McFaul: You're listening to World Class from the Freeman Spogli Institute for International Studies at Stanford University. We bring you in-depth expertise on international affairs from Stanford's campus, straight to you. I'm Michael McFaul, the director of the Freeman Spogli Institute, and the host of World Class.

Today we have Amy Zegart. We're here for a special occasion to welcome and celebrate and applaud, this [McFaul displays the cover of Spies Lies and Algorithms], her brand new book! It's called Spies, Lies and Algorithms. By the way, Amy is one of the most talented writers of titles of anybody I've ever known, and the colon after the title is, “The History and Future of American Intelligence.” It's a big chunky book with lots of footnotes, but very readable, and we're going to talk about some of its main themes today.

Amy is a Senior Fellow here at FSI in the Center for International Security and Cooperation. She's also the Morris Arnold and Nona Jean Cox Senior Fellow at the Hoover Institution. She's an expert on U.S. Intelligence and National Security and has been featured by the National Journal, as one of the ten most influential experts in intelligence reform. I actually didn't know that, Amy, congratulations.

Her new book, as I just said, is Spies, Lies and Algorithms, and it investigates the role and responsibilities of the intelligence community in the United States, from George Washington’s spies to modern espionage satellites, and the emerging world of crowd sourced intelligence. It's a sweeping book, digesting a lot of history and data for us all. It's going be out February 1; be sure to get it!

Amy, welcome back to World Class.

Zegart: Boy, thanks, Mike, you do great advance! And it's such a delight to talk about this book with you, because you've been such a big part of my intellectual journey at FSI. I had so much help from colleagues at FSI and thinking through these ideas, so it's really nice to come home and talk about finishing a book rather than just writing a book.
McFaul: Well, we’re glad to have you here. Well, let’s just talk about the origins of the story for the book. You’ve thought about these issues for a long time, but this brings together a lot of different strands of earlier research you did. What was the basic inspiration? And what do you think is the important topic for people to understand about this issue?

Zegart: Well, I originally was going to write a different book, Mike. The seed idea of the book came before I came to Stanford when I was a professor at UCLA, and I was teaching an intelligence class. And just kind of on a lark, I did a survey of my students and I asked them about their spy-themed entertainment viewing habits. And I also asked them about their attitudes towards certain intelligence topics like interrogation techniques.

What I found was there was a statistically significant correlation between their spy-themed viewing habits and how they thought about certain intelligence practices; people who watch the show 24 all the time were far more pro-waterboarding, among other things, than students who didn’t watch spy-themed entertainment.

McFaul: Interesting.

Zegart: So, this got me really thinking, what do people know about espionage? Where do they get this information? And what I found was fairly horrifying, actually. Most Americans don’t know anything about the intelligence community, and when you’re talking about spy agencies in a democracy, that’s really problematic.

So, the original book was going to be me writing a textbook for the class I was teaching just to educate people about the intelligence community. And then one of the things about, you know, taking so long to write a book, is that the world changed: there’s Edward Snowden, there’s the internet, there’s satellites, AI, all this stuff happened in the past decade.

Suddenly, intelligence was at the crosshairs of this technological transformation. And so that’s why the book’s to the new cast is really through a technological lens, which I find fascinating. And it’s forward looking, not just backward.

McFaul: Right, you probably didn’t have the word ‘algorithms’ in your original title, right?

Zegart: No, it was not in the original title!

McFaul: That’s a great thing to remember, just how much has changed literally just in the last several years. We’ll dig into that in a minute.

Tell me though, what surprised you the most about what you learned? This is a big book; you’ve worked on it for years: what’s radically different about your thinking about these
questions, big or small, than it was when you started? And what details about the intelligence community do you think people reading the book are going to be most surprised about?

Zegart: Well, for me personally, the biggest surprise is the research that I did for one of my chapters about open-source intelligence and nuclear threats. Academics would say it’s a tough test; if ever you would think spy agencies would have cornered the market on intelligence, it would be nuclear threats, right? This is the most secret of the secret.

