ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# What Does it Take to Lead NSA’s Legal Team?

**Interviews and Profiles**

**Technology, Privacy, and eCommerce**



*Photo: Glenn Gerstell, center, with senior leaders from government and ACC. ©ACC Foundation*

---

It is an organization both respected and feared: the US National Security Agency (NSA). From its humble beginnings as a US Army unit charged with decrypting enemy codes during World War I, today's NSA stands at the forefront of technology, privacy, and national security issues. It has played

crucial roles in protecting the United States from foreign threats.

But the NSA's mass surveillance programs, as authorized by statutes such as the US Patriot Act, have also spawned great alarm. In an agency subject to increasing public scrutiny, what does it take to lead the NSA's Office of General Counsel?

The following is *ACC Docket*'s exclusive interview with Glenn S. Gerstell, NSA's general counsel from August 2015 through January 2020. Glenn shared his views on in-house counsel leadership and the future of national security.

## 1. In-house counsel leadership

Like many interviews, we start with background questions. This part goes fast — in the digital age, entire dossiers can be found online, and Glenn even has his own Wikipedia entry (he didn't write it).

There are a few surprises. For someone who became the NSA's top lawyer, I expected a long, prior career of government service. Instead, Glenn spent the bulk of it — nearly 40 years — as private sector outside counsel at the law firm of Milbank LLP.

Glenn, too, was surprised when he landed at NSA's legal top spot. "I didn't think I would get it," he said, admitting that he expected someone with more public service experience to get the position. "I'm not complaining."

I asked Glenn to share his take on meeting the legal needs for a key government agency. The takeaway: the NSA may be an organization shrouded in mystique, but its legal concerns are not unlike those facing other ACC member companies.

> "My clients deal in things you watch in movies," says Glenn. "But the legal side? We have the same issues facing other ACC members — from patents, to corporate law matters, to defending against litigation. I even dealt with the same staffing needs that other GCs face in running a lean department."

Almost ruefully, Glenn shares that, at the start of his tenure, NSA's legal team only had 55 lawyers — "woefully under-resourced" — as he puts it. Changing that became one of his strategic goals. By the time he left, nearly five years later, his team had grown to over 100.

*(Author's Note: Glenn mentioned litigation disputes. Many of my Loyola Law School students know of my favorite trademark case involving the Agency. In 2011, a small business entrepreneur started selling t-shirts featuring a stylized version of the NSA logo and the caption: "NSA: The only part of government that actually listens." The NSA demanded he stopped using the logo. In the ensuing lawsuit, the entrepreneur prevailed on First Amendment parody grounds. Glenn was NOT the GC then.)*

Despite the similarities between Glenn's GC duties to those of ACC's private sector members, there are also differences. "Most companies focus on achieving their own needs and goals," he says. "Their mission is to make money for their shareholders."

For example, most private companies do not, and often cannot, coordinate their business goals with other businesses. Federal agencies, however, dance to a different beat. Government agencies share

the same overall goal to promote the safety and prosperity of the country.

> “But each agency may have a different view of how to achieve this mission,” notes Glenn. “The Department of Commerce (DOC) may have one opinion on achieving that goal, which may differ from the NSA’s, which may differ from the Department of Justice (DOJ).”

He acknowledges that the presence of so many institutional stakeholders often makes coordination tough. For example, much of his team’s time was spent negotiating consensus across different federal agencies. But developing such consensus achieves an important goal. He shares the cyber-related concerns involving the Chinese company Huawei and 5G communications.

Potential threats posed by foreign influence on our communications backbone is an issue that cuts across multiple federal agencies — even cuts across the nation. But Glenn believes the US government’s response to these issues must be coordinated and consistent.

> “It takes significant work to develop consensus and unity across the whole of government,” he says. “In some cases, this may feel slow. But I think our nation works best when we take a whole-of-government, and a whole-of-nation, approach.”

