THE BROOKINGS INSTITUTION

CONFRONTING NATIONAL SECURITY THREATS
IN THE TECHNOLOGY AGE

Washington, D.C.

Wednesday, March 11, 2015

PARTICIPANTS:

BENJAMIN WITTES
Senior Fellow, Governance Studies, The Brookings Institution
Co-Founder and Editor-in-Chief, Lawfare

GABRIELLA BLUM
Rita E. Hauser Professor of Human Rights and Humanitarian Law
Harvard Law School

WILLIAM A. GALSTON
Ezra K. Zilkha Chair and Senior Fellow, Governance Studies
The Brookings Institution

BEN WIZNER
Director, Speech, Privacy and Technology Project
American Civil Liberties Union

* * * * *

P R O C E E D I N G S

MR. WITTES: All right. We're going to get started.

My name is Benjamin Wittes. I'm a senior fellow in Governance Studies here at Brookings. I'd like to welcome you all, familiar faces and not familiar faces.

So we're going to do this without a moderator, so I'm going to sort of introduce it myself and then we're just going to get started.

The occasion is the publication of Gabby and my new book, *The Future of Violence*, and I'd like to start by saying that violence probably has a bright future. So if we had to summarize it in a word, it's pretty good.

What we're going to do is Gabby and I are each going to talk briefly about the book and about what we tried to do in it, and then we're going to get responses from Bill Galston and Ben Wizner, both of whom bring different perspectives on certain of the issues that we treat. Ben, as most of you know, is an ACLU lawyer and one of my absolutely favorite civil libertarian activists.

And Bill -- so one of the things that I did not expect when we started this project was how much it would end up being a work of political theory, which I am many things and Gabby is many things, but one of them that we're not is political theorists. And so we asked Bill, who actually is a political theorist, to kind of give some thoughts about some of the issues that are kind of at the tectonic level of the problem that we describe in the book and that we go into -- we'll go into in today's conversation.

So we're going to try to do all of that in about half the time and then open it up for as long a discussion period as we can. When that happens, please -- I'm going to say this now because I'm going to forget when it comes time -- just signal me and wait for the microphone before you start talking, and start by saying who you are and where you're from.

So, this project started a number of years ago when I was trying to teach myself a little bit about the cybersecurity debate, and was simultaneously asked to write a paper that involved biosecurity, which was a subject about which I knew very little. And what I found as I was simultaneously trying to self-educate about cyber and was working on biosecurity in the context of this project was that the debate was actually the same debate. It involved proliferation of the capacity to launch devastating attacks to ever-greater numbers of people. Less and less need for state involvement to do things that were really bad. Both communities talked as though the other one didn't exist about what they call the "attribution problem," which is that when something bad happens, you don't really know who's responsible for it. It's not like when an army moves, although the Russians deny even that. And that these problems had a way of transcending borders. And both of these communities were sort of talking about this as though this were a kind of unique feature of the environment they were dealing with, and so I started thinking maybe it is a larger feature of technologies that radically empower individuals and that we've needlessly and wrongly siloed these discussions.

The book begins with three hypothetical situations, all of which involve the change of exactly one fact from a real situation. One of them is the Deep Water Horizon explosion. So change one fact about the BP oil disaster and make it that somebody blew it up on purpose. Now, when, in fact, the Deep Water Horizon exploded, that was the working hypothesis of much of the federal government for a not-trivial period of time. So to give you an idea of how realistic it was, this was actually believed by a lot of people in real-time to be what had happened.

Now, a couple of things if we did that, if you run that hypothetical in your mind will jump to mind. The first is that it would have been the most significant attack on the United States since 9/11. Same oil flow volume; right?

The second issue that you would notice is that the response to it was entirely a response by a private party; that is, the group responsible for protecting the shores of the United States from rampaging oil was not the U.S. Coast Guard, was not the U.S. Navy, was no military component. It was British Petroleum, you know, an internationally traded private corporation.

Second hypothetical. Change one fact about the anthrax attacks in 2011. When the anthrax attacks actually happened, the person who did them labeled the envelopes that he used. You know, "Now we have anthrax." They were very clearly labeled. "Get on penicillin now." If you're trying to kill as many people as you can, putting anthrax in a sealed envelope is not an efficient way to do it.

So let's imagine that he had actually not been trying to draw attention to himself but had been trying to increase the lethality to the maximum extent possible of his attacks. So here's something that he could have done that we hypothesized. Take one of these drones, which when we started writing this book were quite exotic. Now they're really commonplace. They're not exotic at all. And you don't need very much of the stuff if you sprinkle it from a high altitude over a stadium.

So the other day at the Super Bowl, they actually imposed a regional "no drone zone" over the whole area. So this is not that far from the realistic imagination of people responsible for the security of the Super Bowl. Then, by the time you have a single person sick, you have a very large number of people infected. It's a very different ballgame.

So I asked a molecular biologist friend of mine, "How realistic is this scenario? Could you do it with just off-the-shelf drone technology?" And he laughed at me. He said, "Why would you want to? That's a wild overinvestment in technology." And I said, "What do you mean?" He said, "Because you get exactly the same effect from driving through a major city with a truck going like this. He goes, "You don't need the drone." So that's example number two.

Here's example number three. This is a real case. A guy named Luis Mijangos. Luis Mijangos was a very talented hacker in Southern California, who engaged in a set of malware attacks on women and young girls in the Southern California area. The FBI has estimated that there are probably upwards of 200 victims, about half of them underage. And what he would do is he would send the malware that would take over the webcams on their phones, use those to take serendipitous nude pictures of them, and then extort -- using those pictures, extort the production of sex tapes for his own use. He actually made contact with apparently a very large number of people. He is now serving a number of years in prison. He was caught.

However, imagine for a minute that he were not in Southern California where his victims were but in one of those parts of the world where all those spam messages come to you from scammers and other things. Then you get into all sorts of jurisdictional questions that run to the reach of even, you know, the tyrannical federal governments' enforcement powers.

If you put all these three examples together, you develop a vision of what Gabby and I have called "the world of many to many threats and defenses." And it's really the subject of the book, which is the question, "How do you govern a world in which anyone can attack anyone from anywhere?" And I don't assert, and we don't assert that we're yet quite living in that world.

But the claim of the book is that we're heading at some rather rapid pace toward a world in which: (a) the power to attack is universal; (b) the distance over which you can conduct those attacks is not limited geographically; and (c) thus, the power of the state or any state, any one state to protect the safety of its people is to some degree or another impaired. In the world of many to many threats, the basic question of the book is how do you govern a world like that?

Now, when we started working on it, I thought that what we were going to come out with was a laundry list of policy prescriptions because, you know, this is Brookings and we do laundry lists of policy prescriptions. And I thought, like, okay, we're going to end with sort of a five-part plan. And the more I worked on it, and particularly as Gabby started raising questions that I really had not focused on -- Gabby, who I will turn this over to momentarily, is an international law scholar and knows things about jurisdiction that I just had never really given much thought to -- where it comes from, where the idea of state jurisdiction comes from. And the more questions we started throwing at each other, the less able to answer at the policy level a lot of questions we became. And so the book became more a book about the political theory and the theories of law that might get you to a place where you could actually govern a world of many to many threats and defenses.

