Introduction

Secrecy is a powerful tool. Information known to one party but not revealed to others gives the knowledgeable party leverage, insight and, therefore, power over the other party. Secrets have helped governments wage war and maintain power throughout history, and the current political climate regarding counterterrorism is no exception. The terrorist attacks of September 11, 2001, served as the justification for administrations around the world to keep secret their controversial and sometimes outright illegal counterterrorism programs. Secrecy is power for individuals as well. Even within a democracy, the right of individuals to keep secrets over their private matters is essential to maintaining freedom of thought and speech. After September 11, two dynamics emerged in many democratic nations: the power of administrations and central governments to keep their activities secret from the public increased dramatically, and governments increasingly saw the ability of individuals living within democracies to keep secrets as a threat. The result after sixteen years is governments holding more secrets than is legal or wise, while individuals are often not allowed to keep their own.

The years since the September 11 attacks have seen a massive increase in the authority granted to and taken by central governments to exercise counterterrorism measures, without a concomitant commitment to oversight and accountability. The result is too much secrecy allowing for abuses and inefficiencies to be covered up. When controversial and arguably illegal government actions occurred in the United States under the Bush and Obama administrations in the implementation of national security policies – including in areas of targeted killings, torture, indefinite detention, extraordinary rendition, warrantless wiretapping, and surveillance – national security secrecy often prevented discovery of those actions. Even when these problematic actions were made public, genuine accountability over abuse remained elusive: secrecy manifested in nondisclosure of counterterrorism policies; executive branch decisions providing legal justification for secrecy were themselves kept secret and beyond oversight; procedural and doctrinal barriers, as well as broad invocation of the state secrets privilege, prevented litigation from progressing beyond the pleadings stage; and judicial reluctance to demand transparency over national

security matters glossed over executive overreaching and undervalued the harms to civil and human rights. This book addresses these problems from a historical, legal and comparative perspective.

Chapters 1 through 3 consider national security secrecy from the U.S. domestic perspective, examining the executive, legislative, and judicial branches, respectively. Chapters 4 through 6 shift the analysis outward. Chapter 4 takes up United Nations and European Union norms for transparency in the area of national security matters. Chapters 5 and 6 consider how international and domestic forces – both legal and political – affect national security secrecy in the United Kingdom and India, respectively. Chapters 7 and 8 consider two other aspects of national security secrecy. Chapter 7 considers how secrecy is enabled by the outsized fear of terrorism that has manifested in the public and political classes in many democratic nations, and Chapter 8 considers how the devaluing of personal privacy by companies and governments alike has inverted the structure of democracies: we have been rendered transparent to our governments, and national security secrecy prevents us from even understanding the extent of it. Together, these chapters illustrate the growth, manifestations, and challenges of national security secrecy, and consider ways in which national security secrecy must be scaled back to preserve democratic values and protect fundamental rights.

**

We live with an overlapping, multifaceted architecture of national security secrecy. As then–U.S. Secretary of Defense Donald Rumsfeld once observed with regard to national security threats, "there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones."[1] Perhaps ironically, Rumsfeld's description could also apply to the multi-layered construct of national security secrecy: the "unknown unknowns" are those policies – and any abuse of those policies that compromises human and civil rights – that are kept entirely secret from other branches of government and the public, thereby shielding the government from effective oversight and accountability. Often the "unknown unknowns" become known only through public disclosures years later, or leaks by those with access to the information. To offer just one example, when National Security Agency (NSA) contractor Edward Snowden's disclosures of domestic surveillance practices were made public in June 2013, it became abundantly clear how effective the national security secrecy architecture had been. All three branches of the U.S. government had worked together in ways that kept the surveillance programs obscure and out of the public light. The executive branch generated its own legal interpretations that the relevant statutes authorized broad collection and storage of the telephonic metadata of all U.S. persons. Much of that

legal interpretation remains secret, although the Snowden disclosures prompted partial publication of the legal authority to conduct other warrantless surveillance. Prior to the Snowden disclosures, members of several House and Senate committees had some access to the NSA and the opportunity to learn about the parameters of the NSA's metadata program, but were not allowed to discuss the program publicly. The Foreign Intelligence Surveillance Court, at that point a non-adversarial court with secret proceedings, approved the implementation of the NSA metadata program after demanding some modifications. Those court opinions were kept secret until public pressure stemming from the Snowden disclosures prompted their disclosure. The program itself was kept largely secret from the public, but the maintenance of the program as this kind of "unknown unknown" was only made possible by the fact that the mechanics of governance and oversight – as such – were themselves kept secret.

