State-Sponsored Hash Searches & the Reasonable Expectation of Privacy

TIFFANY KU*

This Note examines whether, under the Fourth Amendment, the United States government can conduct searches based on hash encryption to comb through large digital databases such as the cloud and find files known to be incriminating. "Hashing" is an encryption process which assigns each encrypted file its own mathematically unique identifier called a hash value. The chances of two files having the same hash value is so improbable as to be almost impossible, unless the two files are exactly the same. A file with a minor edit, such as a document with one added period, will be assigned a completely new hash value by the algorithm. Thus, if two hash values match up, a person (or a computer) can know with certainty, without opening either file, that the files are exactly the same.

In the context of national security, hash values present a powerful opportunity to find criminal collaborators. If the government lawfully seizes one copy of a criminal plan, the government could then use hash searching to quickly identify co-conspirators by searching through the cloud for other accounts storing the same hash value. This Note considers whether the government can run hash searches on large databases without violating the Fourth Amendment. First, the Note locates hash searching within existing Fourth Amendment doctrine and discusses whether hash searches, particularly those conducted by computers, require a warrant. After examining whether existing warrant exceptions apply to hash searches it turns to consider, in the alternative, whether a warrant application based on a hash search could survive Fourth Amendment requirements such as particularity. The Note argues that hash searches fall under existing exceptions to the warrant requirement. In the alternative, hash searching's extreme object particularity will satisfy the warrant requirement even in the absence of particularity regarding target identity and file location.

* Senior Editor of the Supreme Court of California Blog by the California Constitution Center and *Hastings Law Journal*; J.D., University of California, Hastings College of the Law, 2017. Thank you to my Note supervisor, Professor Ahmed Ghappour, for his guidance. Thank you to the wonderful editors at the *Hastings Law Journal* for their support, and in particular the Editor in Chief for volume 69, Christa Hall. And thank you to Professor Jonathan L. Zittrain, George Bemis Professor of International Law at Harvard Law School, for the inspiration that sparked this Note.

TABLE OF CONTENTS

INTRODUCTION 29
I. A HASH SEARCH IS A DE MINIMIS INTRUSION ON PRIVACY INTERESTS 30
A. HASH SEARCHES EXIST IN A GREY AREA OF FOURTH AMENDMENT LAW 32
B. RE-DEFINING SEARCH AS "EXPOSURE TO HUMAN PERCEPTION" INSTEAD OF MERE "INTERACTION" 34
II. A BROAD WARRANTLESS HASH SEARCH IS REASONABLE AS A SUSPICIONLESS SEARCH WHERE THERE IS A LESSENED EXPECTATION OF PRIVACY 38
A. SEARCHING ALL OF COMPANY X'S USERS IS REASONABLE UNDER ROADBLOCK THEORY OF SUSPICIONLESS SEARCH 39
B. SEARCHING COMPANY X'S USER DATA NEEDS TO BE SUPPORTED BY LESSENED EXPECTATIONS OF PRIVACY 41
1. The Government Can Run Multiple Searches on Lawfully Seized Evidence 41
2. A Warrantless Search for Contraband Is Lawful, Particularly If the Search Method Only Alerts to Presence of Contraband 44
3. A Warrantless Search Through Metadata, Such as Hash Values, Is Lawful Under the Third-Party Doctrine 45
III. A SEARCH WARRANT FOR HASH SEARCHING COULD BE SUFFICIENTLY PARTICULARIZED 47
IV. CORPORATIONS ULTIMATELY HAVE A CHOICE IN COOPERATING WITH WARRANTLESS SEARCHES 49
CONCLUSION 50

INTRODUCTION

This Note discusses whether government investigators can use hash search techniques to identify files in corporate databases and focuses on potential issues at two stages of the process, warrant application and warrant execution. A hash search is an investigative technique which confirms that two files are the same by matching their "hash values." A hash value is an algorithmically generated value that is unique to a file. The chances of two files that are not the same sharing the same hash value are astronomically low. To ground our discussion of government hash searches, consider the following hypothetical:

"Company X" has millions of U.S. users for its web-based services, which include internet browsing, email, chat, and a multitude of other applications.[1] While it has many law-abiding users, there are some who use Company X's services for criminal purposes such as sharing and possessing child pornography. Company X knows these criminal users exist, but does not actively try to find them.[2] The government, however, wants to find all Company X users who own child pornography. To do so, the government wants to employ a search technique called "hash searching" on all of Company X's U.S. data, current and archived. The government also wants Company X to run the hash search on itself and report results back to the government because Company X has better technical search capabilities. Once Company X reported results to the government, government would immediately apply for arrest warrants, using the search results to provide probable cause.

First, does a search that touches all of Company X's U.S. users violate Fourth Amendment restrictions on unreasonable searches and seizures? Could the government conduct such a search without a warrant, or does it have to apply for a warrant? Second, should Company X comply with the government's search demands, or is Company X better served by resisting government cooperation?

This Note will address these questions in four parts. First, the Note will introduce hash searching and explain why hash searches should not be considered Fourth Amendment searches requiring a warrant. Second, the Note will consider whether the government can search all of Company X's databases warrantlessly, looking particularly at analogues in suspicionless search jurisprudence. Third, this Note will discuss whether the government could successfully make a warrant application for a drag net hash search. Finally, the Note will briefly contemplate Company X's role as a corporate policy-maker.

I. A Hash Search Is a De Minimis Intrusion on Privacy Interests

Hashing is a modern forensic data identification technique with high accuracy and a low false positive rate that is used to search through digital media.[3] The first step in a hash search occurs when a forensic

[1] For the purposes of this Note, I will assume that Company X's U.S. data is stored on U.S. servers, will set aside provisos in privacy laws which may limit the collection of user data (or assume that Company X meets the standards of those provisos).

[2] Internet Service Providers such as Company X are required by law to report to the government when they "obtain[ ] actual knowledge of any facts or circumstances" where there is an "apparent violation of" a federal criminal law against sexual exploitation of children. 18 U.S.C. § 2258A(a). But the law imposes no affirmative duty on ISPs to ferret out child pornography. United States v. Cameron, 729 F. Supp. 2d 418, 424 (1st Cir. 2012). Additionally, complying with this reporting requirement does not necessarily transform an ISP into a government actor if the government does not "instigat[e] or participat[e] in the search" or exercise "control . . . over the search and the private party." *See* UNITED STATES v. Pervaz*,* 118 F.3d 1, 6 (1997).