So I want to tick off several areas where this world, if you believe that it is developing, challenge some of the basic premises that we work with normally. And then I'm going to talk briefly about one of them and turn it over to Gabby to talk about the other two.

So the first one is the basic relationship between liberty, security, and privacy. This is a relationship that we constantly invoke. When, you know, people don't like what the NSA is doing, they talk about it. When people insist that we need to have more, right, FBI Director Comey was here and talked about that relationship. It's a sort of organic piece of our rhetoric about this.

Now, we argue in the book that the rhetoric is largely wrong and misplaced to begin with. But more to the point, it's really wrong if you believe that you're heading toward a world of many to many threats and defenses. And the reason is -- there's a lot of reasons, but number one, the reason -- the first reason is that the basic promise of the state, the pre, you know, almost pre-civil liberties, is a promise of protection and a promise of safety. And what if the state is not actually capable of keeping that promise anymore; how do you think about what you're willing to do in that situation?

The second issue is that to the extent the state is able to offer that protection, it is often doing it and increasingly doing it through relationships with private actors that involve those private actors kind of pervasively in the provision of that safety. So you see this a lot in the surveillance arena. But I would argue that you also see it in BP's response to that oil spill. The response of the U.S. Government was not to do this itself, not to protect the shores of the United States itself. It was to sort of sit there and hold up, you know, like ice skating judges, you know, 5.6, 5.8, grading BP's response and BP's performance. The kinetic activity was done by BP.

Finally, and I'll stop here, the presumption that there is a balance between liberty and security that we are always tinkering with, and when you put weight on one side, the other side goes up; that there's this real zero-sum balance between the two. It's a very pernicious idea, but it's really pernicious in this area. So if you take this idea at face value, the freest country in the world should be Somalia; right? Because it's the least governed. It's the least secure. And similarly, the safest place in the world should be North Korea. And if that sounds a little bit wrong, or maybe a lot wrong, the reason is that the balance metaphor is flawed and that there is something else actually going on.

Now, this is probably important to our rhetoric in general, but I think it's really important when you're talking about adjusting the foundations of the relationship.

And when we talk about Internet safety, Internet privacy, we're actually talking about the foundations of the relationship. When you talk about a right to tinker with biological materials, you know, are you allowed -- do you have the right to manufacture DNA sequences? That's a foundational question about the scope of human liberty and human rights. You need to think about whether restrictions like that -- what they are going to do to that relationship. And it's worth having a set of metaphors that actually better describe than the ones we currently use.

So the other two areas which I'm going to turn over to Gabby to talk about are the basic liberal theory of the state, which as I say is really predicated on the idea that there is some leviathan that can protect you; right? And the second is how this all works internationally.

So I'm going to stop there and turn it over to my illustrious co-author, Gabby Blum.

MS. BLUM: Thank you.

One thing to say at the beginning remarks is that both Ben and I acknowledge that technology by and large is a wonderful thing. So this is not an anti-technology book. Technology, on the whole, does many more good things than it does bad things, and we don't want to lose sight of that observation.

It is also the case that technology empowers everyone. It empowers not only individuals; it also empowers the state. So as we talk about the threats that are sort of distributing and diffusing across borders and to smaller and smaller entities, we should also keep in mind that maybe the biggest winner of the technology revolution is still states and it's still going to be states. The question is in this arms race, who is going to benefit more on the whole? Or who is going to be threatened more on the whole? And that is still, I think, an open question.

So imagine one of the things that happened in this world of many to many threats or defenses, where ultimately if you take it to the extreme it means that every individual, group, or company or state is a potential threat at least to every other individual, group, company, or state around the world. What does security mean? And one of the things that technology creates or blurs is the line between personal safety and national security. This distinction or that distinction that we sort of operate under the world of law enforcement, of crime, of our sort of personal or even social safety and the lines that deal with the high politics of national security, the safety of the state really become very blurred, and each and every one of us as a user of technology, as a vehicle for technology, becomes a potential transmitter of threats also. We become a potential threat. We become a potential transmitter of threats.

So went the state has been suggested in its original -- the way the nation state was conceived, was around the social contract where we as citizens relinquish power. We give it to the state. The state now has monopoly over force, and their side, the state side of the bargain, is that it protects us. It protects us from one another and it protects us from faraway enemies.

Now, imagine that before a technological revolution, when you talked about outside at least, from external threats, you basically had to protect yourself against every other country or every other leviathan. So in our present, think of it just as a rough number, about 193 UN members. This is what your security environment, very grossly speaking, looks like.

Now with a technological revolution, and of course, it's not a 01, it's a trend that has been going on for decades, the threat environment is no longer 192 other countries. It's 192 other countries, hundreds of thousands of companies and organizations, and seven billion people. Again, this is a very extreme view, but taken to the extreme, this is what the security environment looks like. So then it becomes a question, what is now the bargain -- the internal bargain and the external bargain of how to think about policing, how to think about the right sort of blending of liberties, protection of privacy, other values, and still the yielding of security.

So Ben mentioned earlier the counterfactual about Luis Mijangos. Imagine he was situated elsewhere. So we do actually talk about one particular scenario in which this was the case. In December 2011, a 19-year-old, or somebody who turned out to be a 19-year-old hacker by the name of OxOmar -- this was his pen name, OxOmar -- hacked tens of thousands of Israeli credit card holders' information and posted them online. He was a part of a hackers group self-identified as Group XP, and they were very explicitly anti-Israeli, anti -- challenging the right of Israel to exist, calling for the destruction of the state of Israel, and on top of posting the information of credit card holders, they also hacked the airline's website and the Israeli Stock Exchange.

Now, to this day, nobody is 100 percent sure of who is OxOmar or where he was from, but conventional wisdom is as follows. OxOmar was a 19-year-old Saudi national who was, or it was presumed, operating from a café in Mexico. So basically, an Internet café in Mexico, and causing all this damage to Israeli citizens and Israeli interests. Who has jurisdiction to deal with OxOmar? Is it Israel as the country that has been most harmed by it? Is it Saudi Arabia, as the country where OxOmar is presumably a citizen of? Or is it Mexico, the country from which the actions, again, presumably, were conducted.

And the truth of the matter is that international law doesn't give us a concrete answer to this question. In some ways it says all three to varying degrees. That also means that in some ways it's none of the above. And this is all because international law, for all our progress and conversation and discourse about individual human rights and the individuals becoming the center of international law and international tension, we still very much live in a Westphalian era. A Westphalian era in which states are the important unit and in which states are protected by the sanctity of their borders, of their sovereignty, and of their near-absolute jurisdiction over what happens within their border and very little jurisdiction over what happens outside their borders.