McFaul: And open-source, just to be clear, is information that is available to the public, right?

Zegart: Right. So, information that's available to the public meaning tweets, satellite imagery, reports, posted online, you name it. And what I found was, even in this arena, there's a whole ecosystem of non-governmental people tracking nuclear threats around the world and actually uncovering really important things. And some of those open-source nuclear sleuth are colleagues at CISAC at Stanford.

And so, part of what I learned in this two-year research project, came from walking down the hall and talking to my colleague Sig Hecker, former head of Los Alamos National Lab, and finding that he's doing all this work in the unclassified arena. And the more I dug into this, the more I realized that open-source intelligence, this publicly available information, is the ballgame in the future of intelligence. So secrets still matter; but they matter a whole lot less than they did even ten years ago.

In an area you know well: when Russia invaded Ukraine the last time, the most important intelligence about those activities and that invasion did not come from secrets; it came from selfies, right?

McFaul: Right.

Zegart: Russian soldiers posting selfies on social media for their family and friends. There is so much more insight that we can glean from open-source information. And the intelligence community has to figure out a way to do that better and connect with organizations and people who are in this ecosystem much better.

McFaul: A couple of things on that: I’m curious – because you start with George Washington – about the evolution and the balance of power and the balance of importance between HUMINT and SIGINT, between human intelligence and signals intelligence.

I worked in the government for a while, and so I was a big consumer of intelligence. I was struck by how there were some in the intelligence community that thought SIGINT was everything and signals intelligence and the National Security Agency was where all of our focus should be. And others, more traditional, said, “Without human intelligence, without the
conventional, classic spies like the ones that your students were watching on TV [we're vulnerable].

(By the way, when I was the U.S. ambassador in Russia, The Americans was a very popular television show that people all bootlegged to watch in Moscow).

But how would you assess how that has changed in terms of how you need both? Is one more important than the other? Or are they better working synergistically?

**Zegart:** You have to have both, right? It is an ‘all of the above’ endeavor. But there's been a risk, I think, with technical intelligence. One former intelligence official put it to me this way. He said, “We think if something costs a trillion dollars to get, it must be worth a trillion dollars.” And that's not true. These fancy satellites that we have cost billion dollars to make and launch, therefore the intelligence they provide must be worth it. Sometimes that's true, but often it's not.

**McFaul:** That’s a great point. Whereas other kinds of cheaper ways of acquiring that information might be just as valuable.

Well, related to that, is it possible for one person – because you've now tried to do this – to be expert across all kinds of domain spaces of intelligence? Or has it become so complicated that you can't be an expert on algorithms and spies in the traditional sense, at the same time?

**Zegart:** You know, I don't think it's possible. I've spent almost thirty years doing this, and I'm not an expert in every area of intelligence. And I think it's getting harder. And it’s getting harder, because the technology is harder to understand. So how does AI actually work? What are its limits? Why does an algorithm misidentify a bicycle as a sloth? AI fails in weird ways.

And then there's the other problem which you've lived well, which is the overclassification of intelligence.

**McFaul:** Yes.

**Zegart:** And so even if you're trying to be an expert in intelligence, you don't have access to all the right information. There was this wonderful quote from when the Washington Post did their “Top Secret America” investigation. And they quoted then-director of National Intelligence, Jim Clapper, who said, “There's so many special compartment and programs, the only person with visibility into them all is God.”

And so even if you're in the inside, you don't have access to the full array of intelligence, even when you should have the full array of information to enable you to understand and gain better insight.
McFaul: Well, related to that – and it's something you and I've talked about before: there's also the explosion of data, right? The quantity of intelligence is orders of magnitude today, what it probably was just 10 or 15 years ago. I was in the government several years ago, and I'm sure it's greater today.