[3] Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38 (2006).

analyst takes a digital file and runs it through a complex mathematical algorithm to create a unique numerical identifier called a "hash value."[4] Many kinds of digital media can be hashed, from word documents and images to entire programs.[5] Further, the hash algorithm only works in one direction: "[O]ne can calculate a hash value from an input, but cannot derive the input from the hash value."[6] This means that the amount of information revealed in a hash value is extremely limited. A hash value cannot be reverse-engineered to reveal the original content before it was run through the hash algorithm, and hash values do not indicate anything about the type of information encrypted within. Next, the analyst actually conducts a hash search by comparing the hash value of a known digital file against hash values of unknown digital files.[7] Hash values only match when the two files are *exactly* the same.[8] Changing the contents of a file, even by a single letter, changes the entire hash value for that file, as demonstrated below.[9]

[4] *Id.*

[5] *See id.* at 41.

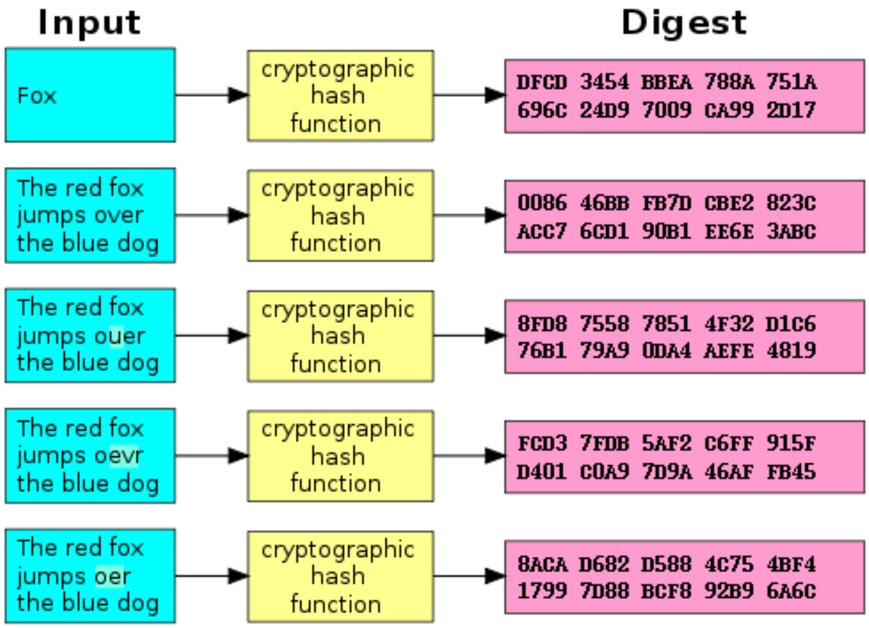
[6] *Id.* at 40.

[7] *Id.* at 40–41.

[8] *Id.* at 39.

[9] Salgado, *supra* note 3, at 39; *see also* Simson Garfinkel*, Fingerprinting Your Files*, MASS. INST. TECH. TECH. REV. (Aug. 4, 2004), https://www.technologyreview.com/s/402961/fingerprinting-your-files (See, embedded in the article, about half-way down, is a hash generator; users can see for themselves how changing a sentence by a single letter outputs a different hash value.).

Figure 1:


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C

Demonstrating how changing a single letter in the sentence "The red fox jumps over the blue dog" results in a completely different hash value.[10]

And so the search is complete. Hash searches, like other new technologies, have the potential to challenge and reform classic understandings of search and seizure because the privacy interests that are triggered by human searchers are not necessarily affected by digital eyes.

A. Hash Searches Exist in a Grey Area of Fourth Amendment Law

The Fourth Amendment seeks to protect citizens from broad, intrusive, and unchecked government interference, or "unreasonable searches and seizures."[11] A citizen's primary form of protection is the

[10] Sebastian Anthony, *How Dropbox Knows You're a Dirty Pirate, and Why You Shouldn't Use Cloud Storage to Share Copyrighted Files*, ExtremeTech (Mar. 31, 2014), https://www.extremetech.com/computing/179495-how-dropbox-knows-youre-a-dirty-pirate-and-why-you-shouldnt-use-cloud-storage-to-share-copyrighted-files.

[11] U.S. Const. amend. IV.

search warrant, which limits government action. The warrant must be particular, stating who will be searched, what will be searched, and what is being sought.[12]A warrant will be issued only if a judge finds "probable cause" to believe that the thing searched for will be where the warrant says it is.

A citizen's second form of protection is the "reasonable expectation of privacy" test. If the government searches or seizes evidence without a warrant, or otherwise acts beyond the authorized boundaries, courts will evaluate whether the fruit of that illegal search should be suppressed.[13] The standard for ex post review is the two-prong reasonable expectation of privacy test, established in 1967.[14] Evidence will be suppressed if (1) the government's actions intruded upon an individual's "actual subjective expectation of privacy" and (2) if that subjective expectation of privacy is one "society is prepared to recognize as reasonable."[15]

Modern difficulties in Fourth Amendment jurisprudence arise when courts are no longer sure what society considers a reasonable expectation of privacy because of technological disruption. These disruptions can be broad and societal, as with social media changing how individuals participate in each other's lives.[16] Disruptions can also be more technical, as in the so-called "seizure puzzle."[17] The seizure puzzle demonstrates the practical tension that arises when pre-computer standards that use analogies such as pen and paper are unable to fully adapt to new technologies involving clicking, dragging, and typing.

The crux of the seizure puzzle is a conflict between pure doctrinal interpretation and practical reality. To illustrate, consider that most digital investigations start with making mirror copies of seized hard drives, for practical purposes.[18] It is as if you copy-pasted everything

[12] Fed. R. Crim. P. 41(e)(2).

[13] Alderman v. United States, 394 U.S. 165, 177 (1968) (holding that nothing seen or found on premises as a result of an authorized search may legally form the basis for an arrest or search warrant).

[14] Katz v. United States, 389 U.S. 347, 361(1967) ("A 'search' does not occur—even when its object is a house explicitly protected by the Fourth Amendment—unless the individual manifested a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable."). *See also* Kyllo v. United States, 533 U.S. 27, 27-28 (2001).

[15] *Katz*, 389 U.S. at 361.

[16] Lower courts are probably doing more to reassess what reasonable expectations of privacy look like in the face of new technology; for example, Facebook has dramatically changed a generation's notions of privacy through it social media service, with founder Mark Zuckerburg even declaring that privacy was no longer a social norm in 2010. Yet, only one case challenging Facebook's effect on societal notions of privacy has reached the Supreme Court and it was denied certiorari. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 19, 2010, 8:58 PM) https://www.theguardian.com/technology/2010/jan/11/facebook-privacy; *see generally* Marek v. Lane, 134 S. Ct. 8 (2013). (denying petition for certiorari where challenge to class settlement following Facebook's invasion of user privacy "might not have afforded the Court an opportunity to address more fundamental concerns surrounding the use of such remedies in class action litigation.")