This is a good system or a good idea if you really believe two things -- that the state is the enduring unit that is capable of yielding the most or wielding the most power, and also, that the state is capable of policing its own jurisdiction and its own territory.

But we're now in a world where the future of the nation state is really at peril, so the U.S. fund for peace and other think tanks here in Washington, D.C., lists dozens of countries around the world as on high alert or as very fragile where their continued existence as a state is really threatened. I happen to think that this is maybe the greatest security challenge of our time, is exactly the future of the state as an entity that is capable to govern its own territory. And this raises important questions about the relevance of borders today, the relevance of this allocation of powers between and among states, and what states can do both internally and externally to protect themselves and the citizens that reside within them.

It also means that it's not only what states can demand from foreigners or from foreign countries, but also what it owes them becomes a serious question. Can the United States continue to say the rights or privacy of German citizens or Argentinian citizens is none of my concern; I only have obligations towards American citizens? That can now, I don't think, can continue to hold as a working assumption and as a framework for regulation.

So that leads me to the question of what does the international system look like going forward? So far, we've allowed states to pick and choose their obligations. We've allowed states to pick and choose how much they want to work alone and how much they want to work in cooperation with other countries. What we currently see, and I think both trends are going to increase in the longer term, is kind of the extreme vision of both unilateralism and multilateralism.

So we countries, the most powerful countries, extending their laws beyond their borders. Think about the United States and the Material Support Witness Act or Material Support for Terrorism legislation that basically exceeds its reach beyond any border around the world. We see surveillance, even aggressive surveillance of citizens in the countries around the world. We see the occasional, basically hijacking you can call it, all kinds of things, but kidnapping or hijacking of individuals, or bringing them "to justice" in the domestic forum, all the way to the most extreme use of unilateralism, which is targeted killings or bombing on a larger scale. Our prediction is that in a world of many to many threats, we're going to see much more of that. We're going to see much more of that not just in the hands of the United States but of an increasing number of powerful actors around the world.

To make sure that we don't live in the Wild West and that we are more effective in what we do, these unilateral efforts are going to have to be complemented by much more cooperation and multilateralism. It means cooperating in intelligence sharing. It means cooperating in strategy. It means cooperating in actual policing and allowing foreign forces jurisdiction in your own territory to be effective in policing activities, and it means caring much more about the capacity of other countries around the world to be effective and functioning countries. It's not just about benevolence. It's not just because it's the humanitarian thing to do to care whether Somali is a functioning country, yes or no. It now becomes really a matter of strategic self-interest to make sure that more countries around the world have the capacity and have the institutional resources and structures and know-how to effectively police their own territories and make them safe, both for their own inhabitants and the inhabitants of the world at large.

So with that I'll turn to Bill and Ben to add their comments.

MR. GALSTON: I guess I'm next, at least I'm seated next.

SPEAKER: I guess we're going left to right.

SPEAKER: Not quite.

MR. GALSTON: I am eager to get to the conversation and to the question and answer. So I'm going to confine myself to two points. In the first of which, I'll fulfill my assigned duty as a political theorist, and in the second, I'll segue to some skeptical remarks about the impact of technology on the questions that we're talking about.

So, the two theoretical benchmarks for this book it seems to me, the baselines, are Thomas Hobbes and Max Weber. And the authors of this book invoke both of those great theorists in ways that I think are germane and in the main accurate, but not absolutely unimpugnable.

So a word about Thomas Hobbes. Hobbes is famous for arguing that the security dimension of the social contract is absolutely fundamental in the sense that if that is missing, none of the other goods of civil life that the social contract seeks to secure are achievable. And Hobbes, of course, has his famous sentence to summarize that line of thought, and in my judgment, both a theoretical judgment and a political judgment, that proposition is absolutely correct. Minus security, everything else is called into question. And it follows, therefore, that the ability of the state as it has been understood for the past four centuries to fulfill that essential human as well as political function is a fundamental practical question. And if Ben and Gabby are right that these technological changes have in some way diminished the capacity of the state to fulfill that function, or diminish the capacity of the state as currently configured with its current policies, then that is a very serious question that we need to grapple with.

Now, let me turn and you'll see why in just a minute to the second theoretical hero, namely Max Weber. And Ben and Gabby quote Weber's famous definition of the modern state as "that human community which successfully lays claim to the famous phrase 'monopoly of legitimate physical violence within a certain territory,' this territory being another of the defining characteristics of the state."

And the point that I want to make is that Weber's definition of the state is, to use another one of his terms, is "an ideal type that can never be realized." The state can never claim a monopoly of legitimate use of violence for a very simple reason, which goes back to Hobbes. The state can never guarantee the absolute security of citizens in the first instance, vis-à-vis one another. And citizens, Hobbes insisted, and I think Weber would agree, retain an inherent right of self-defense, an inherent right to use physical force to defend themselves in circumstances in which the state cannot or will not do so. And that inherent moral right of the individual is just as fundamental to our understanding of not only the modern state, but I would add the modern state system as is the idea of the social contract or international law. Self-defense is not just a small preservation in the framework. It is one of the fundamental moral building blocks of human order, both domestic and international. I'm no great expert on international law, but it seems to me, based on what I do understand, that the inherent right of national self-defense is recognized just as much as the inherent right of personal self-defense.

So when we talk about challenges to the international order, you know, what states may be called upon to do in the name of self-defense, this is not a new situation. This is an extension of a situation that is as old as the social contract and as old as the state system.

One question is what happens -- and this question has been on the table in the United States for a couple of decades now -- what happens within when developments in another sovereign state call into question the sovereign right of self-defense of another state? What happens if there are failed states? What happens if there are states that are knowingly in league with transnational terror groups but decide for various reasons that they're not going to do anything about that? We can argue about how far the rights of the self-defense of the potentially or actually attacked state go, but from the standpoint of the basic structure of the state system, it is impossible to deny in principle that the sovereignty of State A is limited by the inherent right of State B to defend itself.

So that's, you know, that's my first point. And it's inherently difficult because states, as now configured, are in the business of generating what the economists call the negative externalities that affect the well-being of other states. Chinese factories affect the quality of air here in the United States and not just in Beijing. I don't know of anybody who claims that the United States has the right to bomb Chinese factories in order to reduce climate change or air pollution in the United States, but to quote Gabby, it's not a zero-sum question; it's a continuum. And at some point, the threat from activities that are conducted by or tolerated by another sovereign state will reach a threshold point at which some response that is seen as limiting or invading the sovereignty state that is harboring or encouraging those practices will be warranted, and we're going to argue for a very long time about where that line is. That's point number one.

Here's point number two, and this perhaps goes a little bit, you know, cuts a little bit closer to the thrust of the book. The book is called *The Future of Violence*. It might with almost equal justice have been called *The Future of the State*. And the book has a kind of a split personality on that question. You know, if you look at the introduction to the book, it's almost like 1984 but in reverse. "With today's new technologies, the power of states in relation to their citizens is reduced." Page 9 for those of you who are interested in the citation. That sounds bad. Bad news for the state. Citizens up, state authority down. Oh, whoa, what are we going to do?