*(Author’s note: This interview took place prior to the COVID-19 pandemic. Also, Glenn retired from NSA before its start. In my opinion, the need for coordinated action remains the same.)*

## 2. The NSA’s core mission

Though the nature of NSA’s work is covert, its mission and priorities aren’t classified information. Glenn lifts the tent flap, but with a disclaimer: “Please let your readers know that I’m speaking in my role as a private citizen, and not as an NSA spokesperson.” Disclaimer made, Glenn starts sharing.

> “The NSA is 67 years old,” he begins, “and it has always performed two functions. The first is to collect foreign intelligence — and I emphasize the word ‘foreign.’ The agency’s second function is to protect and secure the Department of Defense’s (DOD) communications network, including DOD’s weapon systems. This is, and always has been, a crucial function, for obvious reasons.”

He then shares how the NSA’s mission has evolved, over the last decade, into a cyber-centric one. Due to the ubiquity of the internet in our lives, a malicious cyberattack can affect more than just DOD; it can hit critical civilian-owned infrastructures such as the electric grid, telecommunication systems, and more. A cyberattack, notes Glenn, can paralyze every sector of the US economy. A big enough attack could even cost lives.

One tidbit I found surprising: “You may not know this, but technically, NSA isn’t responsible for protecting US businesses, or even the rest of the United States Government outside of DOD.” Glenn notes this general protective role falls to the US Department of Homeland Security (DHS), working in tandem with law enforcement agencies like the Federal Bureau of Investigations (FBI).

NSA does play a major role, but in a support capacity: to gather information about malicious adversaries’ intentions and capabilities. That information is then shared with US policymakers, who

use it to make informed decisions affecting the nation.

My next question is one that has been long percolating inside me. The NSA likely possesses one of the largest troves of "Zero Day" cyber vulnerabilities in the world. There is a strategic benefit to keeping that trove secret.

For example, the agency can use those vulnerabilities to break into an adversary's systems to gain key information, or for other offensive purposes. But it is equally possible for malicious actors to use those same exploits to hack into friendly US computing systems. I ask whether NSA should publicly reveal all Zero Day vulnerabilities it discovers. Such revelations, after all, could help companies shore up their defenses against attackers.

Glenn explains the balancing act used to determine when to make such information public. "There's a formal process in place," he says, "with a horrible name — the 'Vulnerabilities Equities Process'— which is run out of the White House. It is designed to weigh cybersecurity concerns and the need to protect our country from foreign adversaries."

In addition to these offensive strategies, Glenn shares that making certain information public could inadvertently reveal the sources and methods used to discover that vulnerability. Doing so could render those sources and methods useless — a potentially costly tradeoff.

That said, before Glenn left the NSA, he noticed a growing trend across the government to get more information to the public in a timely manner. "We recognize this type of information can help the public fight malicious cyberattacks," he notes, while sharing that NSA works with public-facing agencies such as DHS and the FBI to address those threats.

> On limited occasions, NSA may even work with private sector companies: "NSA shares more information with the public than you may realize."

In fact, the NSA publicly revealed a Windows 10 cyber vulnerability shortly before Glenn left office.

## 3. Surveillance specifics

Discussions of Zero Day responses soon morph to the specific role that is most associated with the agency: mass electronic surveillance. Glenn's answers to my questions are, unsurprisingly, both careful and methodical. I first ask Glenn about the NSA's surveillance role.

> "As you would expect and hope, the NSA has some terrific capabilities for learning the plans and intentions of our adversaries." But, he adds, "what may surprise you — as it did me — is the extraordinary culture of compliance that exists throughout the agency."

This "culture of compliance" is clearly a point of pride to Glenn, as it serves as something of a counterweight to strong opposition to the NSA's surveillance role by large swaths of US society.

People legitimately may disagree with the policy behind the program, but Glenn stresses that once guardrails regarding that role get set, NSA personnel scrupulously follow them. Those guardrails, Glenn notes, include legal input.

“Many of my private sector in-house colleagues complain about clients ignoring their advice,” he says. “But I am telling you that was simply not the case at the Agency. My NSA clients care deeply about following the law to the letter since, after all, we want to promote the rule of law and maintain public confidence.”