[17] Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 704 (2010).

[18] Salgado, *supra* note 3, at 40.

from one folder on a computer into another, so that the two are identical matches. Searches are usually run on the copy rather than the original, to ensure that any investigator error does not affect the original hard drive, which is preserved as seized.[19] Forensic analysts use hashing to confirm that the copy hard drive is exactly the same as the original.[20] This step is essential to ensuring the integrity of the files for later investigation.[21] However, it would have been unthinkable in 1967 (the year the seminal Fourth Amendment case *Katz v. U.S.* was decided) for investigators to photocopy a room full of documents to be searched later, in the leisure of the police department.[22] If boxes were taken away, some reasonable relation of the boxes' contents to the warrant issued was required.[23] But copying and verifying seized hard drives is such a preliminary investigatory step that it does not make sense to require a warrant. And if warrants were required, are separate warrants necessary for each piece of data copied, just as an agent scanning letters would have to justify copying each letter? The Supreme Court has not yet addressed this issue, but the practice of copying and hashing hard drives lives on in a grey zone. Practically speaking, investigators on the ground know that mirroring a hard drive for later examination is unlikely to be a violation of privacy because society's "reasonable expectation of privacy" has come a long way since 1967.

B. Re-Defining Search as "Exposure to Human Perception" Instead of Mere "Interaction"

One proposed solution to settling the "seizure puzzle" is adopting an "exposure" theory of Fourth Amendment search and moving away from a strictly "interactive" theory of search. The "exposure" theory defines search as the moment information is seen by human eyes (as through an output device like a monitor), and has the potential to reconcile Fourth Amendment jurisprudence with the realities of modern digital search.[24]

Interaction theory is well-illustrated by *Arizona v. Hicks*, which is the seminal case establishing the plain-view exception to the Fourth

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] See, e.g., *Nick v. Abrams*, 717 F. Supp. 1053, 1054 (S.D.N.Y. July 1989) (where defendant identified four cartons of materials responsive to the warrant, and then those cartons were seized; where defendant filed motion to suppress arguing that seizure had been too broad because investigators had seized materials unresponsive to the warrant. This suggests that the proper course of action would have been to examine materials on site before seizing them and taking them away.).

[23] *See generally* Stanford v Texas, 379 U.S. 476 (1965) (holding that a search was unconstitutionally broad and general where search of an office for Communist literature that resulted in seizure of forty-one boxes of non-Communist material).

[24] Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 547 (2005).

Amendment warrant requirement.[25] In *Hicks*, an officer had a warrant to search an apartment and seize any weapons.[26] While he was searching, he noticed an expensive stereo that seemed out of place.[27] Suspecting that it was stolen, the officer reached out and turned the stereo over to expose its serial number.[28] A later database check of the serial number confirmed that it was stolen property.[29] The U.S. Supreme Court held that the officer had illegally searched the stereo system when he manipulated the stereo to reveal the serial number because he only had "reasonable suspicion" to believe it was stolen rather than "probable cause."[30] This was because the officer had limited authorization for search and seizure (weapons) and could not act outside of that authorization unless the evidence, while in "in plain view," established "probable cause" for a warrantless search.[31] Here, more was needed to establish that the stereo was stolen goods.[32] *Hicks* illustrates interaction theory because the officer was at fault as soon as he manipulated the stereo. The holding would not change even if the officer hadn't found a useful serial number at the bottom. What mattered was the government had interacted with evidence outside of the warrant's authorized boundaries.

In the context of the seizure puzzle, interaction theory compels us to ask whether each file was searched when it was copied, even if it was never opened. This reaches back to *Hicks*, where it was the manipulation of the stereo that violated the privacy interests of the Fourth Amendment. Applying *Hicks* to hard drives narrowly focuses attention on the investigators' acts of copy and pasting, asking whether a superficial digital manipulation of a file constituted a search rather than asking the bigger question of "was a privacy interest harmed?" As computer programs become more integral to investigation, a more fruitful way of thinking about the seizure puzzle utilizes exposure theory.

Exposure theory argues that the search analysis should trigger later in the investigation, after the copy-pasting. The real privacy interest is violated not when files are manipulated by, or interacted with, by programs, but when files are exposed to human eyes and read. Exposure theory analogizes the hard drive to a "virtual warehouse" and looks to justifying seizing individual pieces of information from the warehouse.[33] This "focuses judicial attention on justifying the retrieval of evidence

[25] 480 U.S. 321 (1987).

[26] *Id.* at 323.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.* at 326.

[31] *Id.*

[32] *Id.* at 327.

[33] *Id.* at 539.

from computer storage devices" rather than on the necessary but distracting "behind the scenes" details of computer forensics.[34] Highlighting human perception as the moment of transgression also makes sense in an intuitive way since we commonly understand that things like secrets remain private until another person sees, hears, or perceives it. Under exposure theory, forensic analysts can copy hard drives without triggering the Fourth Amendment if no content is read or exposed by humans in the process of copying.

The difference between "interaction" as search and "exposure" as search is evident when comparing an agent rummaging through papers in file cabinets to a computer hash searching files on a hard drive.[35] The privacy consequences of an agent searching through a file cabinet are greater because agents and computers do not search in the same way. An agent searching a file cabinet has to read every file he touches to determine whether it falls under the warrant.[36] Even if an agent read no more than necessary and left with nothing but what the warrant authorized, the agent still exposes swathes of private information to scrutiny. Agents can even use warrants as a pretext to "go fishing" for leads.[37] Such general searches violate subjective expectations of privacy and are repugnant to society.[38] Accordingly, much of Fourth Amendment search jurisprudence has focused on limiting potential human abuse: agents are not allowed to indiscriminately search or seize every book on a shelf or every document in a file without justification.[39]

Computers running hash searches, on the other hand, only compare hash values and do not open or read the contents of rejected non-matching files.[40] A computer cannot engage in fishing expeditions, and

[34] *Id.* at 548.

[35] *See id.* at 537.

[36] Sometimes, human eyes go too far in diligently reading for evidence within the warrant's purview, rudely tearing away the veil of privacy from significant amounts of information. Computers simply cannot process information in a "malicious, voyeuristic, and self-indulgent" way. *See* United States v. Schandl, 947 F.2d 462, 465 (11th Cir. 1991) (denying motion to suppress even though "agents read love letters and seized personal documents, some of which were not relevant to these proceedings" and petitioner contended that agents went on a "malicious, voyeuristic, and self-indulgent rummaging" in their search of his home and office that went far beyond the scope of the warrants).

