In Lawrence Wright’s *Looming Tower: Al-Qaeda and the Road to 9/11*, Wright explains, “There is an anecdote that counterterrorism officials often tell about the rendition of Ramzi Yousef,” the first (1993) World Trade Center attacker.\(^1\) According to Wright’s sources, when Yousef was being transferred via helicopter over Manhattan, one of the SWAT team members removed Yousef’s blindfold and told him, pointing to the World Trade Center, “You see, it’s still standing,” to which Yousef responded, “It wouldn’t be if we had had more money.”

Eight years later, the next attack on the World Trade Center shook the world. Its cost was about $400,000 to $500,000, about $300,000 of which passed through hijackers’ bank accounts, funneled through Germany and the United Arab Emirates, leaving a paper trail that would have been recognized if we were better equipped to investigate it.\(^2\) This article looks at the question of constitutional considerations—with respect to privacy—of expanding our policies to more adequately reveal unknown illicit transactions in order to prevent the next 9/11. It is my opinion that pattern-based transactional data mining, particularly that of financial transactions, constitute a reasonable search, akin to that of a Terry stop.

The accessibility to and capabilities of the Internet and other electronic communication provide tools that were unthinkable at the time when the U.S. Constitution was drafted. These new tools have led to countless innovations; some of the developments the Internet has brought with it have aided those who wish to do our country harm, and others have aided those trying to prevent that harm. Our interpretation of the Constitution need not change as the landscape for combating terrorism evolves, but the framework in which we see the considerations at hand must take into account the fundamental changes to both the threats investigated and resources needed by law
enforcement and the national security community. The question to be answered is whether electronic surveillance—specifically, transactional data mining—can represent an exception to the warrant process when the search is related to an international terrorist threat, even if there is a domestic nexus, so long as the search is pattern-focused as opposed to person-focused.

The term national security, for the purposes of this paper, will be defined as all of the intelligence and law enforcement activities related to the “the protection of United States national interests from foreign security threats.” Specifically, the national security community must investigate and prevent terrorist acts, defined in Executive Order 13224, as

an activity [that] involves a violent act or an act dangerous to human life, property, or infrastructure; and appears to be intended—to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking. In addition, those investigated may either be U.S. persons or non-U.S. persons; EO 13224 specifies that “‘United States person’ means any United States citizen, permanent resident alien, entity organized under the laws of the United States (including foreign branches), or any person in the United States.”

Orin S. Kerr and Richard A. Posner have each examined new approaches to privacy in the age of the Internet, and it is a subset of these approaches that this article attempts to use to analyze the legitimacy of these new approaches and logical implications of particular uses in law enforcement and national security. Posner led the shift in this new trend of constitutional analysis by asserting that the purpose of the government’s use of data mining for national security is data-driven, rather than person-driven, and therefore does not conform to conventional views of privacy. Kerr expands on this analysis to develop what he calls a “dual-path approach” to privacy considerations of surveillance, but, by his own admission, stops short of examining many of the specific powers and structure of the privacy and security balance of the paths he lays out, including curtailing his analysis before attempting to “draw the line between security and privacy.”

This article picks up where Posner and Kerr left off, examining where the national security community has the most flexibility and
authority to use data-mining surveillance. It is my interpretation that the reduced scrutiny given to the investigation of financial transactions and the data-driven impersonal objective and computer-driven means involved in data-mining surveillance of financial transactions alter the need for deference to privacy in pattern-based transactional data surveillance. Moreover, the imminence and overwhelming destructive power of the national security threats posed by Internet-based transactions provide additional legitimacy to warrantless pattern-based transactional data surveillance, in addition to the fact that non-U.S. persons are many times the subjects of the surveillance and that the searches themselves fall into the “special needs” exceptions that are considered reasonable warrantless searches. Thus, this article will discuss a particular subset of Kerr’s dual path approach, with particular attention paid to its unique authority. This analysis suggests that, contrary to Kerr’s implication, the Foreign Intelligence Surveillance Act (FISA) may not need to be updated to provide authority for the particular type of searches discussed, but that the authority is already implicit and any additional authority granted would be redundant, but constitutional nonetheless. That is, transactional pattern-based data mining is a constitutional method of surveillance falling within the Fourth Amendment’s reasonable search standards and representing the least intrusive method to accomplishing its goal.

The first section of this article will provide background on the authority of the national security community to engage in data mining, with particular attention given to financial transactions. The second section will discuss the role of implementation in privacy concerns from a constitutional- and case-based perspective, as well as the need for transactional data mining. The third section addresses the justification for the approach outlined, analyzing the justifications for a warrantless transactional data-mining system for national security searches.

Authority and Concerns of National Security Surveillance

Combating Terror Financing: A Brief Summary of Authorizations

“When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum, for it includes all that
he possesses in his own right plus all that Congress can delegate." Both the legislative and executive branches have actively authorized the investigation of financing that may be related to terrorism, and thus the constitutional legitimacy of such investigations has an actively recognized strength delegated by the two political branches.

The International Emergency Economic Powers Act (IEEPA) grants the president the authority and responsibility of declaring an emergency with respect to an extraordinary threat that originates outside of the United States such that he may investigate and block such a threat. Additionally, the USA PATRIOT Act, particularly Title III, enhances investigatory tools concerning financial transactions with domestic origins that may have ties to a foreign agent's terrorist plot against the United States.

Pursuant to the National Security Act of 1947, Executive Order 12333 empowers the intelligence community to investigate threats to national security by providing "for the effective conduct of United States intelligence activities and the protection of constitutional rights." EO 12333 requires that "all reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available," including the use of electronic surveillance defined as the "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication" (the guidelines of which EO 12333 states fall within the Foreign Intelligence Surveillance Act).