So, how do you aggregate that intelligence? First, how does the intelligence officer do it? And then tell us what you've learned in terms of looking at the research for this book about how are they trying to cope with that. And then how do they do it in a way that can be useful to the consumers, the policymakers and members of Congress – we'll get to Congress in a minute – but particularly to policymakers. It's not very useful to a policymaker if you hand them a 300-page document when they have a very busy day.

So, to the aggregation question and separating out what's important versus what is noise: how does the intelligence community do that? Or how should they? And then how do they prepare products, as they like to say, that could actually be digestible and usable for the policy community?

Zegart: This is something that I was really fortunate to be part of a task force at CSIS that was co-chaired by Avril Haines, the current director of National intelligence, and Stephanie O'Sullivan, another career veteran in intelligence.

We looked at this question of AI and its associated technologies: how can AI be of greater use to the U.S. intelligence community? What do we need to do to adopt it? And this is a moment where, as you say, Mike, we're drowning in data. The amount of data on Earth is estimated to double every two years. Think about that for a minute. It's just an astounding amount of data. And it's too much for any human to deal with.

So, if intelligence is in the business of collecting or finding needles in haystacks, the haystacks are growing exponentially. The intelligence community has to use artificial intelligence and other tools to augment human analysts. There's a big debate about what can machines do better than humans and what humans can do better than machines.

To give you one example: pattern recognition and counting surface to air missile sites over a large piece of territory. One intelligence agency – the National Geospatial Intelligence Agency – developed a partnership with a university team to do a machine learning algorithm to search for surface-to-air missile sites in a huge area of China. And so the algorithm was able to do this with the same level of accuracy as a human analyst – 90% accurate – but the algorithm did it eighty times faster.

McFaul: Wow.
**Zegart:** So what does that do? That frees up the analysts to then ask questions about things like intent, which humans can figure out much better than machines. What is Xi Jinping thinking by putting these missile sites here as opposed to there?

But it goes beyond pattern recognition. Imagine an algorithm that can scan news items that you can't on your Twitter feed – though you are pretty superhuman on Twitter, I have to say. And imagine an algorithm that can scan it and send you stuff that you might not have thought would be relevant to what you're doing based on what your portfolio might be.

Or imagine an algorithmic red team. So, you have humans that are developing assessments of what is Putin going to do in Ukraine, and you've got a red team that's just algorithms aggregating data, so that you have a sort of competitive analysis between humans and machines that can make the humans better. Those are the kinds of things that intelligence agencies need to be doing much more with AI.

**McFaul:** Interesting. And what about then feeding to the consumers? Any lessons to be learned about that?

**Zegart:** I'd be curious to know what you think. You've been at the receiving end of intelligence. When you're doing every other part of your day, you have user interface that tracks what you read, how long you spend on something, and whether you found it useful or not. Well, intelligence needs to do a better job with customers about that, too.

**McFaul:** That's a great insight, actually. Yeah, you're right.

**Zegart:** We need to treat that user interface as a more interactive customer response, because intelligence is only as useful as the policymaker thinks it is. We all react to information formats in different ways, so better understanding that in an evidence-based way would make intelligence more valuable.

**McFaul:** That's a great insight. I was in the government many years ago, but even the way you get it in an envelope and the time it takes to open those top secret classified ones, let alone going to separate room for compartmentalization in a busy day, reduces your incentives to do that. Thinking of the consumers as consumers, and trying to get that right; obviously, artificial intelligence could help with that, too. I hadn't thought of it that way.

**Zegart:** Well, and you've hit on something else, Mike, which is speed. Intelligence has to move at the speed of relevance. And so if you've got policymakers that are seeing things in real time on their phones, but intelligence is waiting for the paper to come with the briefer to get to your office, you've been overtaken by events already.
**McFaul:** And to add to that other point you made about open sourcing, there's a lot more information available to people in real time, including, your great point about 2014 and the Russian invasion. By the way, I was just looking at that with respect to the buildup now, and there hasn't been as many photos from soldiers, and people are wondering why that is. A policymaker has all that as well, so there's more of a competition in this information space.