After the Snowden disclosures, all branches of government moved in the opposite direction – of demanding accountability over the NSA. Yet the government actions and the prolonged public discussion of privacy and security following the Snowden disclosures, and the NSA reforms enacted in 2015, were triggered not by an effective accountability mechanism that was already in place; to the contrary, society depended on the illegal and allegedly criminal leaks of a contractor to understand more fully what type of surveillance has been taking place and to have a real discussion as to whether that surveillance comports with societal priorities and values. Only after the Snowden disclosures began did plaintiffs alleging unconstitutional surveillance have standing to have their cases heard in court. Because the secrecy over the NSA programs had broken down, these plaintiffs were in a significantly better position than individuals subjected to extraordinary rendition and torture on U.S. orders, or those put on the U.S. government's list of suspected terrorists who may be subjected to targeted killing. Those individuals – some of whom have suffered tremendous human and civil rights abuses – have been unable to bring cases against the government because of the secrecy that still surrounds those programs. This is illustrative of a system in which secrecy is valued too highly, resulting in unchecked abuse and government overreaching in ways that have not been shown to be necessary to maintain national security, yet are undercutting U.S. claims of adherence to the rule of law.

**

The basic premise of a democracy is that the power to decide what the government does resides with the people; the government's actions are limited by the parameters set by the constituents, and the people understand what the government is doing to govern. A corollary principle is that in liberal democratic societies such as the United States, the United Kingdom, and India, people have chosen a structure of government that affords equal protection of the law, and values privacy and the right to live a largely private life. These conceptions of the rule of law demand that the

government adhere to the principle that the right to privacy ought not to be violated by the government without individualized cause and without mechanisms of accountability that can work to ensure that any undercutting of those privacy rights is justified, and that government power is not abused.[2]

We can imagine a situation in which a government engages in a high level of control over a population in a democratically elected country, but the constituents can see and fully understand the level of control to which they are being subjected and have the option of changing that level of control through the democratic process. Under those circumstances, we could still conclude that the transparency with which the decision-making is occurring means that democratic principles are at work, at least in a weak form. In this hypothetical world, let us assume that aspiring politicians hit the campaign trail and tell us with some specificity that in the name of national security, they will authorize and engage in programs that will monitor our private communications without a judicial warrant; store available internet and telephonic data concerning us for years in ways that would allow such data to be searchable by intelligence agencies without a warrant; and create various programs involving the profiling, harassment, detention, abuse, torture, financial ruin, and sometimes targeted killing of certain U.S. citizens and non-citizens, and that many of those programs have little or no track record of actually bolstering security. Let us also assume that politicians make clear that the targets of profiling, harassment, torture, and targeting killing will overwhelmingly be drawn from certain religious and ethnic minority populations that have little political clout but, since September 11, have been viewed with skepticism and suspicion by a significant swath of the U.S. electorate.

Let us then assume that we elect those individuals to Congress and the presidency anyway. We certainly would not have equal protection of the law or a protection of the privacy rights that underpin free thought and expression, and, therefore, would not have a society that upholds the liberal democratic values to which we have committed. We would, however, have some level of transparency.[3] As a nation, we would have arguably agreed to trade away a commitment to equal protection, due process and privacy rights in electing these politicians, yet at least some aspect of democratic control over the actions taken by government in the name of national security would be maintained. In such a hypothetical situation, we could rely on a public change of sentiment, or the courts, or Congress armed with an understanding of these publicly known programs, to take action – through applying public pressure, legislation, impeachment, or litigation – to correct some of the abuses of domestic and international law that may be occurring.[4]

Yet national security-related policies in the United States have distorted both of these concepts of democracy: the exceptionalism that is consistently invoked in the national security context has justified programs that do not comport with our ordinary understanding of the legal, structural, and value constraints our society places on the government, and the secrecy with which certain programs are

conducted inverts the democratic structure of transparency in ways that undermine the effectiveness of our governmental structures and lessen our commitment to a society based on the rule of law.