Okay. Then fast-forward 250 pages and you get to the conclusion, and you find that the authors are validly not willing to give up on the state as the major instrument for governing a world of new and heightened risks, and I quote, "The leviathan is still the best friend we've got."

So somewhere in those 250 pages, this unprecedented, technologically-driven threat to the power of the state, has evolved into a not-so-grudging embrace of the state as the continuing best mechanism for dealing with these threats, which means that there is a lot of work going on in the intervening 250 pages.

Now, why my skepticism? Well, you know, Gabby has, in her remarks, has already anticipated what I'm about to say. I think it is easy to exaggerate the long-term consequences of technological change for state-governing capacity, and the reason it's easy to exaggerate is that technological change is typically a two-edged sword. It may strengthen the purveyors of instability, and at the same time strengthen the defenders of order, or maybe not at the same time but sequentially. Insurgents may have a first-move advantage but functioning states will, and typically do, catch up. So it's sort of like an arms race where whatever the level of power was between the two at time T0 is restored at time T2, and at time T1 there may have been some intermediate changes.

So it's been four years since the famous Facebook Revolution in Tahir

Square, but one notes that the old order is back, more entrenched than ever. They figured out what to do. Clearly, the Chinese were perplexed by the IT communications revolution for a while. They seem much less perplexed now than they did 10 years ago. As a matter of fact, that the state controlled this potentially disruptive mechanism strikes me as quite effective. But, you know, what I think doesn't matter. Talk to your average Chinese dissident about how effective this sort of counterauthority mechanism is, and they will all tell you, well, we were doing pretty well 10 years ago, or even five years ago, but we've pretty much lost control of it now.

So you put this together and I think you're led to the following conclusion: We have a lot of issues to think about that we didn't have to think about in a prior technological era, and those issues affect the relationship between citizen and state, and between state and other states in fundamental ways. But the same could have been said, and was said 100 years ago, and here we are still with a recognizable descendent of the Westphalian system, and I will make bold to predict that in 100 years we will have another representative descendant of the Westphalian system.

Over to you, Ben.

MR. WIZNER: Maybe I should try to pick up where you left off. But first, let me just say thank you to Ben and Gabby for including me in this event. I won't be surprised if you leave your current jobs for more lucrative careers as screenwriters because some of the scenarios that you spin in this book are remarkable. You quote a James Bond movie here, perhaps the next James Bond movie, "We'll Take your Drone Spider" and spin a scenario from it.

I really like this book. This is not, don't worry, the proverbial "kiss on the mouth" from the Mafia, although I always tell my colleagues, "If a judge praises your oral argument, get ready; it means you're about to lose." But then again, my colleagues usually are about to lose, so it's a safe prediction.

I want to make just a few observations as well and then we'll get into this conversation. This book covers a huge amount of conceptual and practical ground, and I just want to point to a few things that I think are missing from this conversation case you are considering a sequel. Although I compared you to screenwriters, I actually don't think these scenarios that you spin are so far-fetched. I think the capacity for violence in today's world is enormous, and in fact, you don't really need to be thinking about the future to be worrying about these things, and one question I have as I read this book is, what is your account of why the world is not much more violent now in the ways that you worry it will be in five years or 10 years or 15 years from now? We probably, as your friend said, we don't need drones to deliver these agents. Educated Japanese cultists used sarin gas in a Tokyo subway and killed a dozen people, but Chinese leader separatists used knives in a train station in the west and killed three times as many people. You point out in your book that the weapon of choice in Rwanda was the machete and not any chemical weapon. The original bioterrorism was probably a smallpox blanket that didn't require a fancy laboratory.

And so the question is, what is your account of why there is not more catastrophic violence carried out by individuals? A lot of talk has gone into this in the realm of terrorism and counterterrorism, and you know, I'm persuaded by theorists who look for reason and politics behind terrorism. Generally, there's an outcome. It's not random nihilistic. It's not about causing the most harm and mayhem possible. The same might not be true of certain kinds of religious cultists, but we're going to have to look at motivation. As capability expands, we're going to have to ask the question, why does it happen? Why doesn't it happen? And I think that's a critically important conversation.

Ben mentioned the conceptual discussion in this book about what a lot of us consider to be a superficial discourse of balancing security and liberty, and I think the book makes very important contributions to that discussion. I think though that some conflicts are real. Isaiah Berlin famously said that "Freedom for the wolves has often meant death for the sheep." And it's not the case that we can always say that social goods will be in alignment and that we can redefine them in a way that they are. Now, I agree that the conflict between security on the one hand and privacy on the other, the way that it's been posited in much of the discourse, is wrong. On the other hand, there is an awareness in the technology community and a growing awareness in the policy community that there may be a conflict, not between security and privacy but between security and surveillance. Then, two people who are blogging for your site now, Lawfare, Susan Landau and Bruce Schneider, have both made this point in books. Susan Landau wrote a book called *Surveillance or Security*. And that's because -- and we've learned more about this in the last year and a half from the Snowden revelations -- many of the things that governments do in order to facilitate surveillance involve weakening communications infrastructures. Exploiting and creating vulnerabilities in those systems. And so sometimes the surveillance is not done for the purpose of protecting the platform, but actually undermines the platform for the purpose of getting and extracting information.

So that is a conflict that exists. And I think particularly since you talk about the cyber threat in your book, it's one that I think that you're going to need to grapple with. It's one that the president's NSA review panel did grapple with. I mean, Richard Clarke, who is widely considered one of the cybersecurity experts in this town, testified to Congress that this conflict exists, that it's more important that we be able to protect our systems from China than that we be able to break into theirs, that if the cost of breaking into theirs is weakening ours, that's a cost that we shouldn't pay, and that's because our stuff is worth more. And that's also something to think about. It may be that the countries that have the most to protect should be most invested in rules, not take advantage of their relative power in order to essentially make the rules by their conduct.

My view is that the greatest threat doesn't come from outdated conceptual frameworks but rather from the real failure of our national security politics to grapple with and embrace resiliency. You do discuss resiliency in this book in a few pages but you're talking about the architecture of resiliency. How we can essentially harden our system so that when there is an earthquake, fewer buildings will come down. First responders will be ready. But the politics of resiliency would be a public recognition that some threats simply can't be eradicated but are not existential. And being able to contextualize these threats and to respond with reason as this book does rather than with passion and illogic as our politics do. And I think this has been particularly missing from our politics since 9/11, and there's been a sort of anti-resilience that has taken hold where essentially, the more afraid you are as political leader, the more strong you are seen as a political leader. And so therefore, the people who say -- who said after 9/11 that this is a new kind of threat that we've never faced before, that our legal institutions are not capable of dealing with it, that we need to do things like create prisons outside the law, black sites, use all these other tactics, those people are celebrated as hard-nosed warriors, whereas the people who said, actually, our institutions are fairly strong, you know, this was an awful attack but we don't actually need to dispense with all of that terrorism, will always be with us in some way, but we have frameworks that can deal with it, are often accused of having a naïve pre-9/11 mindset. And think about whether any national politician over the last decade has stood up and said, "Terrorism is not an existential threat."