Glenn continues: “There are over 40 years of precedent involving the Foreign Intelligence Surveillance Act (FISA),” he shares as an example, “as well as internal procedures based on that precedent.” Per Glenn, there are also multiple layers of oversight from the FISA court, the NSA’s Office of Civil Liberties and Privacy, US Congress, and even NSA’s own in-house counsel staff.

> “Most people don’t realize this,” says Glenn, “but the NSA may be the most heavily regulated entity on earth — and that’s a good thing.”

*(Author’s note: In 2019, I took part in “Defend Forward,” a two-day national security wargame held at the United States Naval War College. We actively crafted our responses to comply with legal norms. I wrote about my experience attending the wargames in a two-part series.)*

*Photo: Glenn Gerstell receives commendation from Daniel Sutherland, chief counsel of DHS’ Cybersecurity & Infrastructure Agency. ©ACC Foundation*

## 4. The digital revolution

My time with Glenn ends on a subject of joint interest: predicting the future of US national security. We start with a *New York Times* op-ed that Glenn wrote in 2019 entitled, “I Work for the N.S.A. We Cannot Afford to Lose the Digital Revolution.” If you have not read it, I urge you to do so. In that article, Glenn expresses an almost existential fear that the United States is ill-positioned to meet the technology and cybersecurity threats of the 21st Century.

Changes in law and policy woefully fall short of changes in technology, Glenn observes. But when the stakes involve US national security, this disparity can be devastating. He elaborates:

> "Look at how we [the United States] have traditionally viewed and responded to foreign threats. Traditionally, in the physical world, we dealt with foreign threats by meeting them where they physically reside. For example, if we think North Korea poses a threat, it's typically because they are menacing assets or people in the Korean peninsula. Thus, we station military troops there. We issue sanctions, which effects are felt on North Korean soil, not ours."

But, he stresses, things are different in the cyber world. "Take the 'big four' threats — Russia, China, North Korea, and Iran, which use cyber weapons against us. The source of the threat may reside overseas, but the effect on the United States' interests is felt domestically. We have the Marriott hack, where credit card information was stolen by Chinese actors. Sony, whose stuff was thrown out the window by North Korea. Banks, universities, and even government agencies whose online systems were penetrated by Iran. Even the election mischief by Russia."

Taking on an almost professorial air, Glenn shares how our laws are designed to protect the US domestic spheres. But he fears that the effect of these laws is that overseas actors whose actions impact us domestically can game the system, simply because our system isn't designed to meet those threats. Glenn explains:

> "We need to rethink our entire approach to law, and to national security. That doesn't mean cutting back on the First or Fourth Amendments at all. It just means we need to be thoughtful and candid in addressing these problems."

*(Author's note: In 2018, the DOJ criminally indicted several Russian companies and individuals, accusing them of criminally interfering with the 2016 US presidential elections. One significant issue in the case was whether those defendants could compel the government to turn over highly sensitive data that might reveal information about ongoing investigations, and possibly the sources and methods used to compile evidence against the defendants.*

*This discovery battle became a significant issue in the case for two reasons. First, the DOJ became concerned those defendants could act as a conduit to funnel that information to the Russian government. Second, none of the defendants physically appeared on US soil, and thus faced minimal risk of judicial sanction should they misuse that information. On March 16, 2020, the DOJ dropped its prosecution of two defendants, partially due to these concerns.)*

## 5. The future of national security

Despite the alarming start of these questions, Glenn believes in the United States' ability to adapt to new challenges. In order to best convey that sense of optimism, I end this interview with a transcript of Glenn's responses to my final questions. The following has been lightly edited for length and clarity. But the words, and the sentiment behind them, are all his.

### Q. Let's move to something potentially more hopeful: the private sector's growing role in national security. Please share your thoughts about this

**relatively new phenomenon.**

Before answering that question, let me start with some background by comparing the world of today, to the world when I was a kid. When I was a kid, there was no single private sector company that could change a lot about America.