Likewise, pursuant to IEEPA authority, President George W. Bush signed Executive Order 13224, which recognized "that grave acts of terrorism and threats of terrorism committed by foreign terrorists" and "the continuing and immediate threat of further attacks on United States nationals or the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," and therefore he provided additional tools that would "enable the United States to combat the financing of terrorism." Specifically, EO 13224 addresses the threat of "foreign persons determined by the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, to have committed, or to pose a significant risk of committing, acts of terrorism that threaten the security of U.S. nationals or the national security, foreign policy, or economy of the United States." It states:

[Al]ny transaction or dealing by United States persons or within the United States in property or interests in property blocked pursuant to this order is prohibited, including but not limited to the making or
receiving of any contribution of funds, goods, or services to or for the benefit of those persons listed in the Annex to this order or determined to be subject to this order . . . [and] any transaction by any United States person or within the United States that evades or avoids, or has the purpose of evading or avoiding, or attempts to violate, any of the prohibitions set forth in this order.\(^\text{18}\)

The transactions by U.S. persons associated with international terrorist threats are not only prohibited, but the investigation and prevention of them by U.S. government agencies is authorized in Section 7 of EO 13224, where it states, “All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.”\(^\text{19}\)

There are many different agencies that may handle the various aspects of threat assessment, whether it may be the National Security Agency (NSA) engaging in surveillance of threats of international terrorism, the Department of the Treasury investigating the financial components of terrorist plots, or the Department of Justice preventing terrorism and prosecuting its actors. For the purpose of this paper, the “national security community” will hereafter represent the collective actors pursuing the prediction and prevention of acts of terrorism, including counterterrorism operations, intelligence gathering, and the federal, state, local, and tribal agencies dedicated to the enforcement of the policies embodied in Executive Orders 12333 and 13224, as well as the USA PATRIOT Act and related authorities.

**The Warrant Process in Pursuing National Security Investigations**

Warrants in domestic crimes cases fall under the authorization of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), which contains an exemption for the types of threat analyzed in this paper:

Nothing contained in this chapter or in section 605 of the Communications Act . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities.\(^\text{20}\)

Those electronic searches that fall within that Title III exemption fall under the jurisdiction of the Foreign Intelligence Surveil-
lance Act (FISA) of 1978. FISA "governs governmental authority to conduct, as part of an investigation to gather foreign intelligence information, electronic surveillance and other activities to which the Fourth Amendment warrant requirement would apply if they were conducted as part of a domestic criminal investigation." It is understood that its provisions "provide a minimum standard that must be met before foreign intelligence searches or surveillance may be conducted by the government." Thus, FISA acknowledges a difference between criminal searches and national security searches. Under FISA, the president, through the attorney general, may authorize searches without a criminal warrant, but only by approval from a FISA-specific court "to acquire foreign intelligence information." When "authorizing electronic surveillance or a physical search, [the FISA court] must find probable cause to believe both that the person targeted by the order is a foreign power or its agent, and that the subject of the search is owned, possessed, or will be used by the target." A FISA warrant is analogous to a Title III warrant, but it is required for surveillance when one of the parties involved in a communication is a U.S. person but the investigation is related to an international security threat. Thus, for FISA authorization to be required, the surveillance target must have both a connection to the United States as well as a foreign power and the search must be motivated by and directed toward a particular person.

Thus, law enforcement and the national security community are authorized and required to investigate financial transactions that may be directly or indirectly related to international terrorism, with either foreign or domestic origins. When a warrant is required, it is person-focused and falls under the FISA guidelines; however, there are circumstances under which a warrant is unnecessary but a search is still reasonable. The policies that govern searches are limited by the threat to privacy posed by their implementation.

Background on the Fourth Amendment: Historical Context and Applicability

The Fourth Amendment guarantees the "right of the people to be secure in their persons . . . against unreasonable searches and seizures" and that warrants must be issued "upon probable cause" that describe "the place to be searched, and the persons or things to be seized." As evident by the text of the Amendment itself, a warrant is not necessary for every search, but every search must be reasonable. When
a warrant is necessary, however, the Amendment focuses the content of the warrant on specific places and people, which were priorities fundamental to searches at the time the Constitution was drafted but that have evolved with the advent of the Internet and electronic communications.

The Fourth Amendment was borne out of the Framers’ fear of a law enforcement regime whose searches were modeled after the British general warrant system, which lacked specificity of location and person and was used to “intimidate dissidents, authors, and printers of seditious material by ransacking homes and seizing personal papers.” William Blackstone, the eighteenth-century British judge who inspired much of the jurisprudential thought of the Framers, wrote that a man “will never suffer [his home] to be violated with impunity.” The Framers, motivated by the fear that abuses of power may violate the privacy of one’s home, designed the Fourth Amendment such that searches would preserve the right “to be let alone.” The Framers’ motivation that Americans be “let alone” implies that, should one give reason to believe that they have violated the rules of society, they may forfeit their right to be let alone (which may justify a warrant-based search) or, regardless of suspicion, a search may not violate that right. Moreover, the Framers’ wording of the Amendment suggests that the violation is personal: they feared British law enforcement officials violating the homes of particular people based on bias, which is a person-to-person violation. In an age of automated searches investigating data, the Framers may have had a different view of the violation of privacy.

In addition to evaluating whether the right to privacy has been violated, we cannot ignore whether the right is even applicable. As Justice Rehnquist wrote in the court’s opinion in United States v. Verdugo-Urquidez, “[B]y contrast with the Fifth and Sixth Amendments, [the Fourth Amendment] extends its reach only to ‘the people.’” Justice Rehnquist clarifies that “the people” are the people of the United States and, for that reason, a “search and seizure by United States Agents of property that is owned by a nonresident alien and located in a foreign country” does not require Fourth Amendment analysis; it is simply permitted. He continues,

The available historical data show, therefore, that the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the
Federal Government against aliens outside of the United States territory.\textsuperscript{32}

Thus, the Fourth Amendment must only be considered when the person whose privacy it may violate has a “previous significant voluntary connection with the United States” or a “substantial connection with this country,”\textsuperscript{33} in which case, as previously discussed, an investigation targeting international terrorism would fall into the FISA requirement paradigm.