[37] *Cf.* United States v. Shilling, 826 F.2d 1365, 1370 (4th Cir. 1987) (denying motion to suppress documents seized wholesale because intent of seizure was not "to engage in a fishing expedition through [defendant's] papers" but to preserve legitimate practical concerns).

[38] Go-Bart Importing Co. v. United States, 282 U.S. 344, 357 (1931) ("Since before the creation of our government, such searches have been deemed obnoxious to fundamental principles of liberty.").

[39] *See generally* Stanford v. Texas, 379 U.S. 476 (1965) (holding that a search was unconstitutionally broad and general where search of an office for Communist literature that resulted in seizure of forty-one boxes of non-Communist material).

[40] Salgado, *supra* note 3, at 43 (explaining that using hash to exclude data would not be a search under exposure theory because the contents of the rejected data are never shown to the human eye, or even the digital eye).

computers cannot act on leads outside of their search parameters. Hash searches have even been criticized as searching too narrowly since a criminal can easily change a document's hash values and effectively hide it from search.[41] The privacy concerns raised when agents searched file cabinets are silent in this scenario—but other, computer-specific problems such as the seizure puzzle arise under traditional Fourth Amendment analysis (what I have been calling "interaction theory") as analogies cross wires. Seizure puzzle does not arise, however, under exposure theory.

Exposure theory often leads to the same result as the interaction theory of search while being a clearer and more intuitively graspable rule. Consider the illegally searched stereo in *Arizona v. Hicks*, where the officer saw a suspiciously expensive stereo system while raiding an apartment for drugs and weapons.[42] Interaction theory says that the officer illegally searched the stereo as soon as he touched the stereo and picked it up because interacting with the stereo was interfering with the original owner's possessory interests. Exposure theory says the officer illegally searched the stereo when he looked at the serial number, and again when he ran it through a database and learned that the stereo was stolen. Mere copying is not enough to trigger exposure theory—the moment when human manipulation of the data resulted in learning something new was the moment when a privacy interest was invaded.[43] Either theory would exclude the stereo, but interaction theory reaches the right conclusion using the wrong reasoning. Its reliance on action fails to recognize that "[t]he dynamics of computer searches turn out to be substantially different from the dynamics of home searches. Computers replace the enter-and-take-away dynamic of home searches with something more like copy, scan, and copy."[44] Insisting on analyzing computer searches as traditional home searches leads to doctrinal problems such as the seizure puzzle.

Adoption of exposure theory allows for more sophisticated understandings of when computer-conducted searches are actually Fourth Amendment searches. The theory properly recognizes that everything on a computer is a copy and that a computer's methods of execution do not lend themselves well to analogy to human methods of search. It thus avoids the procedural roadblocks that hinder basic digital

[41] Jonathan Zittrain, *A Few Keystrokes Could Solve the Crime. Would You Press Enter?*, JUST SECURITY (Jan. 12, 2016, 9:05 AM), https://www.justsecurity.org/28752/keystrokes-solve-crime-press-enter/ ("In fact, the match would be so perfect that some might complain that the search is too limited—even a slight change to a copy of the document in question would make it no longer match its counterparts.").

[42] 480 U.S. 321 (1987).

[43] Kerr, *supra* note 24, at 561.

[44] Kerr, *supra* note 24, at 537.

forensics under an interaction theory of search. Exposure theory is even able to parse out two kinds of hash searches for greater analytical sophistication: inclusionary and exclusionary hash searches. Inclusionary hash searches are Fourth Amendment searches under exposure theory, while exclusionary hash searches are not. This is because an exclusionary hash search summarily excludes certain hash values from analysis without exposing any content to the human investigator.[45] On the other hand, inclusionary hash searches are Fourth Amendment searches because the act of reporting a match signals to the human what the contents must be.[46] Warrants might be needed for inclusionary hash searches unless an exception to the warrant requirement applies.[47]

II. A Broad Warrantless Hash Search Is Reasonable as a Suspicionless Search Where There is a Lessened Expectation of Privacy

A hash search that touches all files is one thing, but the Company X search offends sensibilities in an additional dimension because it searches the files of the innocent and guilty without any proof of wrongdoing. The Company X search is also concerning because it takes place on such a large scale, potentially affecting millions of people.[48] This fact pattern is characteristic of a category of warrantless search called suspicionless searches. There are, generally speaking, five recognized categories of legal suspicionless searches:

(1) administrative searches such as inspections or inventory searches;

(2) exempted or secured areas such as borders and airports;

(3) roadblocks;

(4) searches justified by "special needs"; and

(5) searches of persons with reduced expectations of privacy.[49]

[45] Salgado, *supra* note 3, at 43.

[46] *Id.*

[47] *Id.*

[48] A similar company to Company X had at least one billion people using its mobile platform and 900 million using its email service as of May 2015. Max Taves & Richard Nieva, *Google I/O By the Numbers: 1B Android Users, 900M on Gmail*, CNET (May 28, 2015, 11:03 AM) http://www.cnet.com/news/google-io-by-the-numbers-1b-android-users-900m-on-gmail/.

[49] Derek Regensburger, *DNA Databases and the Fourth Amendment: The Time Has Come to Reexamine the Special Needs Exception to the Warrant Requirement and the Primary Purpose Test*, 19 ALB. L.J. SCI. & TECH. 319, 343 (2009).

However, it is unclear whether all recognized suspicionless searches fall into these five categories.[50] Instead, the Court recognized that "[t]he touchstone of the Fourth Amendment is reasonableness, not individualized suspicion,"[51] such that individualized suspicion is not a "irreducible requirement" of a search.[52] Rather, the Court merely tends to make individualized suspicion a prerequisite element of a search when it seeks to accommodate public and private interests.[53] Otherwise, suspicionless searches are still evaluated looking at the totality of the circumstances, weighing government interest and the reasonableness of the government's method against public and private interests in privacy. The case-by-case approach suggested by the uncertainty surrounding suspicionless searches may be particularly appropriate in cases involving technology anyways, where the law has perennially struggled to adequately transpose pre-digital concepts into the digital world.

It may be helpful to analyze the recognized categories of suspicionless search to get a better sense of how government interests and methods are weighed against the privacy interests of others. Three categories of the five categories, however, are not applicable to the Company X hypothesis (administrative search, border searches, and special needs), so only roadblocks and reduced expectations of privacy will be examined in this Note.[54]

A. Searching All of Company X's Users Is Reasonable Under Roadblock Theory of Suspicionless Search

Suspicionless searches that take the form of drunk driving roadblocks, like the Company X hypothetical, involve agents examining potentially large numbers of innocent and guilty individuals for culpability. The Supreme Court has focused on two elements when examining the reasonableness of roadblock searches: does the search advance a substantial state interest, and was the search protocol create a fair and unbiased process?[55] More particularly, in *Mich. Dep't of State Police v. Sitz*, the Supreme Court sought to "balanc[e] the state's interest in preventing accidents caused by drunk drivers, the effectiveness of

[50] *Id.*

[51] *Id.* at 356 (citing United States v. Knights 534 U.S. 112, 112 (2001)).