And I think that that is a serious failure, and it's an important failure, because if we're going to talk about the kinds of threats that you worry about here -- you know, we had a vice president who had a doctrine, the One Percent Doctrine. You know, if the threat is severe enough, even if it's really remote, we have to act. Well, sometimes acting is worse than not acting if acting means invading Iraq in 2003. And so to the extent that this is a call to action because we're worried about violence, it matters what that action is. And what that action is will depend on what the political conversation is. And I worry that the political conversation is antithetical in tone to this book which is so measured, so reasonable in dealing with these issues.

You know, I think the country is ready for that conversation, the resiliency conversation, and I think that we've proven that we are resilient in other contexts. You know, again, you discussed the automobile, but I want to bring it up for a different reason. For as long as we have recorded this, automobiles have caused anywhere between 30 and 50,000 deaths a year. For much of that time it would have been hard to reduce those numbers, but it's not hard anymore. We now have the technological capability to bring that number much, much closer to zero, if we wanted to. We can automate traffic enforcement. We have the capability of measuring the speed limit of every car on the road and issuing tickets. We could add breathalyzers to the ignition mechanism of every car right now so that you couldn't start your car if you were drunk. We could have checkpoints in a lot more places. We could -- there is no technological barrier to our bringing that number from 30,000 to 2,000 if we decided that it was worth the cost. Now, we decided it's not worth the cost. That's probably the right decision. In my view, its worth, you know, the curtailments of freedom that would be involved in bringing that number radically down are a price that most of us would not be willing to pay.

We don't see that kind of conversation when we're talking about terrorism, counterterrorism, and national security. Instead, we see an attack in Paris that takes 12 lives, or one in Boston that takes three or four, and immediately the conversation is, what went wrong, and what do we have to change right now to make sure that this will never happen again? Well, maybe nothing went wrong, and maybe we don't have to change anything, because maybe three people being killed here and 12 people being killed there is not just a cost of a free society, but impossible to prevent even in a not-free society if we're going to have weapons like automatic weapons and be able to make bombs.

And so I think we need to be worried about overreaction, and I think the conclusion of this book very masterfully addresses that issue; that we do have as much to fear from overreaction as we do from nonreaction. And to sum up, I would say, you know, unfortunately, we will not get to decide how we die. We do have a fair amount to say about how we live. And with that, congratulations on this book.

MR. WITTES: Well, thank you.

So we all spoke a little bit longer than I expected, and therefore, I don't want to leave you guys out in the cold. So if it's okay with Gabby, I think I'd like to have us respond to the things that were said in the context of your all's questions and go directly to questions now. Is that okay with everybody?

MR. WIZNER: Yep.

MR. WITTES: Great.

Signal me if you want to get in on the conversation, and I will -- yes, sir.

MR. NELSON: I'm Mike Nelson with CloudFlare, which is a web security firm. I also teach Internet studies --

MR. WITTES: That's our -- protects Lawfare. We love CloudFlare.

MR. NELSON: Great. And the question has to do with the impression I get from the U.S. Government that they feel that they sort of need to protect the world's global information infrastructure by protecting systems and also by collecting information on what's going on out in the Internet. In some cases there's talk of requiring information infrastructure companies to monitor what their customers are doing. We're hearing about hearings on the Hill where Twitter and Facebook are being accused of supporting jihadist terrorists. There's sort of an asymmetry here because we have the U.S. Government saying, "We're going to take action and we're going to act extra-jurisdictionally," and yet we have American companies who are trying to serve customers all around the world who don't necessarily think they fall under U.S. law. And so I'm trying to see if you have any thoughts on how the U.S. Government can provide leadership without somehow providing a global approach to protecting the global information infrastructure.

MR. WITTES: Great question.

I have a number of thoughts about it, and I'm sure others here do as well. So, look, at one level you've really asked at least three distinct questions, and I want to break them down because I think they may have totally different answers.

So one is the U.S. Government wants to protect security of information systems, and so the way it does that is by compelling private entities to do things. So this is actually a bit of a change from the way the government traditionally operates in the security space, which is, say, to do things itself. Right? And this is a very profound change that has been going on for many years but the Internet has radically accelerated, which is that the regulation tends to be not direct regulations of individuals, or in addition to direct regulation of individuals, regulations of the intermediaries through which we do business. And that is a very profound change, and I think it goes directly to the change in the social contract that we describe in the book, which is that the social contract which we have traditionally thought of as a contract between the polity and the state, right, now involves these companies, some of which are not domestic corporations, right, which are party to the security relationship that the state promises. And that's a very profound change that we have not fully thought through the implications of.

The second question is, and this is one that Ben and I disagree about a great deal, but given that relationship, how much should the government be tinkering in the business of people through the companies. Right? How easy access to how much information should they have?

The third question is, what do you do about the fact that there isn't "the government," there's 193 governments, each of which has some jurisdictional claim on the same set of behaviors? And so when you reach that, then you get into all of these jurisdictional issues that Gabby was talking about, as well as this basic muscle question, which is do the most powerful actors, in fact, set the rules because they are the most powerful actors.

And so I think your question is really important. It's a foundational question at the heart of the book, and you know, we try to talk about it both in the cybersecurity arena, but also in the abstract. What do you do when you're dealing with a series of technologies that are inherently networked, that are inherently transnational, that are inherently dual-use, that the interest in privacy is going to be very real and the interest in regulating the way people use is also going to be very real. And look, you know, it's not an accident that the person who's asking this question comes from CloudFlare; right?

And so let me tell you a story about CloudFlare, which is a true story, and it's about how I got involved with CloudFlare, which as a consumer, about a year ago, the website that I run, Lawfare, was subject to a series of denial of service attacks. We never tried to figure out who was doing them. We're not a significant enough actor, and the attacks were not substantial enough to trigger any law enforcement interest. So what do you do? Who do you go to for protection when the leviathan won't protect you?

And the answer is, you hire a bodyguard. And that's what CloudFlare is. And, you know, we went -- just for the record, we've never met and I was not asked to flat CloudFlare is a great example of a class of products that develop when the state isn't actually fully performing its security function. So there's your free advertising.

MS. BLUM: Maybe one more word on it. There may be two interests that the government has here. One is to say, "I'm going to regulate the entire globe because I can, and I'm the most powerful, and therefore, I can set the standard for everyone." And the second interest, which is not incompatible with the first, but it's to protect American interests, because if I do something only domestically or that covers only American companies, I put them at a disadvantage compared to others.

So take an example of the Foreign Core Practices Act. So before the United States legislates the FCPA in its current form, companies in France, for instance, not only are not prohibited from paying bribes and kickbacks to get concessions all around the world; they are actually allowed to deduct bribes from their tax payments. Okay? And so then the United States says to American companies, "You guys can't pay bribes." And they say, "But the French guy not only can pay but can actually make it part of its balance sheet, and that puts American companies at a disadvantage." So now the reason we want to sort of on a global level is not so much because you want no one in the world to pay bribes. That would be an ideal thing but you also want to protect the American companies against disadvantage by competitors.