As we move forward to analyze the ramifications of the Fourth Amendment on searches related to international terrorist threats, we now recognize the applicability of the Amendment rests on the following criteria: location and connection to the United States and whether a person connected to the United States has a right to be let alone, which has been violated. In particular, it is clear that those searches that investigate overseas connections need not require a warrant, and that a violation of privacy hinges on a concern for that which is personal being revealed.

\textbf{Background: Balancing Privacy and National Security}

When investigating a foreign power with no connection to the United States—that is, when the investigation is done outside of the United States concerning non-U.S. persons—the intelligence community rests on the president’s plenary powers as the commander in chief and as the sole organ of foreign policy\textsuperscript{34} and the Fourth Amendment does not apply (as in the Verdugo case); therefore, an investigation is not subject to approval by the courts. When there is a connection to the United States, however, for the government to engage in a search, the search must be reasonable, and it may require authorization via a FISA warrant, analogous to the Title III provisions.\textsuperscript{35} One of the primary cases of judgment in this realm is United States v. United States District Court (the Keith case), which asked whether it is within “the President’s power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval.”\textsuperscript{36}

In Keith, one of the defendants was charged with bombing a CIA building and claimed that the wiretaps submitted as evidence against him were obtained illegally.\textsuperscript{37} The Supreme Court upheld that a court order should have been issued to obtain the wiretaps. However, it specified that its reasoning rested on the grounds that
the scope of the government's search was based on preserving domestic security, an act it claims is a high priority but does not rise to the level of necessity such that exercising domestic security investigations should escape the requirements of the Fourth Amendment. This implies, then, that a domestic investigation of an international threat may fall outside the ruling. In fact, Justice Powell specified in the court's opinion that the Keith ruling "requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."38 Justice Powell went on to invite Congress to address the issue of domestic surveillance of foreign threats, rather than to rule on the issue himself: "Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III."39 This calling for congressional action is what inevitably led to the enactment of FISA; it should be noted, however, that his reasoning for objecting to warrantless electronic surveillance in this case was due to the lack of a foreign nexus of a threat, not the belief that surveillance of national security threats deserves equal scrutiny to that of ordinary crimes, as shown by the distinctions he gives between Title III investigations and those of national security:

We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency.40

Thus, investigations of national security threats have a higher imperative than ordinary crimes, and domestic investigation of foreign and related threats may fall outside the warrant requirements specified in Keith.

In examining where these cases do fall, we must begin with a ruling that came even before Keith, when the dominant warrant requirement paradigm was outlined for all cases, not just those involving national security. In the case of Katz v. United States, the court decided that the Fourth Amendment protections required a warrant
for searches when the target of the search has a reasonable expectation of privacy, but not when they have exposed their activities or statements in plain view of others.\textsuperscript{41} The Fourth Amendment, as Justice Harlan wrote, "protects people, not places," and for a warrant to be required, it must be shown:

that a person [has] exhibited an actual (subjective) expectation of privacy and . . . that the expectation be one that society is prepared to recognize as "reasonable." Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected," because no intention to keep them to himself has been exhibited.\textsuperscript{42}

Therefore, when analyzing privacy concerns, the relevant paradigm outlined by the court is that a warrant is required when people have an expectation of privacy that is considered reasonable and have shown an intention to keep their activities to themselves. This implies that if one has not taken such precautions, that a warrantless search would be reasonable.

In fact, the Supreme Court has explicitly recognized bank statements as falling into the exception left open in \textit{Katz} that allows for a warrantless search when one acts—directly or indirectly—to relinquish his or her right to privacy. In \textit{United States v. Miller}, the government was challenged for its warrantless use of bank records as evidence against a man conspiring to commit tax fraud; the government subpoenaed the bank for the records rather than obtaining a warrant for the individual's personal records.\textsuperscript{43} Justice Powell wrote, "The checks are not confidential communications, but negotiable instruments to be used in commercial transactions. All of the documents obtained . . . contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."\textsuperscript{44} In other words, when an individual engages in a transaction, the transactors, as well as the funding providers (usually banks), are exposed to the information inherent in the transaction, and they are exposed with the knowledge of all of the transactors. Thus, any given transactor knowingly diminishes his or her expectation of privacy by entering into a transaction.

This theme was expanded upon when the court rejected a Fourth Amendment challenge to the recovery of transactional data from phone companies in \textit{Smith v. Maryland}, on the grounds that "[w]hen [the subject] voluntarily convey[s] numerical information to the phone company and 'expose[s]' that information to its equipment in
the normal course of business, he assume[s] the risk that the com-
pany would reveal the information." This ruling also began a new
path in Fourth Amendment jurisprudence in light of the Katz case,
demonstrating a clear difference between investigations of the sub-
stance of communications and the data related to those communica-
tions (for Smith, the words used in the phone call as opposed to the
numbers dialed) and also the abrogation of privacy when providing
information to a third party (in Smith, the phone company, and in
Miller the bank). Specific to data mining, the circuit court decision
of United States v. Fregoso ruled that "telephone company custom-
ers do not retain a reasonable expectation of privacy in account
information held by the telephone company." Thus, according
to the Eighth Circuit, account information ("noncontent account
records") does not require a warrant, extending the idea that re-
vealing a threat through impersonal means has a lower threshold of
privacy considerations.