[52] *Id.*

[53] Knights, 534 U.S. at 119.

[54] Administrative search is not applicable here because the government is not conducting a routine inspection. Border search is not applicable here because the search is not taking place near an international border. Finally, special needs does not apply here either because the government is conducting the search explicitly for criminal purposes, which falls outside the ambit of special needs. *See* U.S. v. Kincade, 379 F.3d 813, 822-26 (2004) (discussing and distinguishing the border searches, administrative searches, and special needs searches).

[55] Regensburger, *supra* note 49, at 345–46.

sobriety checkpoints in achieving that goal, and the level of intrusion on an individual's privacy caused by the checkpoints."[56]

The Court found that the government's roadblock searches in *Sitz* were reasonable because drunk driving was a severe epidemic which the government had a substantial interest in stopping, the checkpoints were effectively catching drunk drivers, and the intrusion each driver experienced because of the sobriety test was "slight."[57] But most importantly for the Court, the officers lacked discretion to choose which vehicles to stop; every car had to pass through the checkpoint and every driver had to submit to the same test.[58] The checkpoints were not randomly chosen by officers, but "selected pursuant to the guidelines."[59]

In contrast, the Court struck down "random, suspicionless searches of automobiles" in *Delaware v. Prouse* because the search, being unrestrained, could not be said to follow any standard of "reasonableness."[60] In *Prouse*, officers were empowered by the state to conduct discretionary spot checks, pulling motorists over for license and registration checks.[61] Unlike *Sitz*, *Prouse* involved the "'kind of standardless and unconstrained discretion' which the Court had previously disapproved of, insisting that the discretion of the officer in the field be 'circumscribed, at least to some extent.'"[62] The lack of fixed protocol and the relative discretion enjoyed by officers unacceptably increased the potential for the subjective intrusion into the privacy of motorists.[63]

A hash search of Company X's databases, like roadblocks, would involve minimal intrusions on privacy, support a strong government interest in apprehending criminals, terrorists, and other national security threats, and are tightly constrained searches that affect every file and every person equally. Therefore, under a roadblock-theory of suspicionless search, the government would probably be able to ask Company X to hash search all of its U.S. databases for users who own child pornography, despite the large number of people implicated in the search, so long as the government's search applied equally to everyone in a fair and regulated way.

[56] Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 449 (1990) (citation omitted).

[57] *Id.* at 451.

[58] *Id.* at 450.

[59] *Id.* at 445.

[60] 440 U.S. 648, 661 (1979).

[61] *Id.* at 650.

[62] *Id.* at 661.

[63] *Id.* at 655.

B. Searching Company X's User Data Needs to Be Supported by Lessened Expectations of Privacy

As to the question of what will be searched, the government can attempt to justify a suspicionless search on Company X's user data demonstrating that the users have a lessened expectation of privacy in that user data. If the government can show that users were not entitled to full Fourth Amendment protections, then their case for a warrantless hash search is bolstered. This Part will attempt to describe the various theoretical approaches the government could take in arguing for warrantless searches.

1. *The Government Can Run Multiple Searches on Lawfully Seized Evidence*

Though the Company X search seems extreme and unprecedented because of its scope and size, state and federal governments routinely query a certain government database of over eleven million people, conducting suspicionless searches with the purpose of finding guilt.[64] That database is called the Combined DNA Index System ("CODIS") and it is one of the closest procedural analogues to the hypothetical Company X search.[65] CODIS compares long strings of DNA information against each other and reports back whether the strings match. This is done without regard to who or what the DNA may have been sourced from. Like hash searching, DNA matching attempts to match a known piece of data to an unknown piece of data, has a relatively low error rate, and only reports back the identity of those who match.[66] CODIS searches are unlike the hypothetical Company X search, however, because CODIS is firmly entrenched in the criminal justice system. While CODIS's constitutionality has been questioned several times over the years, even on Fourth Amendment grounds, the practice and the institution remains intact and unaltered.[67] Indeed, the issue has never even reached the Supreme Court.[68]

CODIS began as a federal collection of genetic material seized from felons, but the scope of collection has been expanded several times to include other people like sex offenders, convicted misdemeanants, illegal immigrants, and, in some states, even arrestees and juvenile offenders.[69]

[64] *Id.* at 938.

[65] *Id.*

[66] *Id.* at 936.

[67] *See id.* at 940–41.

[68] *Id.*

[69] *See generally* DNA Act; *see also* United States v. Kriesel, 508 F.3d 941, 943 at n.3 (9th Cir. 2007) (summarizing amendments to DNA Act); Boroian v. Mueller, 616 F.3d 60, 66 (2010) (citing Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub.L. No. 109-162, 1004(a), 119 Stat. 2960, 3085 (2006) (codified as amended at 42 U.S.C. § 14135a(a)).

In CODIS, a person's DNA profile "is subject to repeated and indefinite use by law enforcement officials across the nation, who perform searches to match unidentified biological evidence from crime scenes to an individual in the database in hopes of solving a crime."[70] The fact that a person is "never formally charged or convicted of a crime has little impact on the analysis or continued use of her DNA profile," to the outrage of CODIS critics.[71]

Much scholarship surrounding CODIS focuses on whether the initial cheek swab for genetic material is a Fourth Amendment violation.[72] Like in roadblock theory, courts have generally held that cheek swabs are not Fourth Amendment violations because the "totality of the circumstances," including minimally intrusive nature of the actual collection, the state's interest in identifying criminal perpetrators, and the limited identification use of the collected DNA outweigh individual privacy concerns.[73] Much less has been said about whether storing the DNA in CODIS to be compared against in subsequent searches against new DNA samples is a Fourth Amendment violation. However, those subsequent searches are most analogous to our searches of Company X hash values.[74]

The foundation of CODIS search is lawful seizure of the DNA sample to be entered into the database.[75] The government must demonstrate a high standard of need to justify taking blood or DNA samples from a person, since it amounts to a highly intrusive search and seizure on an individual's body.[76] But once that standard has been met, and once the government has lawfully obtained the disputed sample, the individual

[70] Ashley Eiler, *Arrested Development: Reforming the Federal All-Arrestee DNA Collection Statute to Comply with the Fourth Amendment*, 79 GEO. WASH. L. REV. 1201, 1202 (2011)

[71] *Id.*

[72] Kimel, Catherine W., *Note: DNA Profiles, Computer Searches, and the Fourth Amendment*, 62 DUKE L.J. 933, 933 (2013) ("Yet, courts and scholars that have addressed DNA databasing have focused their attention almost exclusively on the constitutionality of the government's seizure of the biological samples from which the profiles are generated. This Note fills a gap in the scholarship by examining the Fourth Amendment problems that arise when the government searches its vast DNA database.").