So you legislate this law that basically says all you need, the kind of connection to the United States that you need is to happen to clear a check through an American bank or make a phone call that just happens to be rerouted through the United States and that's it; you're on the hook. And I think that's the kind of stuff you're going to see more of.

MR. GALSTON: I wonder if I could just add a word on what I see as a very significant civic downside of the move to privatize security functions. And that is in a number of Latin-American companies, the wealthy and the powerful resort almost entirely to private security -- firms, bodyguards, private militias, in effect, that they hire -- and a direct consequence of that is that they care less and less about the general security function that's provided to citizens who don't have the wealth and power in Cloud. And so I think that we should think very, very hard about the devolution of functions to intermediaries that will have the effect of rendering this essential zone of civic society, namely order and security for all, much less viable.

MS. BLUM: That's exactly right, and it's sort of connected to a point you raised in your remark about this question of self-defense and sovereignty and how do you respond to threats from other places? And one of the things we note is that the rise of vigilantism in that sphere. So imagine that it's not clear how or whether and in what way Israel can respond to OxOmar -- Israel, the state. It turns out there is a big Israeli hacker community that decides to take action against Saudi nationals. It had nothing to do with OxOmar but sort of in the face of kind of paralysis at the national level, the government can't protect you from the hacking and also isn't going to take action even though some bloggers later -- it turns out that OxOmar died of an asthma attack and the blogosphere was all, yeah, right, asthma. The Mossad over again.

But I have no reason to suspect that the Mossad had an interest to deal with OxOmar or had the capacity to induce an asthma attack if they could find him. But what was interesting was sort of the kind of people to people's response, which you get when the government isn't either capable or interested and that's part of the concern about the devolution of power, is the sort of rise of vigilantist response across borders.

MR. WIZNER: One other point. There's a lot of discussion in this book about increasing cooperation between the government and the private sector, and one very interesting by product of the Snowden revelation has been the increasing adversity between the government and some of the world's most profitable corporations. We saw the director of the FBI to the Press Club to criticize Apple. We saw the British prime minister criticize technology companies for using too much of that encryption. And you can understand the frustration of governments. One of the responses of these technology companies after reading about ways in which the GCHQ and the NSA had exploited and created vulnerabilities in these systems was to make them more secure. Technologists believe -- almost all technologists believe that there is no golden key that could allow proper law enforcement surveillance without also inviting another parade of horribles -- hackers, foreign governments and the like -- and so you have this very real conflict. These are both social goods. If you believe in any kind of government surveillance, as most of us do, you worry about the situations where the government has a lawful warrant to get information and yet is unable to do so because of product design. On the other hand, if the cost of enabling that access is to undermine the security across the board, then you have to decide what's more valuable.

So there was another very interesting exchange between the chief technology officer at Yahoo and the new NSA director -- the NSA director saying, "We can find a way to build backdoors on these products to allow lawful access." Yahoo wanted to know, "If I create this technological capability, what do I do when China comes to me with a warrant, because I operate in that country, and I have to be subjected to the laws in whatever country I'm in."

So you get back to Richard Clarke's point, what is more important here? And I think there are valid arguments on both sides. And I think you could say, "We're willing to pay this price in security, in communications security, in order to ensure that law enforcement has access. That's not where many people come down on this question. Bruce Schneider's new book certainly comes down on the other side.

MR. WITTES: So just to dramatize Ben's point a little farther, because he mentioned what the Yahoo representative did the other day. Shortly after the Snowden revelations -- I'll just give you an idea how far Yahoo has moved on this -- I was on a panel with a different Yahoo representative who was presented by, I believe, Bruce Schneider, with the question, "If you could engineer tomorrow the ability to not be able to access your own systems so that you couldn't turn it over to law enforcement, would you do that?" And she responded with horror, "Of course not, because there's all sorts of abusive stuff that goes on on our systems and we don't want to be hosts to that."

And so I think this, you know, whether you think the movement is toward the direction of the side of the angels or the side of the devils, the movement has been very, very substantial on the part of the technology companies.

People are quiet.

MR. GALSTON: There's a hand behind the camera right over there.

MR. WITTES: I am blind to it.

MS. HARRISON: I don't know if I can articulate this properly. I am Ava Harrison. I'm a retired professor.

But I hear the need for security, and I hear your concerns about it. I don't hear anything about the fact that the governments are more and more -- or less and less interested in civil society and protecting the rights of citizens and their common interests and more and more despite what's been said, on the sides of vested interest in companies. So whose security are we really protecting, and are we paying a terrible price for that in terms of the common person?

MR. WITTES: A couple of thoughts on that. The question of whose security is one that we often skate over, but I think it's a really important question.

Let me just give you what will sound initially like an off-the-wall example. But consider the second amendment for a moment. Now, if you were thinking in pure mass security terms, a constitutional right to keep and bear firearms would seem kind of maladaptive; right? Particularly if you can imagine modern weaponry. On the other hand, if you're thinking as the framers of the constitution did in terms of the ability of a free state to defend itself, it actually makes all the sense in the world.

Now, contrast, and Ben mentioned that we talk about this a little bit in the book. So that's a question of whose security are you thinking about. Right? Are you thinking about the security of the state itself and the capacity for self-government? Or are you thinking of protecting the security of people, say, against school shootings?

Contrast the way we handled the new technology of firearms with the way we handled the new technology of the automobile. Now, if you had said, "I have a great idea. Let's have a constitutional right to drive. It's part of the right to transportation. People have the right to go where they want. Why don't they have a right to get in a vehicle and drive the way they would have the right to get on a horse?" And the answer is, well, because having large numbers of people operating heavy machinery at high speeds in condensed places is really unlikely -- is really likely to produce bad outcomes if you don't regulate it.

And so in contrast to the Second Amendment, where we affirmatively protect the right to own and use firearms, in the case of cars, you have to get a license in advance. You have to -- the state has the ability to take away that license. You have to operate and insure a registered vehicle that's identifiable from a distance. So you can't drive anonymously. And you're potentially liable for action damage that you inflict in the course of your registered licensed driving of the vehicle.

Now, this, to me, shows that when we see new technologies, it is not a given that we say, hey, this has beneficial uses, both firearms and cars have beneficial uses, yet our approach to them is very, very different. And part of the reason it's different is exactly what your question suggests, which is that we are asking different questions of whose security and whose rights we care about.

MS. BLUM: And also where the source of the threat is. So I like the idea that you brought the sort of corporations. So there's always this debate about who do you fear more, the Big Brother or the Little Brother; right? Which has been kind of the social contract debate all along. Who got it more right -- Hobbes or Locke? And we sort of suggest Locke got it more right in the sense that the Big Brother can be a source of threat as well.