In response to this shift, Congress authorized the Foreign Intelli-
gence Surveillance Court (FISC) to issue orders to third-party record
holders for transactional records, without a court order, through
National Security Letters (NSL). Law enforcement had to certify
through a written statement that it was requesting customer infor-
mation pursuant to an investigation concerning an international
terrorist threat. This authority was broadened through the USA
PATRIOT Act, which required that NSL searches be related to
international terrorism investigations, rather than directly involv-
ing a foreign nexus (such as a communication involving a non-U.S.
person as an interlocutor). Thus, as Kerr observes, NSL authorities
"regulate less intrusive measures designed to reveal agents of foreign
powers rather than monitor known ones." Similar to the NSL
program, but for electronic communications, the government may
require a service provider to turn over transactional information,
provided it can prove relevance to an ongoing criminal investiga-
tion, as authorized by the Electronic Communications Privacy Act.
It follows that Congress has explicitly authorized a search paradigm
with lower scrutiny than a warrant system: simply the authorization
of the law enforcement body conducting the search. NSL searches
are, like FISA warrants, person-focused, and show that engaging in
a transaction constitutes relinquishing an expectation of some level
of privacy, or else a full warrant would be required.

This is a significant shift, as the court has begun to recognize
that technological innovations have made it more difficult to dis-
cover threats through traditional surveillance and that the privacy concerns of the means of a search are more severe when a person is monitored rather than when situations are analyzed to reveal threats.

The predominant hurdle that investigations must pass is that of "reasonableness." While the Fourth Amendment states that warrants are sometimes necessary, it states that in all cases (where the Fourth Amendment applies), the search must be reasonable. The reasonableness standard opened the doors to a notable exception to warrant requirements known as the "special needs" doctrine outlined in the case of *Chandler v. Miller* (1997), which stated, "To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing. But particularized exceptions to the main rule are sometimes warranted based on 'special needs, beyond the normal need for law enforcement.'"53 The *Chandler* case balanced Georgia’s need to drug test its candidates for state office with the intrusiveness of the drug tests and the purpose of the tests. The court ruled that the substantial need for drug testing must be "sufficiently vital to suppress the Fourth Amendment’s normal requirement of individualized suspicion," but that, in the case of Georgia’s drug testing, there was little risk of the problem being addressed (drug use by candidates), and the means were not closely tailored to the ends claimed by the state (the testing process was not the best way to curtail drug use).54

However, in the case of *Skinner v. Railway Labor Executives’ Association* (1989), the Supreme Court determined that drug testing of rail workers was a compelling state interest, that the means of the test were reasonable, and the tests comported with "justifiable expectations of privacy."55 More recently, in *Board of Education of Independent School District No. 92 of Pottawatomie City v. Earls* (2002), the Supreme Court ruled that student athletes have a diminished expectation of privacy because they choose to participate in a regulated and supervised program.56 Moreover, the tests were viewed as minimally intrusive, and the court decided that "[i]n the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable 'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'"57 Given the need for the school to perform its custodial duties over the children and the impracticability of obtaining a warrant, the court ruled that it was permitted to engage in suspicionless searches.
The special needs exception has been related to national security in the form of airline passenger screenings. As recognized in the district court case *United States v. Davis*, passengers are subjected to a "regulatory" search, whose scope is not to prosecute criminals but to prevent weapons from being transported on a plane. In actively attempting to become a passenger, the potential passengers diminish their expectation of privacy, so a search is legitimate; likewise, those people who do not wish to become passengers are not searched.

Applied to similar security concerns, the district court ruling in *MacWade v. Kelly* outlined the paradigm by which the government's police powers may typically outweigh a fundamental right (in *MacWade*, privacy): when the needs of the government are "of the very highest order" and the means it uses to implement its powers are narrowly tailored to the ends. The ruling established that the New York City subway system container inspection policy only "minimally intruded" on privacy and yet was the most effective way to prevent a terrorist attack like that of the 2004 Madrid commuter train bombings. In other words, for a warrantless inspection program to be constitutionally valid, its purpose must be directed toward national security, rather than law enforcement, it must be the best means to achieving that goal in the particular context, and it must minimize its intrusion on privacy. Thus, privacy is not violated without consent, even though the consent is indirect, particularly because the search is suspicionless and not person-focused but applies to every passenger. Therefore, the special-needs exception can be said to permit warrantless, suspicionless searches in the event that the government has a vital need to perform the search, the means are tailored to the ends, and either the subjects have a diminished expectation of privacy or the test comports with a justifiable expectation of privacy.

This shift toward the purpose of the search marked a shift of jurisprudential thought toward searches and away from the focus in *Katz* and *Keith*, which Kerr refers to as "identity of who is searched or seized." Contemporary cases focus on the "relevant primary purpose" or "programmatic purpose" of the search and depth of the intrusion.

Although the special needs cases are relatively new, the court has long recognized certain suspicionless searches as legitimate. Notably, *Terry v. Ohio* paved the way for searches that, absent individualized suspicion, are legitimate without a warrant when the investigator has cause to believe that the circumstances (rather than the person)
are suspicious. The case concerned the legitimacy of an officer confiscating the concealed weapon of a suspect. Based on his years of experience, the officer determined that several men were acting in a suspicious manner (possibly planning a "stick-up"), and he elected to confront them about their activity; after further watching the two men, approaching them, and identifying himself as a police officer, he frisked Terry and found a concealed gun, which the officer confiscated and for which Terry was charged with carrying a concealed weapon. As for the authorization to frisk Terry and confiscate his weapon, the court ruled that the officer's conduct fell within the realm of scrutiny that typically is used when an officer frisks a person and confiscates a weapon: whether the frisking was for the police officer to protect himself from fatal injury and whether the confiscation was incident to a lawful search.

However, the search did not begin with the frisking; the search began when the officer noticed suspect behavior and acted to investigate further. As previously stipulated, in relation to the NSL program, Orin Kerr noted that the reduced scrutiny of the NSL program was related to the fact that it is dedicated to reveal suspects, rather than monitor known ones. Likewise, the court recognized that the police officer in Terry initiated his search in order to reveal a possible criminal, without a warrant, or even probable cause that a crime was being committed; his investigation was based on his expert opinion of suspicious behavioral patterns.