But I want to pivot here, because I know we don't have much time. There's this word “lies” in the title of the book. Tell us what that word connotes and why I was surprised when I first saw it. “Spies and lies.” Spies aren’t supposed to lie! Tell us what that's about.

**Zegart:** So it's really about two things, right? One is about the history of deception, because intelligence is about deception. We don't want our enemies to understand all of our military capabilities, for example, or what our intentions are. We have strategic ambiguity with respect to Taiwan, for example, and what U.S. defense commitments might be. Some believe that's really useful. Others are now questioning that.

But the point is: if you think about D-Day, we did lie. We deliberately deceived Hitler about where we were going to land, and that is what helped win the war.

**McFaul:** And that's part of the game, right.

**Zegart:** But I think the technology piece of the line is that deception has gone from elites deceiving elites about where their troops are, and whether they're going to attack, to mass audience deception and this disinformation-information warfare of domestic audiences like we're experiencing here in the United States.

Understanding deception, not in a pejorative sense, but just as an in an analytic frame – how does deception work? How is technology changing the deception game – is really important.

**McFaul:** That's a great insight. I know this is an unfair question, and it's going to lead to my last question about “How does one research a book about something that's classified?” But, how is the United States doing compared to our adversaries in the world of spies, lies and algorithms? Are we ahead of the game? Slightly ahead? Where are the Russians? Where the Chinese? How do you see that today as a snapshot, and where do you see it going in 10 or 20 years?

**Zegart:** Well, Mike, you've given me a question for my next book.

**McFaul:** I know, it’s unfair.

**Zegart:** Totally unfair! That's comparative analysis of intelligence agencies around the world.
**McFaul:** Right, I should point out that this book is only about the U.S.

**Zegart:** Only about the U.S. But thanks for that homework assignment. I appreciate that.

What I will say is, we already know in some areas that are concerning where the Chinese appear to be ahead. So, public information has reported that when it comes to our human assets on the ground in China, that network was blown a few years ago. Many were executed. Others were imprisoned. And of course, the $64,000 question there is, “Why?” What was the counterintelligence failure there?

**McFaul:** And we still don’t know, right?

**Zegart:** We still don't know. There's some evidence that it could have been a human mole. But it also appears that there was a technological weakness in the system that enabled communication between CIA case officers and their assets. That system appears to have been really weak, and that led to the blowing of this entire network.

**McFaul:** Which is a great theme from your book, by the way. That's something you wouldn't have had 30 years ago. It would have been all physical.

**Zegart:** Exactly. And even worse than that, it was a temporary system. This again comes from public reporting, that it was a temporary computer system to communicate with unvetted people.

**McFaul:** Wow.

**Zegart:** But it had a weakness so that you could migrate from the temporary system to the permanent system?

**McFaul:** Oh, wow.

**Zegart:** Which was really bad. So, I think the Chinese are really good at that. And they're very good at offensive intelligence here in the United States and penetrating lots of different areas. Are they better than United States? I don't know. And to preempt in your last question, I don't know the full story because it's classified.

But I will say this: I think in terms of tradecraft, I think the United States is ahead. And by tradecraft, I don't just mean case officers and how they meet with people. I mean analytic tradecraft.

One of the benefits of being in a democracy as opposed to an authoritarian regime is we challenge each other. We have dissenting views, and we won't get executed if we present
them. And that makes for better intelligence and analytic tradecraft. And I think that's a real comparative advantage.

**McFaul:** Well, my two last questions are related to that. First, how do we in a democracy have sufficient oversight over the intelligence community and what they're doing? We have our congressional intelligence oversight committees, but how do you assess how they do their jobs when, by nature, it's a difficult thing to do because everything is classified?

**Zegart:** It's a hard thing to assess, but there are some metrics we can use. We can – and I have – looked at any kind of metric I can for oversight in Congress. How many hearings do they hold? What percentage of those hearings are public? Because a key oversight function isn't just making sure that these agencies obey the law, it's also being the ambassador between the secret world of intelligence and public support. These agencies can't talk about what they do. They only have Congress, and they only have the intelligence committees to vouch for them for the American people. So those open hearings are actually really important for the committees to hold.