Why have we allowed these two enormous shifts? The most basic justification is fear, specifically fear of another terrorist attack after 9/11.[5] This has motivated a shift in substantive laws and policies away from a largely crime-based model in which terrorist acts are – for the most part – investigated after the fact and dealt with as most other serious and violent crimes, like murder or sexual assault. Instead, the post–September 11 focus of law and policy has been to move national security investigations toward a preventive model that is predicated on zero tolerance for terrorism. This shift is predicated on a type of national security exceptionalism: with other violent crimes, there can be no serious suggestion that the law ought to move in the way that national security law moved. As a society, we do not believe that a murder rate of zero in the entire United States is the only acceptable outcome.[6] Instead, with crimes such as murder, we try to create a balance:[7] we have laws and a structure in place that will and prosecute murders in ways that attempt to punish offenders, promote justice, and deter those acts in the future. Based on history, education, and experience, we hope that these steps keep the murder rate down, but we don't craft our laws and policies to suggest that one murder in a city per year means that the law has failed.

Yet that is precisely what we do when it comes to terrorism. With a societal and political zero-tolerance for terrorism in the post–9/11 context, the Bush, Obama, and Trump administrations have pushed the boundaries of national security exceptionalism in separate ways to suggest that a different set of laws and rules apply to government counterterrorism efforts, and that the public does not have a right to know what those laws are. Congress, for its part, allocated vague but expansive powers to the government immediately after September 11; until mid-2015, there was little legislative success in curtailing these powers.[8] Courts have generally reified and justified this national security exceptionalism by allowing executive branch policies to go unchecked for many years, except in the most egregious of circumstances.[9] At the same time that these vague and expansive powers have been allocated to or simply asserted by successive presidential administrations, the high pressure put on intelligence agencies to find terrorists before they strike or even make significant headway in their planning has not abated.[10] Finally, administrations have defined terrorism and related crimes broadly to encompass all kinds of activity, such that making a donation to a charitable organization can result in a terrorism-related conviction.[11]

The same zero-tolerance posture stemming from the fear of another attack has also justified the layers of secrecy surrounding national security laws and policies. Certainly national security secrets are often genuinely necessary to maintain the integrity of a particular program or policy, gain a tactical advantage, or simply protect the individuals involved in running a program.[12] I do not argue that open

government principles ought to be applied at their strongest in the national security context; however, we ought to ask harder questions as to whether national security secrecy as it has manifested in our post–September 11 political and legal culture is necessary and appropriate, or whether aspects of that secrecy have been so corrosive that they need to be substantially curtailed by improving institutional incentives and structural constraints.

TYPES OF NATIONAL SECURITY SECRETS

Our starting point is understanding that there are numerous national security secrets that have been kept by the post–September 11 presidential administrations. Further, if we understand that the basic definition of a law is a rule that sets parameters for behavior of the government or businesses or private individuals, then many of the policies and interpretations that authorize and limit counterterrorism activities and national security programs should be thought of as secret laws. Donald Rumsfeld's views on "known knowns," "known unknowns," and "unknown unknowns"[13] provided a means by which to consider, categorize, and assess national security secrets.

David Pozen uses Secretary Rumsfeld's framework in considering the possibility of a spectrum between deep and shallow government secrets,[14] which, given the nature of national security policy-making, would be held by the executive branch. Deep secrets, which would include Rumsfeld's "unknown unknowns," might encompass counterterrorism activities such as the waterboarding of detainees by the U.S. government. The existence of a waterboarding protocol was kept secret from the public and other branches of government and, in fact, actively denied by the Bush administration until information about the protocol was leaked to the public. Once its existence became known, it became a shallow secret or a "known unknown" – a program about which the existence is known to the public, but about which much remained secret. As more information about U.S. waterboarding of detainees continued to be made public, even over a decade after the waterboarding commenced,[15] the whole program became a shallower secret.[16]

There are many secrets that start out and continue as shallow secrets in national security and counterterrorism work. Examples include specific military or counterterrorism strategies; we know that law enforcement and intelligence services personnel use in-person surveillance to investigate domestic terrorist groups, but we often don't know the specific targets of that surveillance or particular methodologies of surveillance. This shallow secrecy is sometimes rightfully justified from a utilitarian perspective by the idea that the programs' effectiveness is predicated on some level of secrecy, without which the targets of investigation would simply outmaneuver the government.[17]

So, at least in some instances, shallow secrets are validly held and are often accompanied by adequate oversight and accountability mechanisms that help ameliorate the antidemocratic concerns of operating in secret. Deep secrets, on

the other hand, are problematic from a transparency perspective and are almost always troubling with regards to accountability, democratic governance, and the rule of law. In order to consider more fully whether instances of national security secrecy are problematic from a rule of law perspective, however, we need to add the gloss of analyzing how national security secrets – particularly those that constitute a secret law or policy – are developed, deployed, and justified by the government. I offer three interconnected and overlapping ways in which I see these secrets developing and being maintained, all of them justified in various ways by the Bush and Obama administrations as necessary and legal even though they represent an exceptionalist view of the power that should be allocated when it comes to national security-related matters.