[73] *Id.* Critics of CODIS fear that technology will one day allow agents to extract more than identity from DNA unless the DNA is obtained by a "procedure that made it virtually impossible to extract sensitive information" such that "information related to identification and nothing else could be obtained from it as a point of comparison." Kaye, D.H., *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL'Y 455, 482 (2001). Hash searches are less intrusive than CODIS searches because a hash search will not return more than what it was asked to look for, and does not even open the file it identifies and flags for human review. It is also potentially less intrusive as a doctrinal matter because it does not delve into an individual's bodily autonomy or privacy.

[74] *Id.*; *see also* Boroian, 616 F.3d at 615–616 (holding that it is constitutional for government to retain and access qualified federal offender's DNA profile in CODIS after his or her term of supervised release or probation has ended).

[75] People v. King, 663 N.Y.S.2d 610, 613 (1997).

[76] *Id.*

"can no longer assert either privacy claims or unreasonable search and seizure arguments with respect to use of that sample."[77] Further analysis and manipulation of the sample, so long as still within the original limited purposes the sample was originally collected for, does not involve any further search and seizure. This means that an agent does not need a search warrant to conduct new tests or analyses on already-seized evidence. Once legally seized, privacy expectations immediately begin to fade, such that even intimate fluids such as blood become ordinary tangible evidence, like guns or controlled substances.[78] Officers are empowered to seize DNA samples by statute, but there are other ways officers can lawfully obtain evidence without a warrant.[79]

Critics of CODIS database searches attempt to argue that a person's privacy expectations towards their bodies is irrevocable and cannot fade away, even after lawful seizure.[80] The information carried in DNA is so personal that citizens ought to have lasting control over how their DNA generally is used, especially in the context of CODIS (suspicionless search seeking to assign culpability).[81] The potentially serious consequences of a match, argue critics, mean that individuals deserve higher protections, especially since people have been convicted based solely on a cold DNA match.[82] Therefore, say critics, an unlawful Fourth Amendment search occurs each time a person's genetic material in CODIS is handled without a warrant.[83] Officers should get warrants every time he wants to search the database, specifying who he wants to compare the samples against and demonstrating probable cause supporting why.[84] The holdings of various court cases, however, do not favor such a procedural rule, even if an individual has finished his sentence and is now free.[85] The data will always remain in the database.[86]

The overwhelming defeat of bodily privacy interests in the CODIS context demonstrates that the crucial inquiry for suspicionless searches is whether the government had authority to seize the evidence. A bright-line rule develops: if the government manages to lawfully seize data, then the government can run whatever searches they like on the seized data, however many times they want, even if the data set

[77] *Id.* at 614.

[78] *Id.*

[79] Kimel, *supra* note 72, at 940 (citing the DNA Act).

[80] Kimel, *supra* note 72, at 940.

[81] Kimel, *supra* note 72, at 943.

[82] Kimel, *supra* note 72, at 959.

[83] Kimel, *supra* note 72, at 934.

[84] *Id.*

[85] Although the United States Supreme Court has yet to issue an opinion on this topic, federal and state courts alike have largely downplayed these privacy concerns, almost universally upholding DNA databases against Fourth Amendment challenge. Regensburger, *supra* note 49, at 323; *see also* Boroian, 616 F.3d. at 67–68.

[86] Boroian, 616 F.3d. at 67–68.

encompasses millions of people. The government could even gather a database of seized hard drive evidence to periodically run hash searches against. Government demonstrations of a lawful right to seize certain pieces of data might be very persuasive to companies who are unsure of whether to comply with the government's warrantless request or not. However, the crux of this hypothetical warrantless search is Company X's cooperation. The CODIS-derived rule heightens the importance of Company X's role as a metaphorical gatekeeper in situations where the government wants Company X to run the search rather than seize the data for itself.[87] Accordingly, the analysis turns to other ways the government could demonstrate a warrantless right to seize a Company X user's data through a lessened expectation of privacy.

2. *A Warrantless Search for Contraband is Lawful, Particularly If the Search Method Only Alerts to Presence of Contraband*

The government could try to persuade Company X to search and share results by pointing out that the government already has a lawful right to seize child pornography without a warrant, since contraband like child pornography does not entitle its possessor to a reasonable expectation of privacy. A hash search which targets contraband files may not be a Fourth Amendment event requiring a warrant because there is "no legitimate interest [of privacy] in possessing something that is illegal to possess (for example, contraband), [so] there is similarly no search when an investigator uses a tool that reveals only contraband."[88] Further, a test that "merely discloses whether or not a particular substance is [contraband] does not compromise any legitimate interest in privacy,"[89] particularly if that test "does not expose non-contraband items that otherwise would remain hidden from public view."[90]

In the hypothetical proposed above, the government is interested in finding instances of child pornography, which is contraband material. Therefore, though a hash search for child pornography would necessarily expose the results by positive inclusion (thereby becoming a Fourth Amendment event under Kerr's exposure theory), the contraband nature of the material nullifies the intrusiveness of the search such that there is no longer a Fourth Amendment event and no warrant would be required.

[87] One reason government might prefer Company X run the search is easier access; the government probably does not want Company X to turn over the contents of their entire servers since that would be a hassle. In addition, the government may be trying to take advantage of X's superior proprietary search algorithms and the like.

[88] Salgado, *supra* note 3, at 44; *see also* Illinois v. Caballes, 543 U.S. 405, 409 (2005); United States v. Jacobsen, 466 U.S. 109, 124 n.24 (1984).

[89] Jacobsen, *supra* note 88, at 123.

[90] Caballes, *supra* note 82, at 409 (citation omitted) (quoting United States v. Place, 462 U.S. 696, 707 (1983)).