The court investigated the Terry search "at its inception" because, as Justice Warren noted, it "has held, in the past that a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope . . . The scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible." In Terry, Justice Warren explains, it was not necessary that probable cause be established to justify the search, because, as he wrote, "[W]e deal here with an entire rubric of police conduct—necessarily swift action predicated upon the on-the-spot observations of the officer on the beat—which historically has not been, and, as a practical matter, could not be, subjected to the warrant procedure." If the investigator (such as the officer in question in Terry) can point to "specific and articulable" facts that warrant the intrusion, he may "approach a person for the purposes of investigating possibly criminal behavior even though there is no probable cause to make an arrest." Thus, once an officer's "specific reasonable inferences" about a situation tell him
that investigating that situation is "reasonably related in scope" to the prevention of a crime, with no time to obtain a judicial order, he may take reasonable steps in investigating the likelihood of a crime being committed. Terry, marking a departure from person-focused searches to pattern-based searches, represents the justification for a warrantless search in order to reveal a possible crime, as opposed to searches based on a predetermined probable cause for one.

Conclusions: Authorizations and Boundaries for Searches of Transactional Data

We can conclude that there are certain circumstances under which a warrant is unnecessary for the government to conduct a national security-related search. Authorized to declare an emergency with respect to a specific threat and to investigate financial data that may be related to terrorist plots, the intelligence community's transactional surveillance may or may not require a warrant. If a warrant is not required, then the search must not involve U.S. persons or it must be "reasonable."

The circumstances under which a warrant is unnecessary for transactional surveillance can be summed up as follows: when there is no connection to the United States or a U.S. person, when there is reason to suspect that outside parties are capable of obtaining the data, and when the purpose of the surveillance is for a greater need than typical law enforcement and the intrusion on privacy is minimal. That is, the role of U.S. citizens, the need for the government to violate privacy, and the extent to which it is violated are the three most notable tests that must be passed for warrantless surveillance to be considered reasonable and constitutional.

The central question that remains is whether data mining of financial transactions fits into one or more of these circumstances, and to consider the consequences of allowing such surveillance.

Implementation and Need for Surveillance

As determined in the previous section, the implementation of transactional data mining must not have a U.S. connection, or the needs of the government to protect national security must outweigh the violation of privacy in order for a warrantless system to be implemented. This section will examine the practice and capabilities of
data mining with regard to its connection to U.S. persons, its need, and the extent to which it violates privacy.

**Data Mining: Use by the Intelligence Community**

The National Security Agency (NSA) "provides intelligence to other civilian and military agencies and officials" using "computers to collect massive amounts of data" by "sophisticated key-word searching and other techniques" referred to as "data-mining." 69

Orin Kerr offers a concise insight into how data-mining actually works:

Whereas traditional phone calls required a closed circuit between the parties, modern communications networks work by breaking down communications into packets and sending them across a sea of connected computers... Packets are really just strings of zeros and ones, each equivalent to roughly a page of information... begin[ning] with a "header," roughly equivalent to the addressing information on a letter... [including the packet's] origin and destination IP addresses... and other similar information... followed by the payload of the packet, which is the actual communication transferred.70

Thus, the information personal to the surveillance subject and the content of the communication sent is stored separately in the signal transmitted. These signals can be tracked with supercomputers such as the NSA's. Each Internet signal is sent from a computer connected to the Internet, which "breaks the communication into packets... [which] are then shuffled along by computers known as 'routers' that... direct the packet along the path that seems likely to get the packet to its destination most quickly."71 Kerr explains, "Packets are often routed across the country or even across the world," suggesting that a signal from a user in Pakistan could be routed through computers in the United States, or vice versa.72 The conclusion, Kerr notes, is that "today's surveillance tends to be divorced from the identity and location of the parties to the communication," and that data-mining is therefore focused "for known traffic characteristics rather than known identities" or locations.73 This shift in technology and policy opens the door for a departure from the person-focused surveillance model to a "programmatic purpose" one. This implies that searches of known traffic characteristics fall into a Terry search paradigm, and data divorced from location cannot be determined to be a domestic investigation.
For domestic law enforcement, the Federal Bureau of Investigation (FBI) used a similar program “to intercept information passing through the Internet, including e-mail, attached documents, and instant messages” that can be programmed to “intercept and collect specific messages that are of particular interest to the FBI, such as those sent from a particular network or e-mail account” provided that the FBI has “obtain[ed] judicial authorization in the form of a warrant identifying the nature of the subject matter to be intercepted.”

Similarly, for national security surveillance, an NSA supercomputer, consisting of “a network of computers that [may have been] used to process intercepted signals” that could include “all forms of global communication, including land-line and cellular telephone calls, satellite communications, electronic mail, facsimiles, and various forms of radio transmission.” According to reports, the NSA efforts “also [tie] into data from an ad-hoc collection of so-called ‘black programs’ whose existence is undisclosed . . . Among them [may be] a long-standing Treasury Department program to collect individual financial data including wire transfers and credit-card transactions.”

The data filtered by these programs is too complex and voluminous for human analysts to sift through, so the programs are used “to filter [criteria-conforming] data before it is seen by a human analyst.” The umbrella under which these programs fall can be described as a “dictionary computer” designed to “automatically extrapolate interesting pieces of intelligence,” and when the data sifted meets a predetermined “target criteria,” it is sent automatically “to the agency that specifically requested it.” Thus, a pattern is investigated, not a particular person, and no person is sifting through the data, but rather a machine.

To give an example of pattern-based searches in the realm of terrorist financing, the Treasury Department is aware of patterns indicating threats that could be used in a similar system (if it is not already). For example, Suspicious Activity Reports (SARs) and other Bank Secrecy Act (BSA) information can be compiled to determine suspicious patterns. The Financial Crimes Enforcement Network (FinCEN) has publicly provided outlines of several cases in which terrorist financing took on a set pattern, such that that pattern could be used to track future cases, for example:

Use of a business to collect and then funnel funds to a smaller number of foreign beneficiaries, both individual and business, in a Persian Gulf State;
Use of a business account that would not normally generate the volume of wire transfer activity, into and out of the account, as reported;
Use of a business account to make payments to a brokerage firm;
Large currency withdrawals from a business account not normally associated with cash transactions; and
Funds generated by a business owned by nationals of countries associated with terrorist activity.82

Thus, FinCEN could use this or other patterns to reveal terrorist financing in other contexts, or even determine patterns using sources other than SARs or even unrelated to BSA requirements or institutions to determine patterns indicative of terrorist financing. Those patterns could then be ranked in terms of the likelihood to involve terrorist financing and the highest risk patterns could then be explored after obtaining a FISA warrant for the specific actors engaging in those patterns.