First and perhaps most obviously, we have secrets based on a straightforward lack of disclosure by the government. These could be deep secrets, in which case the public is not even aware that a secret is being kept, or shallow secrets, in which case the public has some sense of what type of information is being kept secret. This type of straightforward secret is characterized primarily by the administration simply not letting Congress, ordinary civilian courts, or the public know about a policy or program. In the first instance, the CIA detainee waterboarding program, at least when it began in 2002, fell into this category.[18] Likewise, the Bush administration's Terrorist Surveillance Program, a warrantless surveillance program that was put into place in late 2001, was predicated largely on the assertion that the president had Article II constitutional authority both to decide whether such a program is necessary and whether to tell any other entity – including Congress, courts, or the public – about the program.[19] Both of these programs moved from being deep secrets to more shallow secrets as information was leaked to the press and the public more generally. Notably, once they became public, these two programs were viewed with disfavor by courts, subsequent administration officials, Congress and much of the public. All of these actors have found them to be largely unnecessary, unauthorized, and in violation of existing statutes, if not constitutional and international legal constraints as well.

Second, we have secrecy that is created or maintained based on misinformation or misleading partial disclosures by the government. This type of secrecy is particularly corrosive given the fact that it includes an administration actively concealing information when another branch of government is trying to exercise its oversight authority. As discussed earlier, Snowden's 2013 disclosures of surveillance practices made clear how effective the national security secrecy architecture had been, perhaps because inadequate oversight measures lulled us into believing that accountability existed even when it did not: the executive branch ran its surveillance based on its own secret legal interpretations; members of Congress that had access to the NSA and the opportunity to understand the parameters of the NSA metadata program were not allowed to discuss the program publicly, even during oversight

hearings; and the Foreign Intelligence Surveillance Court issued secret opinions validating the program.

Before the Snowden disclosures, publicly known oversight was in some ways a vehicle for the government to give misinformation in order to protect its secrets. One prominent example stems from a Senate oversight hearing on March 12, 2013, in which Senator Ron Wyden specifically asked Director of National Intelligence James Clapper if the NSA was systematically collecting information on the communications of millions of Americans.[20] Clapper denied this, yet subsequent revelations by Snowden confirmed that the broad scope of the data collection included metadata for telephonic communications, as well as content data for emails, texts, and other such writings.[21] After public discussion of the discrepancy in his testimony, Clapper commented that he gave the "least untruthful" answer possible under the circumstances.[22] Senator Wyden expressed disappointment and frustration that Clapper misled the Senate while under oath at an oversight hearing.[23]

Third, we have secrecy that is created by the government's reinterpretation of the meaning of words in laws and policies in ways that differ from common understandings, and keeping secret the actual meaning being used by the government. Semantic dissonance occurs in U.S. law and policy regularly and has done so for centuries. We only need look at Thomas Jefferson's language in the Declaration of Independence that "all men are created equal" to see that the literal meaning of these words was not what Jefferson intended nor what contemporaneous readers of the Declaration of Independence understood it to be. Instead, the phrase might be more accurately understood along the lines of "all* men** are created equal***," since only white men who were landowners possessed the full legal rights to be afforded in the United States, and even were one to qualify, the law treated wealthier men with more privileges than others. However, the difference between the words on the pages of the Declaration of Independence and the meaning of those words that was given legal effect was not kept secret – to the extent that all women, non-white men, poor white men, or other men were being excluded from this aspirational language, that information was publicly available.[24] Ta-Nehisi Coates made a similar observation with regard to President Abraham Lincoln's aspirational language in the Gettysburg Address, in which Lincoln states that "the government of the people, by the people, for the people, shall not perish from the earth." Coates notes that, in 1863, "the people" did not include African Americans, and observes that "America's problem is not its betrayal of 'government of the people,' but the means by which 'the people' acquired their names."[25] In the post–September 11 national security context, we can see similar semantic dissonance, but without the ability to know whether the words that U.S. administrations have used to articulate the law surrounding counterterrorism programs mean what most people think they mean.

