although Google Dorking would not be considered "hacking" under the CFAA according to its language, it is important to note how commonly it is referred to as an act of hacking in government documents and publications. The Office of Intelligence and Analysis and FBI stated that Google Dorking is "also known as 'Google Hacking,'[63] and many contributors to Dorking have utilized these terms interchangeably as well.[64] Johnny Long himself, the creator of Google Dorking, released books titled 'Google Hacking for Penetration Testers'".[65] The public, cybersecurity community, and creators of Google Dorking all view the act as some form of hacking.

Google Dorking would not be considered "hacking" under the CFAA's language, but the question remains as to whether it is treated as legal in court: "Although it may seem intimidating, Google Dorking is not an illegal activity."[66] Per the CFAA, access to publicly available information is legal, despite public and cyber opinion regarding Dorking. The cases in which courts treat Google Dorking as illegal usually involve another statute or part of the CFAA, not just Dorking itself. Each of the cybercriminals noted above was charged for wrongdoing after Dorking, such as selling personal information, stealing, or hacking SCADA systems or webcams. Thus, Google Dorking as a standalone act remains legal, but it could still facilitate crime resulting in criminal prosecution.

[61] Universal City Studios Productions LLLP, 2018 WL 1568698, at *9.

[62] *Id.*

[63] OFFICE OF INTELLIGENCE AND ANALYSIS, *Malicious Cyber Actors Use Advanced Search Techniques* (2014), https://info.publicintelligence.net/DHS-FBI-NCTC-GoogleDorking.pdf.

[64] *Id.*

[65] *Johnny Long*, WIKIPEDIA, https://en.m.wikipedia.org/wiki/Johnny_Long&sa=D&source=docs&ust=1656887386055423&usg=AOvVaw0IE1W0enOCohu9xK0i-L9C (last visited Jul 3, 2022).

[66] Lance Vaughn, *What Is Google Dorking*, RUETIR (Oct. 3, 2022), https://www.ruetir.com/2022/09/10/what-is-google-dorking/.

II. THE DANGERS OF LEGAL AMBIGUITY REGARDING GOOGLE DORKING

Aside from concerns of compromised privacy through Google Dorking, there are additional concerns for the average Google User, White Hat Hackers, and Journalists relating to Due Process, and our rights as citizens of the United States.

Vagueness of the Computer Fraud and Abuse Act

The Fifth Amendment states that no one shall be "deprived of life, liberty, or property without due process of law."[67] Due Process refers to the fair treatment of citizens in the justice system. The Supreme Court applies the Due Process Clause to the prohibition of vague laws which can interfere with citizens' fair treatment under the law and allow for discriminatory enforcement.[68] A statute may fail to reach the standards of Due Process if it is "so vague and standardless that it leaves the public uncertain as to the conduct it prohibits."[69] A statute is further "void for vagueness" and unenforceable when it is "too vague for the average citizen to understand."[70] As discussed earlier, the CFAA is inherently vague, confusing, and misleading.
The 'hacktivist'[71] group Anonymous made a statement about the vagueness of the CFAA, referencing the "erosion of due process, the dilution of constitutional rights [and] the usurpation of the rightful authority of courts by the 'discretion' of prosecutors."[72] They additionally note that "the federal sentencing guidelines… enable prosecutors to cheat citizens of their constitutionally-guaranteed right to a fair trial, by a jury of their peers… in clear violation of the 8th Amendment protection against cruel and unusual punishments."[73] Google Dorking falls under the umbrella of vague, overbroad computer-activities that the Justice System can stack CFAA charges on. Hacktivists, journalists and curious Google users are at risk from

[67] U.S. CONST. amend. V.

[68] City of Chicago v. Morales, 527 U.S. 41, 56, 119 S. Ct. 1849, 144 L. Ed. 2d 67 (1999).

[69] Hoffman v. United States, 256 A.2d 567 (D.C. 1969).

[70] *Vagueness Doctrine*, https://en.wikipedia.org/w/index.php?title= Vagueness_doctrine&oldid=1113430826 (last visited Oct. 25, 2022).

[71] A "hacktivist" is a person who uses hacking to promote a political or social agenda. This term is a combination of the words "hacker" and "activist," and refers to individuals that use technology to protest against perceived injustices or to bring attention to specific issues.

[72] *American authorities charge UK Man With Hacking Army, Missile Defense Agency and NASA websites*, RT INTERNATIONAL, https://www.rt.com/usa/lauri-love-anonymous-lastresort-853/ (last visited October 14, 2022).