So, I looked at that and, in fact, the number of open hearings or the percentage of open hearings has actually gone down over time compared to the sort of heyday of the 70s and early 80s.

Then we can look at what kinds of questions do the intelligence committees ask when they do have hearings. For example, I looked at I at the confirmation hearing of Bob Mueller to be FBI Director before 9/11. He started the job one week before 9/11.

**McFaul:** Just one week before, wow.

**Zegart:** So, I looked at the hearing and I thought, “Was the Senate Intelligence Committee really worried about terrorism?” The answer was no. There were only three questions asked of the nominee, Director Mueller, about terrorism. And they all came from one Senator John Edwards, amazingly enough.

The committee spent more time asking about kidnapping than they did terrorism, which is a pretty good indicator that the committee wasn't looking ahead despite getting briefings for three years in a row that terrorism was among the top three threats facing the country. They didn't ask tough questions of the FBI director.

**McFaul:** Well, that leads to my last question. I was living in Russia in the 90s: ’94 and ‘95. And I'm a graduate student at the time, and friend of mine came, an economist. And I asked her what she's writing about, and she said, “Oh, I want to write about corruption in Russia.” And I looked at her and I tried to talk her out of it. How can you write about that issue? It was kind of dangerous to write about corruption in Russia in the 1990s as an American. And I just
wonder, in closing, how do you do this kind of research? I mean, these are hard topics. What are the things you've learned for how to do this kind of research and some of the things that are just too challenging that you just have to leave in the black box?

Zegart: Oh, such a hard question! It's a crazy field to go into because as an academic, your whole career hinges on data. And you don't know whether you're going to get data in the intelligence community, and you don't even know who to call to get data.

So, I had an experience that I write about in the book where at one point, a senior public affairs officer from the CIA came with a bunch of analysts to do a simulation for my class. And he wouldn't give me his business card or tell me his last name. This is a guy in public affairs!

McFaul: Wow!

Zegart: So yes, there are some challenges there. But I've learned a couple things. Number one: there is information in the public domain, and you have to be tenacious about reading it, and hunting down the footnotes. There's great stuff in footnotes that most people overlook. I found a lot in footnotes in DOJ Inspector General reports and in appendices to congressional hearings, for example. So, you have to be sort of a tenacious, sort of primary source researcher. There's good stuff there, you just have to search for it.

And the second thing I learned is that you have to talk to people on the inside. Everybody's got an agenda. We can't, from the outside, understand the constraints and the operations of this intelligence community without talking to people. I spent a lot of time trying to develop trusted relationships with people so that I can better understand where they come from. Now, that doesn't mean I always agree with them; I disagree with a lot of my sources. But I try to give them the courtesy of saying, “Here's my perspective, and I'd like to get your answer. What's your response to that?”

I really am trying in this book. I take it very seriously. I hope people will read this book and say, “She was fair. And she was accurate.” And come away feeling that I don't take aside on one thing or another – I try not to – and that students understand the best arguments on both sides of a debate like NSA warrantless wiretapping. I want them to challenge their own thinking, not proselytize one point of view.

McFaul: That's a great place to end. Thanks, Amy, for being with us on World Class. Congratulations on the book. For those of us who have written books, they're really hard things to finish. It's really hard to get publishers to put out these kinds of big, thick research books, and they won't publish them in the future unless you buy them.

So I want you to go out February 1, and get your own copy of Amy Zegart's, *Spies, Lies and Algorithms: The History and Future of American Intelligence*. 
Thanks, Amy, for being here!

**Zegart:** Thanks, Mike!

**McFaul:** You've been listening to World Class from the Freeman Spogli Institute for International Studies at Stanford University. If you like what you're hearing, please leave a review and be sure to subscribe on Apple, Simplecast and SoundCloud to stay up to date on what's happening in the world, and why.