But this is a matter of personal sensibility. So, you know, as far as I'm concerned, the NSA can read all my emails. Okay? This is a free pass to the NSA to read any and all my emails. Do you know what I'm worried about? You said you were a former professor -- my colleagues reading my emails. That's what I worry about. And I walk around certain that there are teenage kids who can hack my account with relative ease. I don't know how true it is, but that's what I'm worried about. And in a world where you're worried more about the Little Brothers -- and some of those Little Brothers are becoming very big. Some of them are corporations. Some of them are cults or just -- which also brings me to another point that Ben raised about, you know, do we need new technology to be violent? And I think the answer is clearly no. And a lot of what we see is sort of a return. One of the reasons I think ISIS is so eerie is because of those kind of old methods of killing people that they use, whether it's burning them alive or beheadings. I think what's interesting is that the technology, it doesn't replace the old violence; it introduces new actors.

So you could imagine the certain personalities are geared towards the traditional forms of violence. Okay? It takes a particular kind of person to get up close to someone and physically assault them. You don't replace that. What you do is add. I think the technology adds a host of actors who wouldn't be comfortable with the physical proximity, but the moment that you can inflict harm by clicking on your computer, it's just it becomes more attractive. So I can imagine Luis Mijangos. I've never met him. I don't know anything about the guy himself, but he may have not been comfortable being a Peeping Tom and actually peering out the windows and taking photographs of the women he was victimizing, but the fact that he could do everything through this mediated medium or mediating medium of a computer allowed him to do all kinds of stuff that he wouldn't otherwise do.

So in that kind of role of the threat, I am with you. I think that, you know, we talk a lot about the states and the governments and, you know, them as a source of threat and them as a source of defenses, but I'm totally with you that I'm also worried about how much attention is given to corporations and shielding their rights in exchange of the rights of individuals.

MR. GALSTON: I wonder if I could take you up on this IS question for just a minute, Gabby.

MS. BLUM: Yes.

MR. GALSTON: Because it seems to me that it sheds a very interesting, and perhaps contrarian light on some of the arguments in the book. And I'd make a handful of points in no particular order.

First of all, it seems to me that IS represents a fundamental critique of Al-Qaeda. And it's a very traditional critique; namely, if you're not a state with the attributes of statehood -- you know, territory, monopoly of violence, the capacity to administer a tax code, you know, and governing -- then you're nothing. Now, granted, as a nation state, IS has a somewhat capacious definition of the nation, the state it seeks to be. You know, 1.8 billion located around the world and perhaps more depending on how fixated they are on forcible conversion, but we don't have to go there. So that's the first point -- that IS represents an affirmation of the traditional idea of statehood.

The second point is this: that there is nothing particularly technological about the means of violence that IS employs. AS a matter of fact, it's about as retro as you can get. You know, curved knives to behead. Well, that takes us back 1,200 or 1,300 years. So the real effect of technology on IS is the multiplication of the number of people who are exposed to visual representations of the acts of violence. That's what's new.

MS. BLUM: And the recruitment mechanisms.

MR. GALSTON: And the recruitment mechanisms, too. That's absolutely true. Although I'd suggest to you that given the social circumstances that have nourished IS, and in some sense created it, very, very traditional networks would probably be, if not quite as effective in remote places, still remarkably affected. The willingness of disaffected young men and increasingly disaffected young women as well, to cast aside the restraints of a society that they feel doesn't recognize and honor them, and to join forces with something that promises not only dignity but revolutionary excitement, which every young person craves in one way or another. In other words, I guess the gravamen of all of my remarks is that there's less new here than meets the eye.

MR. WITTES: Okay. So let me try to talk you out of this.

MR. GALSTON: All right.

MR. WITTES: And this dovetails with a point that Ben made earlier, which is, why haven't we seen more of this? And the more you study the literature about what is possible, the more mysterious this question becomes. I don't actually want to talk much about what's possible because, you know, the answer is --

MR. GALSTON: It might give them ideas.

MR. WITTES: You know, I don't think anybody in this room is going to have ideas, but eventually C-SPAN is going to run this, and I just don't want to give people ideas.

The realm of the possible here is immense, and if you take some of it at face value, you have to at least consider the possibility as Nathan Myhrvold describes it, as species-ending. That is, you're talking about the possibility of individuals genetically engineering bugs that we have no treatment for and enhancing the lethality of those microorganisms. And I think that fact alone is qualitatively different from anything we've ever dealt with as a society before.

MR. GALSTON: Nuclear weapons?

MR. WITTES: So nuclear weapons --

MR. GALSTON: Species-ending.

MR. WITTES: Well, yes, in the hands of states.

MS. BLUM: A handful of states.

MR. WITTES: A handful of states. Now you're talking about the proliferation of that attack capacity to not anybody who wants it but to a much, much larger number of people not subject to regular surveillance. And that is a fascinating problem and a terrifying problem. And anybody who thinks I'm hyperventilating here needs to look at the literature and needs to look at the literature about what bugs have been created and what have been done to them. And it's all in the public domain. It's available.

So this makes Ben's question even more mysterious. Given this, why isn't -- why is ISIS beheading people? Why is Hamas doing suicide -- the run-of-the-mill mortar attacks; right? All these terrorist groups, they're so unambitious.

MR. WIZNER: Actually, that's not a hard question though, because we know that Hamas has political goals that would be undermined by killing probably millions of people with a bug. Right? And even ISIS has political goals. The real question -- the harder question --

MR. WITTES: Is the millenarian actors; right? The sort of -- so one possibility, and I flirt with this as the answer to the question -- it's a reassuring answer -- is that there actually aren't that many people who want to end the world. And if you control that for the number of them that have the sort of training it takes to do this, you're getting a vanishingly small number of people who are more likely than average to do crazy things that get them arrested. And so the problem may be that the universe of people that want to get it done is sufficiently limited.

The second component, which I think is a really important component, at least with respect to the terrorist groups, is that terrorist groups are both, as Ben says, often pursuing political goals, but even when they're not, they actually do tend to be relatively unimaginative and focus on what worked last time. If you look at the rise of the suicide bombing which happened starting in the '80s and then into the 1990s, the trajectory is like this. It goes from essentially never used anywhere to being the tool of choice over the course of a very small number of years. And the reason was that first Hezbollah used it modestly effectively, and then Hamas figured out how to mass produce it in 1994 and 1995 in a fashion that was extremely effective, and it operated as a demonstration project. And people saw it and that shaped their idea of what they should do. Every now and then you get one of these -- and this is going to sound like a weird thing to say -- a real genius terrorist entrepreneur, like KSM. And this was, you know, what KSM did on 9/11 was a very impressive reimaging in my mind of how you could use tools available to yourself to achieve grotesque horrible ends. And if you look at what Al-Qaeda has tried to do since then, a huge amount of it involves airplanes. Right? They have not similarly reimagined the great attack.

So I think part of the answer is that our foes are not always as imaginative and terrifying as we like to think they are.

MR. WIZNER: In that case you've done a profound disservice in publishing this book, haven't you?

MR. WITTES: Well, we've worried about that.