[73] *Id.*

the constitutional violations that the CFAA creates in the Justice System. Since Google users are unaware of what searches are prohibited, and the court holds full discretion as to how to interpret and apply the law, the CFAA is dangerous for citizens' constitutional rights under the Due Process Clause.

The Department of Justice (DOJ) announced in May of 2022 that they will not prosecute individuals involved in "solely 'good faith' security research."[74] The revision remains vague, maintaining discretion within the Justice System regarding how research is classified. For example, courts can make independent determinations on whether research was conducted "exclusively" to test security without any ulterior motives such as making money, which is what White Hat Hackers do. The "DOJ policy fails to provide concrete, detailed provisions to prevent the CFAA from being misused to prosecute beneficial and important online activity."[75] The DOJ's rules are neither permanent nor binding on courts. Cybersecurity specialist Orin Kerr stated, "it's just a policy, not a law, so it's just something to guide prosecutorial discretion and doesn't create any rights in court."[76] Furthermore, the rules do not reduce the risk of frivolous CFAA lawsuits against journalists, security researchers, and Google users[77]. "The policy is a good start, but it is no substitute for comprehensive CFAA reform."[78]

Legality of Accessing Public Information

In *hiQ Labs v. LinkedIn*, the Federal District Court differentiated cases that discuss access to "public data" from older CFAA cases regarding alternate types of "hacking."[79] The court stated that the CFAA was not "intended to police traffic to publicly available websites on the internet",[80] and the court clarified that access to websites which require password authentication for access is

[74] Andrew Crocker, *DOJ's New CFAA Policy is a Good Start but does not go Far Enough to Protect Security Researchers.* ELECTRONIC FRONTIER FOUNDATION (June 6, 2022), https://www.eff.org/deeplinks/2022/05/dojs-new-cfaa-policy-good-start-does-not-go-far-enough-protect-security.

[75] Andrew Crocker, *DOJ's new CFAA policy is a good start but does not go far enough to protect security researchers, Electronic Frontier Foundation* (June 6,2022), https://catalyst.independent.org/2022/06/02/doj-cfaa-policy/.

[76] *Department of Justice: We Won't Sue "Good Faith" Hackers, Promise, Maybe*, THE STACK (May 20, 2022), https://thestack.technology/department-of-justice-we-wont-sue-good-faith-hackers-but/.

[77] Crocker, *supra* note 73.

[78] *Id.*

[79] hiQ Labs, Inc., 273 F. Supp. 3d 1099.

[80] *Id.*

unauthorized.[81] Although scholars and courts appear to agree that the CFAA is intended to exclusively limit access to non-public data, real-world cases have played out differently.

The Verkada[82] hacker, Kottmann, was a hacktivist[83] with a passion for educating the public on how easy it is to "hack" and gain data and information online. According to Kottmann, weak security standards at Kottmann's targeted companies allowed them to find data for their hacks. Kottmann talked openly in interviews about how they obtained sensitive data by using Google Dorks with the intention of exposing companies' lack of cyber security before malicious actors exploited it.[84] Kottmann stated that they "only search... often with simple Google Dorks, when I get bored and I am always amazed that there seems to be little thought on defense."[85] While Kottmann's actions paralleled many cyber researchers and White Hat Hackers, they wanted to warn the world rather than merely inform companies privately.

Kottmann's web-searching activities appear to have been motivated by innocent curiosity. But the United States Government viewed the situation differently.[86] The government found that "as of March 2021, Kottmann has hacked dozens of companies and government agencies and... published internal files and records... for public review and download".[87] The court equated their hacktivism with "knowingly and willfully… commit[ing] offenses against the United States" and the act of "intentionally access[ing] computers without authorization,… in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(ii) and (iii)."[88] For Google Dorking and exposing dangers to the public, Kottmann was indicted

[81] *Id.*

[82] Verkada is a video security company that develops cloud-based security systems for various buildings.

[83] A "hacktivist" is a person who uses hacking to promote a political or social agenda. This term is a combination of the words "hacker" and "activist," and refers to individuals that use technology to protest against perceived injustices or to bring attention to specific issues.

[84] James Vincent, *'Anti-capitalist' Verkada Hacker Charged by US Government with Attacks on Dozens of Companies,* THE VERGE (Mar. 19, 2021), https://www.theverge.com/2021/3/19/22339625/tillie-kottmann-swiss-hacker-verkada-charged-us-government-verkada.

[85] *Id.*

[86] *Verkada Hacker Indicted on 8 Counts of Computer Crimes and Fraud,* NETSEC.NEWS (Mar. 25, 2021), https://www.netsec.news/verkada-hacker-indicted-on-8-counts-of-computer-crimes-and-fraud/.