3. *A Warrantless Search Through Metadata, such as Hash Values, Is Lawful Under the Third-Party Doctrine*

One of the most powerful tools the government has in its kit for digital search and seizure is the third-party doctrine. Third-party doctrine explains that individuals have a lessened expectation of privacy in data that they have voluntarily shared with third parties *for the third party's use*.[91] This is an important distinction because it explains why "records that the computer operator must routinely use" are disclosed under third-party doctrine, but contents of phone conversations, personal files, and emails are not.[92] When information is routinely used, the third-party has a legitimate purpose in accessing and using the information.[93] Users generally have a lessened expectation of privacy in data generated about them by the company, called metadata, because metadata is information created by the business in the normal course of operation, and is not user-generated.[94] But otherwise, a user has a legitimate expectation of privacy in content "even when the system manager makes backup copies of such records."[95] Third parties can choose what to do with the data that has been shared with them; they can choose to disclose the information in response to a warrantless request from the government, or refuse.[96]

This means that the government cannot pull files directly from Company X without a warrant. But can the government compel Company X to simply run the hash search, since hash values are not content created by users but metadata routinely created in the course of business?

Corporations commonly hash their databases as part of their backup procedures.[97] If a Company X server were to crash, for example, Company X would restore an older version and run a hash search to determine which files had changed and which files had stayed the same.[98] Hash values, in this sense, are analogous to the metadata generated by telephone companies (location of calls, duration of calls, who the call was with) for the business purposes of ensuring quality service and accurate billing.[99] It is not user-generated content and thus does not entitle

[91] WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f) (5th ed. 2015); *see also* Orin Kerr, *The Case for Third-Party Doctrine*, 107 MICH. L. REV. 561, 568 (2009).

[92] LaFave, *supra* note 91.

[93] *Id.*

[94] Joseph D. Mornin, *NSA Metadata Collection and the Fourth Amendment*, 29 BERKELEY TECH. L.J. 985, at 997 (2014).

[95] LaFave, *supra* note 91.

[96] *Id.*

[97] *Solution Brief: Understanding Data Verification and Disaster Recovery Using Barracuda Cloud LiveBoot Recovery*, Barracuda, https://www.barracuda.com/assets/docs/White_Papers/Barracuda_Backup_Solutions_Brief_Cloud_LiveBoot_US.pdf (last visited May 31, 2017).

[98] *Id.*

[99] *What Is Metadata?*, PRIVACY INTERNATIONAL,

someone to a reasonable expectation of privacy. Even if someone could have an expectation of privacy in a hash of her files, "the true degree of intrusion into private matters is, at most, de minimis . . . . Because hashing is 'minimally intrusive' and is driven by 'operational necessities,' there is little constitutional significance."[100]

The end result is that the government can likely request Company X to run a hash search without needing a warrant or impinging on users' reasonable expectations of privacy because hash values are accessible under the third-party doctrine. Company X, however, still has the power to refuse a warrantless request.

In summary, the government's best chance at convincing Company X to help with the hash search is to demonstrate that the government has a legal right to seize the disputed evidence anyways. This has the effect of making Company X more willing to help the government, since the government is not gaining information it could not already probably compel and is not conducting a search it would not already be authorized to conduct.

To demonstrate that the government has a legal right to seize evidence without a warrant, the government must show that the target evidence has a lessened expectation of privacy. Evidence already in possession of the government has no expectation of privacy; neither does contraband or metadata generated by a third-party. However, there is a difference between advancing on contraband versus third-party metadata theories of privacy.

Users have lessened expectations of privacy in the contraband items themselves, meaning that the government can seize the contraband immediately once it is found, while users under the third-party doctrine retain expectations of privacy in user content but lose privacy in metadata, or data generated about that user content. Hash values probably qualify as a type of metadata because they are descriptors of the user content and not actually content. Thus, advancing under a third-party theory gives the government the right to search and seize hash values, but would require the government to obtain another warrant to seize the contraband indicated by the hash value search.

Finally, to circle back and attempt to the untangle the interlocking privacy-interest scenario this Part started with: a user who stores contraband on their phone (or in their email or in their cloud storage account) has no expectation of privacy towards the contraband itself, but the rest of the contents of the phone may be protected as user-generated content. Metadata associated with the phone is not

https://www.privacyinternational.org/node/53 (last visited May 31, 2017).

[100] Salgado, *supra* note 3, at 42–43.

protected by expectations of privacy and can be seized by the government without a warrant.

III. A SEARCH WARRANT FOR HASH SEARCHING COULD BE SUFFICIENTLY PARTICULARIZED

Before assessing whether Company X can decline to help the government, and if so, what the government can do to compel the search, it is useful to cover all of the bases and ask whether, if a warrant is needed for a hash search, the government would be able to formulate a valid warrant. In order to be valid, a warrant must be reasonable and particular.[101]

The particularity requirement is designed to prevent "general searches" by requiring "a neutral judicial officer to cabin the scope of the search to those areas and items for which there exists probable cause that a crime had been committed.[102] It requires that "the warrant must clearly state what is sought."[103] "Particularity" concerns arise when a warrant's description of the place to be searched or the items to be seized "is so vague that is fails reasonably to alert executing officers to the limits of their search [and seizure] authority."[104] To satisfy the "particularity" requirement, "[a] warrant must be sufficiently specific to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize."[105]

Assessing particularity has two main components.[106] The Sixth Circuit has determined that the particularity requirement encompasses two main issues. The first issue is "whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take."[107] The second issue is "whether the category as specified is too broad in the sense that it includes items that should not be seized."[108] "However, the degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought."[109]

In some cases with warrants that authorized search and seizure of digital media, the warrants seemed overbroad but were upheld as sufficiently particular given the special difficulties of electronic search

[101] LaFave, *supra* note 91, §§ 4.5–4.6.

[102] Baranski v. Fifteen Unknown Agents of Bureau of Alcohol, Tobacco & Firearms, 452 F.3d 433, 441 (6th Cir. 2006).

[103] United States v. Cioffi, 668 F.Supp.2d 385, 390 (2009) (citation and quotation marks omitted).

[104] United States v. Clark, 638 F.3d 89, 94 (2d Cir. 2011).

[105] United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000) (alteration in original) (citing United States v. LaChance, 788 F.2d 856, 874 (2d Cir. 1986)).

[106] *See* United States v. Neuhard, 149 F.Supp.3d 817, 822 (E.D. Mich. 2016).