Data-mining can fall into one of two categories. The first is when law enforcement and the intelligence community gather intelligence on subjects already being investigated at an accelerated pace ("subject-based searches"),83 reflecting the person-focused approach of the traditional warrant system. The second means of using data-mining can be called "pattern-based" and is used when "the government investigator develops a model of assumptions about the activities and underlying characteristics of culpable individuals or the indicators of terrorist plans. The government official then searches databases containing transactional and personal information" to find instances of personal and transactional behavior matching the pattern determined to exhibit threat behavior.84 Thus, the method to reveal a threat is a warrantless pattern-based search based on the threat expertise of the investigator, much like the officer's expertise in the Terry case.

**Terror Financing: The Threat Posed by the Internet**

The Internet—used for legitimate and illicit financial transfers—poses an affordable, accessible, omnipresent, and sparsely regulated comprehensive means to achieving legitimate and illegitimate goals, including the raising of capital. As previously discussed, financial transactions represent a unique area of constitutional legitimacy, and financing is a primary means to facilitating terrorist threats to U.S. national security.
As Todd Hinnen observes in *The Cyber Front in the War on Terrorism*, terrorists use the tools presented by the Internet in four notable ways:

1. They solicit donations, indoctrinate adherents, share information, and recruit supporters directly via websites, chat groups, and targeted electronic mailings;
2. They take advantage of charitable organizations, soliciting funds with the express purpose of clothing, feeding, and educating a population, but with the covert intent of exploiting contributors’ largesse to fund acts of violence;
3. They perpetrate online crimes such as identity and credit card theft, intellectual property piracy, and fraud, and support their mission with the proceeds of such crimes; and
4. They use the Internet as a pervasive, inexpensive, and anonymous medium of communication to organize and implement fund-raising activities.  

Many of these uses are legitimate on their face, but they are used for nefarious ends, making them difficult to identify as threats without a method to reveal them as different from the legitimate uses these acts would satisfy in other circumstances. While the uses of the Internet by terrorists are diverse, most are difficult to identify with a person-focused approach; the nature of these uses lends itself more toward a data-driven surveillance system to investigate them. When law enforcement and the intelligence community investigate the patterns associated with these practices, they are confronted with several problems, some of which are exacerbated by the current framework of the warrant system.

First, the Internet is inexpensive, which not only allows the opportunity for use by many users but also increases the incentive for Internet Service Providers (ISPs) to maximize their customer base while minimizing overhead, making it unlikely that they will require their subscribers to provide thorough identification or to monitor or save such records. Thus, it is unlikely that, even with a warrant, the necessary records would be available to seize retroactively.

One of the most fundamentally significant impediments to a person-focused approach to intelligence gathering is the capacity for the Internet to hide the people involved in the transaction, as well as their location. Internet users can enter into transactions anywhere, encrypting the transaction and concealing their identities; meanwhile, the signals of their transaction can potentially travel through
routers at any location, foreign or domestic. An Internet user can adopt multiple online identities,\(^87\) provide inaccurate identifying information,\(^88\) or use an easily available anonymizer, "which replaces the IP address for the user’s home computer with another IP address that cannot be traced back to the user."\(^89\)

Key to determining whether or what type of warrant is required for a search is determining whether the user is a U.S. person and if the transaction is taking place in the United States. However, the Internet poses a serious impediment to determining location in several ways. As Kerr points out, "If I am in Washington and request a webpage from a webserver in Chicago, the packets of traffic may travel to California or even a foreign country in the course of delivery,"\(^90\) making the interception of the signal from any given router necessarily precede determining the origin or end location of the signal. In fact, one method of anonymization for users is "onion routing," which directs signals "from their source to their destination via a sequence of proxies . . . that reroute messages in an unpredictable path."\(^91\) Moreover, most of the signal traffic is routed through sources within the United States, so “[m]onitoring a particular river of packet-based traffic in the United States will pick up an incredible diversity of traffic, ranging from your mom’s family’s email to parts of an encrypted phone call sent from Afghanistan to Iraq."\(^92\)

Thus, two of the primary determinations before exploring a warrant-based surveillance method are the person surveilled and their location and origin. However, the Internet obfuscates both of these aspects, making them virtually impossible to determine until it could be too late. Moreover, investigations cannot be effective if location must be known before the search is initialized, and pattern-based searches are paramount to revealing threats.

**Internet-Based Surveillance: The Particular Problem Posed by Innovative Financing**

While a terrorist attack would unlikely be carried out just anywhere, it can certainly be financed from anywhere and cannot proceed without financial backing. Searching for transactional data under the warrant-based surveillance system is not only difficult but also it is virtually impossible given the means of financing in the digital age. The most notable impediment is the lack of regulation, which also accompanies a lack of information on various forms of finance.
First, terrorists may use online charities to raise capital. While some charitable organizations that may be used as vehicles for terrorist financing may file regulatory records in order to achieve charitable status, charities that are primarily online are not subject to the same scrutiny as brick-and-mortar charities, charities can mask what they contribute to both from law enforcement and from the donors, and online charities can base themselves anywhere in the world. Thus, finding information on individual charities, determining whether charities are being used to fund terrorism, determining the intent of donors, and determining the location of the charities and donors are all burdensome steps that would be necessary in a warrant-based search paradigm.