[87] United States v. Till Kottmann, U.S. District Court W.D. Wash., Case 2:21-cr-00048-RAJ, Indictment, filed Mar. 18, 2021 https://www.justice.gov/usao-wdwa/press-release/file/1377536/download.

[88] *Id.*

on eight counts of computer crimes and fraud, and as of October 2022 they are facing up to 27 years in prison.[89]

It is not just White Hat Hackers, journalists, and researchers who have due process rights at risk from obtaining publicly accessible data, but also average United States citizens. A curious internet user who goes by the name "Kim", was arrested in a separate incident for collecting publicly accessible data through Google Dorking from 2010 to 2012.[90] It should be noted that he did not "hack any websites."[91] Rather, he used Google to locate names, resident registration numbers, addresses, and other information. After collecting data out of "curiosity, without any specific purpose",[92] he was arrested for gathering and posting information that was already public.[93] As the case illustrates, the CFAA poses risks to oblivious citizens of being prosecuted for hacking if they simply find and use data already available to the average Google user.

III. WHAT SHOULD BE DONE TO PROTECT US?

1. Should Google Dorking be Legal?

To restore our privacy and security, we need to update the law to avert crimes from Google Dorking. A change in federal law is vital since the cases discussed herein are the tip of an iceberg of countless misinterpreted or uncharged cases. By leaving the law as is, we are allowing hackers and malicious actors to access our entire lives without our consent. Although government regulations could be viewed as a threat to free speech and freedom, the lack of freedom occurs when we lose our rights to our identities, our property, and our sensitive personal information. We are prisoners to those online who want to maliciously take advantage of us without our knowledge.

The use of Google Dorking to access private and sensitive information should be illegal and clearly outlined in the law because of the harms caused by exposing personal information to strangers, including addresses, social security numbers, and credit card

[89] Netsec Editor, Verkada Hacker Indicted on 8 Counts of Computer Crimes and Fraud, NETSEC.NEWS (2021), https://www.netsec.news/verkada-hacker-indicted-on-8-counts-of-computer-crimes-and-fraud/ (last visited Oct 15, 2022).

[90] 희 신현, *Reclusive Man Arrested for Collecting Data of 8.84 M People Using Google*, THE KOREA HERALD (2012), http://www.koreaherald.com/view.php?ud=20121030001124 (last visited Oct 3, 2022).

[91] *Id.*

[92] *Id.*

[93] *Id.*

numbers. As long as it remains improperly regulated, stalkers, cybercriminals, and thieves can access webcams, home addresses, credit card numbers, social security numbers, and more online without any deterrence or fear of prosecution. In this technological age, freedom of information should include reasonable limits to personal and private data. If the sensitive data can be accessed only by government entities, journalists, or good faith researchers, then the public should not have access to the data. There needs to be a clear indication of what is "legal" and "illegal" research, along with who can and cannot do it. Due to the fact that defensive hackers only need to use Dorking because it exists as a tool for criminals, its benefits for defensive ethical hackers are outweighed by its harms. Lastly, government officials should be required to obtain warrants to access sensitive information through Google Dorking to comply with the Fourth Amendment right to be free from unreasonable searches.

While Dorking can provide accurate and less filtered results, there are other methods to achieve the same or better results without irreparable damage. We should amend search engines to prioritize unbiased, unfiltered, and untainted information, so we do not have to "hack" their systems. It must be prohibited for search engines to provide inaccurate or biased search results or sponsored paid content intended to influence users who are seeking unbiased information. It is also imperative to prohibit search engines from allowing simple queries to display sensitive information not intended to be found online without the owner's permission. Laws must be changed to eliminate stalking, lack of safety, hacking of accounts, stealing of credit cards, and killings due to this practice.

2. What Could be Done to Protect us From the Public Safety and Privacy Dangers?

It is critical to create a new law to limit the crimes facilitated by Google Dorking, and to protect average citizens who often fall victim to these crimes without any knowledge, justice, or remedy.

A brand-new law is needed because even Google itself has failed to control Google Dorking, which it attempted by shutting down SOAP search API Keys. SOAP stands for Simple Object Access Protocol, and it is a standard messaging protocol for operating services to communicate. SOAP is also an Application Programming Interface (API) that allows applications to communicate as well.[94]

[94] Indeed Editorial Team, *What is Soap API?*, (Definition and benefits explained) Indeed (2021), https://uk.indeed.com/career-advice/career-development/what-is-soap-api (last visited Oct. 25, 2022).