MS. BLUM: And maybe just one more, again, on the sort of more pessimistic side, we've seen more and more of that. So we've seen -- Ben mentioned Hezbollah and Hamas. Hezbollah has increasingly been using drones or trying to be using drones, some that it received from Iran and some that it's been trying to build itself. Hamas, in every round of the last few years clashes of Israel with Hamas, there has been more and more use of cyber and cyberattacks, whether from Gaza itself or of sympathizers with the Palestinian cause using the cyber domain as another battleground with Israel. None of this has so far been very harmful or even particularly noteworthy, but when you see more and more attempts, you see more and more of the sort of entering that world. I think it's going to change.

MR. WIZNER: But do these things belong in the same conversation? Cyberattacks which can cause harm but no one would argue, I think plausibly, that they remotely cause existential harm. Drones, suicide attacks, all of these conventional weapons, and the potential for a species-ending event. And I think the book kind of takes on all these scenarios. I think they're very different scenarios.

MS. BLUM: They're very different, and in some sense this is the sort of quote from Woody Allen at the end, "Why would you worry about homework if the world is going to end?" So that's right.

But we didn't want the entire conversation to be swallowed up by that because we don't want to get to the One Percent Doctrine. So we don't want that to be the conversation. We actually want the conversation to be about the much more -- if you want to call it mundane -- but possible or likely that is still going to be harmful even if it's not on massive existential levels.

MR. WIZNER: Right. The reason why I worry --

MR. WITTES: And which leads -- and which leads to the problem that Bill was describing, which is a problem of an erosion of confidence in state capacity to defend.

MS. BLUM: Or giving excuses, which is what you worry about. Giving excuses to governments to worry about that, and therefore, you know --

MR. WIZNER: Which is my concern. My concern is that if the message is fear, and that fear message includes the species-ending event, our politics are not capable of the kind of reason discourse that this book has done. And we're going to see people saying, "What do you want to do about Saddam's weapons of mass destruction? I mean, that's the kind of debate that we have right now. And so when you introduce the species-ending event into a policy world where actually we have responses, like in cybersecurity, like in drones and all of these, and you bring those into one conversation, I think we're going to have the worst politics and we're going to have worse responses.

MR. WITTES: It's a very legitimate concern.

We have time for -- we need to wrap up but we have time for one more question.

MS. BOVAT: I'm Sharyn Bovat, Voice of a Moderate. And I blog and I get a lot of cyberattacks. I have a bunch of dead computers that are Acers and HPs, and I switched to Apple. And I keep trying to get investigations and it's really hard. And then I finally went to a Cybercrime conference because they told me to go to the local police. I've gone to the FBI. I've gone to all these different agencies. And now they've finally created a system, but now they need an international system if the hackers are from China, or if they're from Russia, if people hire offshore hackers. So when you talk about cyberterrorism, they could be trying to terrify me by taking away my freedom of speech. And that's what I see these hacks are doing. When I get a virus or -- but I'm curious, when you start looking at terrorism, do you consider taking away a person's rights terrorism?

MR. WITTES: You know, this is such a good question, and it's a great one to end on.

Last year, when we had these attacks on Lawfare, I did feel myself to be a victim of crime, a victim of an attack in a way that being held up at gunpoint on the street never felt violated in the same way. And the reason was that somebody or some group of people was trying to shut us up. And almost, you know, I don't know who it was. I don't know why. I have theories about it but I have no evidence. But yes, there are a gazillion Little Brothers around the world who have the capacity to shut you up. And that is, actually, if you think about it just from a free speech point of view, a terrifying and horrible thing that, you know, we used to have to worry about government censorship, and now, you know, I pay protection money to a private company. I love CloudFlare. I'm not saying they're in a protection racquet. But I bitterly resent having to do it. And I do think that is a weird feature of the world of many to many threats that Little Brothers all around the world get to censor us and make us spend money to prevent ourselves from being censors. So I don't claim that money is speech for constitutional purposes, but sometimes speech costs money and this, you know, I do very much sympathize with the question.

MS. BLUM: And the other thing that it raises, which I think is really interesting, is the relevance of motivations. Right? So one way we sort of differentiate conceptually between crime and terrorism or crime and war is the motivations of those who do it. Ben Wizner raised earlier this puzzle about why we care so much about X number of deaths from terrorism but we are willing to bear costs of accidents that are thousands time larger. You could even take it to the world of crime and war, and even accidents, which is sort of more remote, but this country has anything from 13,000 to 17,000 cases of homicide a year. Okay? And we tolerate it. Second Amendment, crime, gun control, the normal way we deal with crime, and yet when there is one terrorist event, you know, statistically we're talking about 10 to 20 casualties a year, this is what we're talking about in terms of terrorism, the entire country is sort of in a much greater state of anxiety than it is about the 13,000 to 17,000 cases of homicide.

So it turns out that the motivations really matter to us. And even in your -- kind of the way you posed the question, with cyberterrorism or cybercrime, and the question is, does it matter? Right? How much do motivations matter? Does it matter that OxOmar, the guy I mentioned earlier wants to destroy the state of Israel, even though he -- you know, do his motivations matter anymore than the 16-year-old MIT freshman, you know, who is hacking just for fun -- should we have a different response to it or should we just think objectively about what is it that is being done and sort of address it as more in the actions?

MR. GALSTON: Maybe if we're winding down by giving our individual responses to this question, let me just add my two cents. Taking you up on the point you just made, which perhaps express some of the differences between us. You talked about feeling much more violated by what happened to Lawfare than being held up at gunpoint. Well, I was held up at gunpoint the month after I moved to the District of Columbia, and the sense that I experienced as I was asked to lie down on the grass, expecting that the next sound I heard would be the last sound I heard, that convinced me that Hobbes was absolutely right. Okay? If someone takes your life away -- someone, you know, absent religious convictions which vary, has taken everything away. All the rights in all 10 amendments, your constitution, your marriage, everything. And so if I ask, which is more significant personally and humanly, you know, an attack on my physical security or an attack on a right to disseminate my thoughts, I will simply repeat, "Hobbes was right." Life comes first. Everything else depends on it.

MR. WITTES: Ben, take the last word.

MR. WIZNER: Well, I'm happy to say that I've never been held up at gunpoint, or subjected to a denial of service attack. But maybe this is a way of circling back to the conceptual framework of this book; that liberty and security don't need to be thought of in this zero-sum tension. I am aware every day of what a privilege it is to be a human rights lawyer in a country that is both free and secure. I have colleagues in other countries who don't just have to worry about losing their cases, but have to worry about who steps into the elevator with them, or who's behind them in an alley. And so I urge everybody to read that discussion and to engage with the issues in this book, and I appreciate being able to engage with all of you today.

MR. GALSTON: Likewise.

MR. WITTES: Thank you to you both for joining us, and thanks to you all for coming.

Gabby has got to get to the airport right away, so please do not detain her on the way out. She's going to make a beeline for the door.

MR. GALSTON: So Ben will have to sign the books.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016