Additionally, there is a wealth of financial exchanges that can take place over the Internet, from standard mutual fund companies and stock trading to alternative remittance systems, all of which make it possible to mask intent or layer transactions to obfuscate the goals of transactions. Formal financial institutions, such as “securities and futures brokerages, mutual fund companies, and investment companies” are “included within the definition of ‘financial institution’ set forth in the anti-money laundering provisions of the Bank Secrecy Act (BSA), and pursuant to the USA PATRIOT Act” and therefore “must establish anti-money laundering programs reasonably designed to prevent their use for money laundering or terrorist financing.” Thus, for formal institutions, the records created by BSA-compliant institutions may be helpful after the national security investigation determines a particular transaction or person to be subject to the level of reasonable suspicion for a warrant.

However, the BSA guidelines neglect to prevent or regulate innovations in value transfers, such as new or underground forms of financing; many of which would likely be aided by or specifically designed to use the Internet, therefore not legally requiring substantive—or any—regulation or information. For instance, in virtual worlds, such as Second Life or Entropia Universe, “millions of users can interact with each other,” including participating in “virtual economies” to “conduct financial transactions” where virtual currencies can be exchanged for real currencies and new marketplaces are created that terrorists can use relatively unregulated. These systems require user consent to use them (diminishing their expectation of privacy as in the case of an airport search) and are virtually impossible to investigate without first engaging in a pattern-based search.
Informal value transfer systems, such as hawala, are "reliable, efficient, anonymous, and available twenty-four hours a day, seven days a week." Hawala, simply an informal fund-transferring system used particularly in areas where bank regulations would be too burdensome, are commonly used as a remittance system for expatriates sending money home to their families, but the lack of regulation makes them vulnerable to terrorist financing as well. Billions of dollars are exchanged through informal value transfer systems, with little knowledge about the customers and recipients. However, given that the primary attraction to these systems is their lack of regulation, including them in BSA guidelines would most likely almost eliminate use, driving illicit transactions further underground and stifling legitimate development in impoverished areas. According to Hinnen, "Although the vast majority of hawala transfers are legitimate... experts believe that much of al Qaeda's funds for September 11 transferred through hawalas in Dubai and that terrorist organizations continue to use hawala to transfer funds." While many hawala transactions are done in cash and arranged over the phone, any wire transfers used to replenish a hawaladar's reserves could be useful in stopping a threat. Thus, innovative financing presents a unique problem to traditional surveillance methods that suggests that investigations of such transactions must be data-focused, rather than person-focused. However, the means to investigate financial data through a pattern-based approach falls into the category of a "reasonable" search, as their programmatic purpose and minimal invasion of privacy align with the reasonableness paradigm outlined in previous case decisions.

Conclusions and Analysis: Justification for Warrantless Transactional Data Mining

As we have seen, from a policy perspective, transactional surveillance is not only of the highest importance (one of the key means to stopping plots such as 9/11) but also virtually impossible to perform within the typical warrant-based search paradigm. The person and location of a given transaction can be completely masked, while an unregulated transaction system can be used without formal records of the actors or places. In order to stop transactions for terrorist financing from taking place and to find and stop those performing them, a data-mining approach is paramount, and the warrant-based system is relatively useless.
When Judge Posner addressed this subject, he described the need for privacy with the metaphor of a photograph to represent online data. If a woman learns that a stranger has seen a naked photo of her before the photo was destroyed, she will still feel a violation of her privacy because it is the person-to-person privacy invasion and memory of the invasion that triggers an emotional feeling of violation. However, "in the initial computer sifting designed to pick out data meriting scrutiny by an intelligence officer, only facts bearing on national security will trigger scrutiny." Thus, the data-mining approach to surveillance recognizes the shift in communication since the eighteenth century: there is no longer a person violating the privacy of another person, and there are no longer two specific and known interlocutors involved. The Framers were concerned that biased investigators would improperly violate the privacy of innocent citizens; data mining does not allow for bias because the computer cannot be biased, it can only recognize a predetermined pattern, and once a human is made aware of the threat, he or she must obtain a warrant before investigating further or engage in an otherwise reasonable search.

A transactional pattern designated by national security authorities as prone to terrorism financing could be used, similarly to the expertise of an officer such as the one in the *Terry* case being used to determine suspicious behavior. The pattern would be authorized pursuant to IEEPA and EO 13224 authority, to sift through massive amounts of financial data payloads and identify transactions fitting a risk pattern without a warrant. Once that program identifies the threat risk transactions, an intelligence officer can be notified and a FISA warrant could be issued to decipher the headers to determine the people involved. In that way, the only time the intelligence officer would see the personal information related to the search (the person-to-person violation of privacy) would be after a warrant was issued based on the initial search. This falls into the *Terry* paradigm because it is to reveal a threat based on reasonable suspicion, and once the suspect himself or herself is singled out, the standard regulations apply (such as the officer needing to confiscate the gun incident to a lawful search being similar to the person whose pattern triggered an alert being investigated further with a FISA warrant).

As previously discussed, the courts have designated lawful warrantless searches as those of non-U.S. persons, and those where the violation of privacy is reasonable in comparison to the threat and the means to addressing it are narrowly tailored. Given that the
location of the person and the transaction can be hidden, can be anywhere, or can travel through foreign countries and the United States, it is difficult to say that an initial data-mining search lacks a foreign nexus or is not completely foreign-based. Thus, the results of a search may fall within the Verdugo paradigm of not needing a warrant, but the investigator could not possibly know that until the search is performed.

Moreover, the programmatic purpose of the search would not be to catch Bernie Madoffs, but Osama bin Ladens (interdiction vice prosecution), and therefore it is more analogous to a national security “special needs” search, such as public safety screening in New York City subways, than a warrantless search of a suspected drug dealer’s car. The need for the government to determine the financing of terrorist plots must be agreed to be as dire as the need to investigate drug use among railroad workers, and, given the anonymity of the Internet and innovations of new types of financing, the means to finding threat financing require a pattern-based data-mining approach.