[107] *Id.*

[108] *Id.*

[109] *Id.* at 822–23.

and seizure.[110] At the same time though, "while recognizing the inherent risk that criminals can easily 'hide, mislabel, or manipulate files to conceal criminal activity,' we must also take care not to give the Government free rein to essentially do away with the particularity requirement by allowing it to examine every file on the device."[111]

To demonstrate, in *Rarick*, a warrant for digital media which authorized seizure "any and all electronic data" and "any and all communications" without specifying a date (as a means to restrict the search to before and after said date) was held to be constitutional despite admittedly broad language for several reasons. First, "the *Rarick* warrant contained portions that were specifically targeted to the 'images' and 'videos' that the officers had probable cause to search, although the exact folder location was unknown."[112] Second, the warrant was executed in such a way that the overbroad portions did not actually affect defendant.[113] Finally, the reviewing court gave deference to the findings of the trial court, which had a policy of assessing reasonableness on a case-by-case basis.[114] Despite not restricting the search to a certain time period or certain folders, the court found that the description, at least, of the type of file to be seized (videos and photos of an underage girl) was as specific as possible, given the circumstances and nature of the activity being investigated.[115] Further, the warrant was held valid even though a specific search methodology was not outlined in the warrant for fear of unduly limiting the government's ability to find misnamed and hidden files.[116] "Courts tend to tolerate a greater degree of ambiguity where law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant."[117]

Turning back to the Company X hypothetical, the government could probably write a warrant that satisfies general particularity standards and concerns. Using a hash search, for example, severely restricts what the officers will be looking at or seizing such that the officer has little to no discretion on how to conduct the search. In addition, the search protocol for a hash search would be included in the warrant since a hash search, by its very nature, requires the officer to know exactly what file is being searched and seized. The only parts that are vague would be what

[110] *Id.* at 825.

[111] *Id.* at 826 (citing United States v. Rarick, 636 Fed. Appx. 911, 915 (6th Cir. 2016)).

[112] *Id.*

[113] *Id.*

[114] *Id.* at 823.

[115] *Id.* at 826.

[116] *Id.*

[117] United States v. Buck, 813 F.2d 588, 590 (2d Cir. 1987) (quoting United States v. Young, 745 F.2d 733, 759 (2d Cir.1984), *cert. denied,* 470 U.S. 1084, (1985)).

span of time the warrant covers, and where the officer expects to find the files. The span of time could be tailored to the statute of limitations associated with possession of child pornography, which would be a reasonable limit.

A magistrate judge looking at the "where" of this hypothetical warrant is likely to assess the public safety goals of the search and weigh the extremely slight actual intrusion of a hash search against the substantial interest served by finding and eradicating child pornography. Though some magistrates may disagree, the government probably has a strong case for executing an all-U.S. Company X users warrant, especially in light of similar practices surrounding CODIS and the lack of privacy inherent in contraband material. The hypothetical search even has the benefit of being a more narrowly conducted search than typical CODIS or digital searches, since it knows exactly what file to seize, has no human eyes looking for "plain view" evidence, and will categorically ignore items not specified in the warrant. Thus, the government is likely to succeed in either justifying an all-U.S. users search, with or without the warrant.

IV. CORPORATIONS ULTIMATELY HAVE A CHOICE IN COOPERATING WITH WARRANTLESS SEARCHES

The law seems to be at least plausibly permissive of allowing the government to run a search across all of Company X's U.S. databases, with certain limitations. The question now is whether Company X should cooperate. As a matter of procedure, Company X can refuse the government's warrantless requests because warrantless searches do not carry the authority and weight of a judicial order. However, if the government has made a successful warrant application, Company X can still go to court and challenge the reasonableness of the warrant.[118] If Company X loses the warrant challenge in court, then it must cooperate with the government according to the warrant.

There are several reasons why Company X might decide to cooperate with the government: as discussed previously, the law seems to be in favor of executing a "finely tailored" search such as a hash search. [119] The hash search is sophisticated and accurate enough that innocent people are unlikely to be implicated in the search beyond having their files briefly touched by a computer program. Helping the government by running the minimally intrusive hash search has the significant societal benefit of apprehending criminals.

[118] This is the course of action Apple took when confronted with a warrant to unlock an iPhone used by the suspected San Bernardino terrorist. Rob Price, *Why the FBI Is Demanding that Apple Hack into the iPhone—and Why Apple Says It's a Terrible Idea*, BUSINESS INSIDER (Feb. 17, 2016, 7:00 AM), http://www.businessinsider.com/apple-challenges-fbi-demand-to-hack-into-san-bernadino-shooter-iphone-5c-court-order-2016-2.

[119] Zittrain, *supra* note 41.

On the other hand, Company X has many legitimate reasons to refuse to aid the government, especially because suspicionless hash searches are not doctrinally limited to obvious instances of contraband such as child pornography. Nobody wants child pornographers around, and it is relatively simple to prove whether or not such a file is illegal. However, this Note grew out of a thornier hypothetical scenario, written by Professor Jonathan Zittrain, where the government was asking a web service company to help track down terrorists.[120] In that hypothetical, terrorist plans were found on a seized laptop and the government wanted to search through the company's online databases to find out who else had the same plans, and therefore had to be collaborators.[121]

This scenario is not impossible to imagine in real life. Indeed, the government has probably already circled around this idea and probably has already propositioned certain companies for help. For example, the government has successfully pressured Facebook into altering its services to combat terrorist propaganda,[122] and the so-called Apple v. FBI case is widely considered a "test case" by the government to see how forcing corporations to help in the war against terror would fare in the court of law and of public opinion.[123] Companies like Twitter have publically resisted assisting the government for ideological reasons like protection of free speech.[124] The real decision for Company X, it seems, is not a legal one—it is a moral and ethical question, tightly bound up with the company's public image and values.

CONCLUSION

Hashing is a promising digital forensic technique because of its accuracy, specificity, and minimal invasiveness. As more and more of our lives migrate to the cloud and other digital forms, reconciling the paper-bound fact patterns and rationales of the Fourth Amendment will become increasingly necessary and urgent. Exposure theory presents a novel and common-sense way of updating the Fourth Amendment to recognize how computers function. As more and more of our lives migrate into the hands of private corporations, society's expectations of privacy will also demand a re-drawing of search and seizure limits and

[120] *See id.*

[121] *Id.*

[122] Natalie Andrews & Deepa Seertharaman, *Facebook Steps Up Efforts Against Terrorism*, WALL ST. J. (Feb. 11, 2016, 7:39 PM), http://www.wsj.com/articles/facebook-steps-up-efforts-against-terrorism-1455237595.

[123] Andy Meek, *We Asked Every Congress Member with a Computer Science Degree about Apple's War with the FBI*, BGR (Mar. 23, 2016, 10:19 AM), http://bgr.com/2016/03/23/apple-vs-fbi-congress-interviews/.

[124] Christopher S. Stewart & Mark Maremont, *Twitter Bars Intelligence Agencies from Using Analytics Service*, WALL ST. J. (May 8, 2016, 7:54 PM), http://www.wsj.com/articles/twitter-bars-intelligence-agencies-from-using-analytics-service-1462751682.

will require a clarification of the nebulous relationships between corporation and government. Though it seems today that Company X is ultimately in a position to refuse to help the government, the government probably has enough doctrinal leeway to make a real run at forcing Company X to run a dragnet hash search tomorrow. All they need is a judge to sign off.