Past transformational technologies, like the radio, television, or cars, took decades before they became ubiquitous. And even then, those technologies didn't impact the nation to the same level as technology today. Maybe GM could produce more cars, but the impact isn't anywhere near what modern technology companies have on society today.

Look at social media. We have tech companies that collect vast amounts of personal data about us. Misuse of that data can result in grave consequences that simply don't match the risk posed by older technologies. Cambridge Analytica comes to mind. We are still far from figuring out the proper role of this technology in our society.

*(Author's note: I suggest watching the Netflix documentary, "*The Great Hack*," which chronicles Cambridge Analytica's impact on the world of social media.)*

Here's another example: intelligence gathering. Thirty or forty years ago, if someone in the [United States] needed information about activities happening in a foreign country, the only way to know what was going on was to send over a U2 spy plane.

Today, we have private sector companies with satellite imaging technology approaching that of the US National Geospatial Agency. If you're a commodities broker curious about Russian wheat crops, for example, you can literally order up pictures online. Malicious misuse of this data isn't hard to imagine.

All this is not a bad thing by any means…we have benefits today that would have been unimaginable thirty years ago. But these new technology advances mean that private sector companies today have the ability to project a type of "national power" that profoundly impacts our society and our national security.

## Q. It's a variation of "with great power comes great responsibility," and I say that in complete seriousness. Are there any "success stories" of the private and public sectors teaming up to protect national security?

There are success stories, particularly with some of the nation's critical infrastructure sectors. If you look at finance and energy, those two sectors stand out. In general, those sectors do a lot to make sure their members and customers are postured with the US government to protect against common cyber threats.

But that is just the start. In the years to come, the private sector will need to take on an even greater role in this arena, and they will need the active support of our nation's national security apparatus to be successful.

We need to find ways to share threat information between the public and private sectors more effectively, for example. This may be daunting for some. Both sides are still learning each other's capabilities, and to trust each other. But it is something that is vitally important if we, as a nation, are

to thrive in today's "digital revolution." But I think that is happening.

*(Author's note: Glenn is not alone in urging greater cooperation on national security matters between the public and private sectors. In 2019, the US Congress created a new think tank, the "US Cyberspace Solarium Commission," to develop legislative policy recommendations for protecting US national security.*

*On March 11, 2020, the Commission released the Solarium Report to Congress. Spanning over 80 recommendations, several of them focus on creating new laws intended to: (i) foster greater cooperation between the public and private sectors, and (ii) to bridge the trust gap between the two. Several key examples include recommendation nos. 3.3.2, 5.1.1, 5.1.2, and 5.2.)*

## Afterward and parting thoughts

At the start of this article, I described the NSA as an organization that is both respected and feared. Many of its programs generate controversy, and understandably so. But when the stakes involve the security of the nation, there are no easy answers.

Glenn's observation about the "culture of compliance" at NSA shows that guardrails can be put into place, and that lawyers play a role in securing them. His opinions on increasing national security collaboration between the public and private sectors are ones that I also share as a lawyer specializing in cyber national security.

Glenn retired from government service on January 31, 2020. Coincidentally, his final speaking engagement as the NSA's general counsel took place three days earlier at the ACC Foundation's annual Cybersecurity Summit. Along with senior leaders from the FBI, the Office of Director of National Intelligence, and the US Department of Homeland Security, Glenn spoke on many of the issues discussed in this interview.

I asked Glenn for his parting thoughts. After a pause, he told me that, as a 40-year private sector attorney, he never would have imagined having this unique opportunity to engage in public service.

Glenn stressed the honor of serving the United States, and hopes that his actions will inspire others to carry the torch forward. He is now a senior advisor at the Center for Strategic and International Studies, a board member, and a corporate consultant.

---



Robert Kang

Professorial Lecturer

George Washington University Law School

Robert Kang is a Professorial Lecturer at the George Washington University Law School, and a consultant. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation’s Cybersecurity Advisory Board.