Finally, because the search is that of transactional data, it can already be said to be in the public view, as a third party is allowed access to the data (whether it be the financial institution; the medium, such as Second Life; or the Internet Service Provider routing the signal) and thus the transactor has an expectation that others will see the data. When opting to use the Internet for such a transaction, one is following a similar path to a potential passenger on a flight: the person is opting to use a public medium (the Internet) and thus diminishes his or her right to privacy, and if he or she wishes not to have that right diminished, they may not use the Internet. This prevents the Internet from being used to finance terror analogously to preventing airplanes from being hijacked.

As Orin Kerr suggests, surveillance methods should “correlate the likelihood that terrorist intelligence information will be collected with the invasiveness of the surveillance practice; the more invasive the practice, the greater threshold required.”104 Investigation of financial transactional data has been recognized as a minimal invasion of privacy, but it represents a significant need for the national security community. Kerr proposes that “Congress should enact two sets of surveillance rules: a data-focused regime when identity and location are not known with certainty, and a person-focused regime when identity and location become known.”105 However, within the data-focused regime, Kerr notes that “the special needs exception
may make a warrant unnecessary . . . [and] individuals monitored may lack a sufficient connection to the United States.” Financial transactional data clearly falls within one of these two exceptions and thus carves out a minimal threshold within the data-focused regime outlined by Kerr. The Treasury Department program mentioned in section two that (assuming it exists) monitors transactional data most likely operates under the assumption that this approach is constitutionally valid. If its constitutionality were challenged, it is my belief that the program is valid, even without a warrant.

**Implementing the Policy: Addressing Possible Concerns**

There are two primary concerns that need to be addressed if accepting the legitimacy of a warrantless data-mining policy: that it will be used for illegitimate reasons based on liberal interpretations of national security, and that there will be a chilling effect resulting from the fear of being investigated.

As previously stipulated, the program in question would be established, and the patterns determined, pursuant to the authorities granted by the IEEPA, the USA PATRIOT Act, EO 13224, and others, and any individual misusing the program outside of those authorizations would be punished as any other person using a national security investigation for improper ends. To address these concerns, Richard Posner suggests that the programs themselves be subject to a FISA court approval, rather than each search, which may prevent biased patterns from being developed. However, given that the people identified as threats could only be investigated personally if a warrant were issued after the program identified them, it is unclear that this is even necessary.

As for the chilling effect, Posner acknowledges that there may be less people willing to discuss terrorist activities over the Internet, even if their discussion is innocent rather than planning a terrorist act. He dismisses this as an issue because, once people “realized the scope of the agency’s program,” they would recognize that their conversations would be discarded before a formal investigation were launched. However, I am skeptical that the public would so readily accept the limited scope of the problem and that the chilling effect resulting from data mining of communications may raise legitimate First Amendment concerns. However, the concerns are less severe with a program focused on transactional data. First, as previously discussed, transactional data are subject to lower scrutiny
than speech (as in *Smith v. Maryland*, etc.). Second, any chilling effect resulting from public knowledge of the program would not deter speaking on the topic of the interlocutors' choice, but rather hesitancy to engage in transactions that the transactor believes may be risky. While this may have a moderate dampening effect on legitimate charities or investments in emerging economies, it is likely that that dampening would decrease over time as more information is made public on the legitimacy of the charities and the soundness of the investments. Meanwhile, a strong government interest will have been served.

Thus, while these concerns are certainly legitimate, they fail to acknowledge the basis of the initial search falling into the *Terry* pattern-based paradigm and then requiring a warrant for person-based investigations and also the lower scrutiny given to transactions.

**Notes**

5. Ibid.
6. Professor, George Washington University School of Law.
7. Judge, U.S. Court of Appeals for the Second Circuit; senior lecturer in law, University of Chicago.
10. Ibid.
11. *Youngstown Sheet & Tube Co. v. Sawyer* (“Steel Seizure Case”), concurring opinion of Justice Jackson.
15. Ibid.
16. Ibid., at note 4.
17. Ibid.
18. Ibid.
19. Ibid.
22. Ibid.
24. Ibid., at note 21.
31. Ibid.
32. Ibid.
33. Ibid.
37. Ibid.
38. Ibid.
39. Ibid.
40. Ibid.
42. Ibid.
44. Ibid.
47. Ibid.
50. Ibid.
51. Ibid., at note 9 (emphasis added).
54. Ibid.
57. Ibid.
58. United States v. Davis, 482 F.2d 893.
60. Ibid.
63. Ibid.
64. Ibid.
65. Ibid. (citing Warden v. Hayden, 387 U.S. 364 [1964]).
66. Ibid.
67. Ibid.
68. Ibid., at note 62.
69. Ibid., at note 27.
71. Ibid.
73. Ibid.
Analyze FBI's E-mail Surveillance System for Safeguards," Chicago Tribune, September 27, 2000.

75. Ibid.


77. Ibid, at note 74.


80. Ibid.

81. Ibid.


84. Ibid.


86. Ibid.


88. Ibid.

89. Ibid., at note 86.

90. Ibid., at note 9.

91. Ibid., at note 84.

92. Ibid., at note 9.

93. Ibid., at note 86.

94. Ibid.

95. Ibid. Hinnen notes that the reader should see 31 U.S.C. §§ 5313(a) (2), 5318(h) (2000).


97. Ibid.

99. Ibid.


101. Ibid., at note 8.
102. Ibid., at note 8.
103. Ibid., at note 8.
104. Ibid., at note 9.
105. Ibid., at note 9. Kerr references Judge Posner (Ibid., at note 8).
106. Ibid., at note 9, footnote 70.
107. Ibid., at note 8.
108. Ibid., at note 8.
109. Ibid., at note 8.

**Ryan B. Greer** is currently a State Department employee. The views expressed in this article are his alone and do not reflect those of his current or previous employers or the U.S. government. Greer holds a master of public policy degree from Georgetown Public Policy Institute and a B.A. in government from Skidmore College.