The SOAP API keys were utilized to generate mass-scale Google Search Queries from 2006-2009 and shutting this down had a short-term effect. Even though this move limited mass-scale hacking tools, it proved to be ineffective against individual Google Dorkers.

White Hat Hackers and individuals in the private sector have taken numerous actions to stop Google Dorking as well. Dorking was recognized by the private sector early on, leading to the release of Foundstone SiteDigger v1 and the Google Hack Honeypot in 2004 and 2005, respectively. To protect website owners from potential Google Dorks that could attack their site, Sitedigger uses the Google Hacking Database and Google API to run Google Hacking signatures against specific websites. [95] Google Honeypot identifies hackers who attack through search engines by disguising itself as a vulnerable web application to get indexed by search engines, which is hidden from regular Google users but visible to Google Dorkers. [96] It then creates a file containing information about the hacker, such as their IP address, so website administrators can learn and build defenses against them. [97] The benefits of defensive tools like these can only be realized if one knows about Search Engine Hacking and is technologically proficient enough to utilize these tools. Thus, these tools are worthless to the majority of targets, and the average U.S. citizen.

Even with these efforts, hackers cannot be completely prevented from exploiting vulnerable files and using sensitive data. Despite the desire of the private sector, White Hat Hackers, online search engines, and victims of Google Dorking for guidance from the government on how to avoid Google Dorking, the advice given has been useless, often misleading, and sometimes even harmful. No solution has worked so far, and new legislation would provide transformative results. Regulation of Search Engine Hacking and addressing Google Dorking is long overdue. Privacy is a right. American citizens are entitled to be safe in their own homes, and secure with their financial and personal data.

3. What Could be Done to Protect Against Legal Ambiguity Regarding Google Dorking?

[95] *Defending yourself from Google hackers*, INFOSEC RESOURCES (May 31, 2012), https://resources.infosecinstitute.com/topic/defending-from-google-hackers/ (last visited Oct 24, 2022).

[96] *The "Google Hack" Honeypot,* GHH (last visited October 24, 2022), https://ghh.sourceforge.net/.

[97] *See Id.*

Setting clear standards around Search Engine Hacking will ensure more cybercriminals are stopped and prevent innocent people against unjust imprisonment. The legality of accessing public resources must be clarified to let Americans know when they are committing a crime or innocently researching.

The CFAA has been revised numerous times to fit our current definition of cybercrime, and there is an ever-growing number of scholarly writings on why revising the outdated CFAA is ineffective. In the CFAA, hacking is defined as unauthorized and exceeded access, not as access to publicly available information. A broadening of the CFAA to cover publicly accessible information would cause the definitions to depart so far from the intent and language of the statute that it would violate our due process rights. The revisions unfairly require citizens to evaluate constantly changing statute definitions to determine whether their behavior will impair their life, liberty, or property.

The CFAA revisions in May of 2022 are vague, confusing, and unjust, as anyone the government deems as a "bad faith" actor, or even just short of "good faith", may be violating the law. This would suggest that curious citizens using Google to research their dates online before meeting them in person could potentially violate the law. To try to bend and mold the CFAA to handle every cybercrime would make it overly confusing and overreaching, and it would be potentially illegal and unjust due to the fact that it is open to the courts and individual judges' interpretations of intent. To address the legal ambiguity regarding Google Dorking and Search Engine Hacking, a new law is vital.

CONCLUSION

The benefits of Search Engine Hacking are considerable for White Hat Hackers, journalists, and innocent users alike, but the harms associated with allowing everyday users to access sensitive personal information need to be recognized and regulated properly. Although these benefits should be considered during the creation of new policy. The owners of personal data should be required to consent to the release of their data, and to be fully informed about how and where their data will be displayed. Personal data should be viewed only with the owners' specific consent and knowledge, and only on a case-to-case basis. Due to Google Dorking's ambiguous legal status, individuals are unaware of and unable to control hackers' access to their private information. Americans should have a reasonable expectation of privacy for information that they intend to keep private, such as their credit card numbers, addresses, and social security numbers. We must evolve alongside technological advances and ensure that cybersecurity law remains effective in protecting citizens of the United States. Bad actors sponsored or sanctioned by hostile countries are trained in Search Engine Hacking to access industrial and government secrets, extort financial, public, and government institutions, and commit theft and fraud against the United States, while we remain unaware and unable to defend ourselves. Educating lawmakers about this danger is vital to drafting and implementing new legislation. Legislation must be passed to regulate Search Engine Hacking and halt the damage that has occurred and will continue to proliferate until we address Google Dorking.