The United States has long been party to international treaties prohibiting torture as well as cruel, inhuman, and degrading treatment. Among them are the Universal

Declaration of Human Rights,[26] the Geneva Conventions,[27] the International Covenant on Civil and Political Rights,[28] the American Convention on Human Rights,[29] and the Convention Against Torture.[30] On the domestic level, the Fifth, Eighth and Fourteenth Amendments to the U.S. Constitution have been interpreted as prohibiting torture,[31] and various domestic laws codify the obligations in the Convention Against Torture: the federal Torture Statute,[32] the Torture Victim Protection Act of 1991,[33] the Alien Tort Claims Act,[34] and the Foreign Affairs Reform and Restructuring Act of 1998.[35] Yet President Bush's famous (or infamous) statement that "we don't torture"[36] would perhaps more appropriately be read as "we don't torture*" to reflect the Bush administration's temporary redefinition of "torture" as a narrow set of activities[37] that did not comport with the commonly understood international or domestic legal understandings of the term.[38]

Similarly, DNI Clapper's response of "no" to the query as to whether the NSA "collect[s] any type of data at all on millions or hundreds of millions of Americans" is better understood as a "no*" because Clapper and the NSA used a 1982 Defense Department regulation to define the word "collect" to mean the point at which searches – which are most certainly run through the database of information held by the NSA on hundreds of millions of Americans through its metadata program – provide results, and those results are analyzed by a person.[39] Leveraging this definition, Clapper offered the post hoc justification that "collection" does not occur at the point at which the data is gathered or even when algorithms are used to sort the data for relevance, even though a plain reading would suggest that the Defense Department regulation could be interpreted such that "collection" occurred at a number of points earlier in the NSA's data gathering and sorting process, since humans were actively querying the database of information.

When later pressed about his statement after the Snowden disclosures, Clapper stated that he understood that there were semantic differences in understanding what "collect" might mean under particular circumstances, and that, based on his understanding of the 1982 Defense Department regulatory definition, he had actually been honest in responding to Senator Wyden's question.[40]

These two examples offer slightly different but related understandings of how national security secrecy might exacerbate the problems of redefining words in unconventional ways. In the first example, the Bush administration's unconventional and later retracted definition of torture is kept secret from the public. The public attitude of the administration is one of substantive compliance with previously understood legal norms (i.e., "we don't torture"), but the law that actually governs the administration's decision making is substantively different and extreme in the way it defines torture, and is kept from the public. In this respect, the Bush administration's policy on detainee treatment and abuse is part of a body of secret national security law that congressional oversight and public

debate cannot reach without the benefit of a leak of the Office of Legal Counsel memoranda containing the Bush administration's new definition of torture.[41]

The second example, of DNI Clapper's semantic dissonance with regard to whether the NSA "collected" information in its metadata program, suggests a slightly different and perhaps more complicated problem. Senator Wyden attempted to engage in oversight of the NSA when he posed his question, but Clapper relied on the semantic distinction between the common understanding of "collect" and the Defense Department regulatory definition of "collect" to answer Wyden's question. Could Wyden have found the 1982 regulatory definition and used it to ask follow up questions of Clapper? Perhaps. But it seems clear that if Wyden had used any number of synonyms for "collect," such as "gather," or "intake and store," Clapper might not have been able to defend his seemingly disingenuous answer by leveraging a relatively obscure definition. In that sense, Clapper engaged in a type of *constructive secrecy*, where the legally operative meaning of a term may be theoretically available, but if the administration chooses not to volunteer the meaning that it uses, and if it's not clear to oversight bodies that a particular meaning would apply, then it is likely that the administration could retain secrecy around its policy while denying that any part of it is secret at all. The alternative, that Senator Wyden's staffers would dig through voluminous federal regulations to find each distinct definition of each and every word that Wyden uses in questions or that Clapper gives in response, is unrealistic and absurd, which only serves to increase the possibility of administrations using constructive secrecy to justify their actions and evade serious oversight.

These programs exemplify both substantive national security exceptionalism – the argument made by a President or administration that sometimes the government needs to run programs that may be in many respects above the law – and national security secrecy – the reality that even when Congress or another body tasked with effecting oversight asks direct questions attempting to learn about those programs, the administration may decide that it needs to lie, mislead, or misdirect questioners. Together, these two strands demonstrate the complexity and corrosiveness of national security secrecy to maintenance of the rule of law. The first type of secret described here – one of straightforward non-disclosure – is the kind that is often considered in debates regarding the need to create better oversight mechanisms for national security secrecy.[42] But in many respects, the second and third types of secrets undermine the rule of law to a further extent in the sense that congressional, judicial, or public understanding of a program or its limits may be based on an incomplete or faulty understanding of the parameters of particular national security programs. The public may believe that real oversight exists, even when it merely serves as a veneer of accountability and legitimacy.