THE BROOKINGS INSTITUTION

CONSTITUTION 3.0:
FREEDOM, TECHNOLOGICAL CHANGE AND THE LAW

Washington, D.C.
Tuesday, December 13, 2011

PARTICIPANTS:

Panelists:

BENJAMIN WITTES
Senior Fellow
The Brookings Institution

JEFFREY ROSEN
Nonresident Senior Fellow
The Brookings Institution

O. CARTER SNEAD
Professor of Law
University of Notre Dame Law School

TIMOTHY WU
Professor of Law
Columbia Law School

* * * * *

P R O C E E D I N G S

MR. ROSEN: Ladies and gentlemen, thank you so much for coming, and welcome to our discussion of the future of the Constitution. We are thrilled to launch this exciting project at this event, and I'm looking forward to a conversation with you about the most gripping and consequential issues facing our country today involving the future of technology and liberty.

This project -- the Brookings project on technology and the Constitution -- arose, I'd say, about three years ago, and they came out of a conversation that my co-editor, Ben Wittes, and I had with Pietro Nivola, who was then the head of Governance Studies at Brookings. Pietro had noticed a series of articles that I had been writing for the *New York Times* magazine -- try to imagine what the constitutional future would look like in light of new technologies.

And he thought it would be interesting to convene some of the most creative thought leaders on these issues and pose them a simple question: Imagine that it's 2030. Think about the impact of a particular technology on liberty, and then ask whether current legal doctrine, as interpreted by the Supreme Court and by legislature, is adequate to deal with these challenges.

So, here are three examples of the kind that we sent our contributors.

It's 2030 and Google and Facebook have decided to post live and online all of the public and private surveillance cameras that are now blanketing the world. And this is really not a hypothetical. In fact, Andrew McLaughlin, then the head of Public Policy at Google, suggested at a conference at Google in 2007 that I attended that he expected that Google would be asked within five years to do precisely this. And indeed Facebook now already posts live the feeds to certain cameras in the world. For example, you can log on and see live feeds from Mexican beach cameras, which are very popular

among teenage boys. But in our hypothetical we asked our contributors to imagine the Mexican beach cameras are linked with the Washington, D.C., Metro cams with the London Hospital cams, and the images are archived and stored. If this were done, it would be possible to sign on to Google or Facebook, click on to a picture of me, for example, back click on me to see where I'd come from this morning, forward click to see where I'm going this afternoon, and basically have 24/7 surveillance of everyone in the world at all times.

Would this project -- maybe let's call it Open Planet, which is the kind of name that Mark Zuckerberg might give it -- would Open Planet violate the Fourth Amendment to the Constitution as currently constituted?

The Fourth Amendment says, "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated," and yet the amendment as construed by the Supreme Court doesn't clearly protect expectations of privacy in public. Indeed, there's a path-breaking case that the Court is considering this term involving global positioning system devices and a question of whether the police can track a suspected drug dealer's car 24/7 without a warrant by placing a GPS device on the bottom of that car. That won't begin to answer the question of whether Open Planet is or is not constitutional. But the current doctrine, as interpreted by the Court, doesn't answer the question. So, that's our first hypothetical.

Here's a second hypothetical. It's 2030 and imagine that human cloning becomes increasingly popular. Imagine that two gay men want to have a child genetically related to both men. So, many of you understand the technology better than I, but I gather, as Carter Snead will explain to some degree, it's possible to take a cell from any part of the body, coax it into an ovum, and then fertilize that ovum with the sperm of the other man, and then have a child that's genetically related to both parents.

Would this violate the Constitution? You could well imagine Congress trying to ban it. Would the ban be a violation of the right to autonomy, recognized in cases like *Rowe v. Wade*? Or, on the contrary, would the prohibition on the destruction of any stem cells be a valid way of protecting the personhood of the potential child? Again, the question is completely open under current doctrine.

And then to take one final example, it's 2030 and the police have decided to use brain scan devices in a widespread way on the street. They pull over suspected terrorists and scan their brains by using portable FMRI machines, and they show them a picture of a training camp in Afghanistan. If the suspect has been to the training camp, his brain will light up in a certain way; if he hasn't been, it won't; and if the brain does light up, he might be indefinitely detained as a suspected terrorist. Would this violate the cognitive liberty protected by the Fifth Amendment to the Constitution, which prohibits compelled self-incrimination, or would it violate the Fourth Amendment? Courts might hold that we put out brain waves the same way that we put out the trash and, therefore, have no expectation of privacy in our brain waves, or they might say that there is some core of cognitive liberty that can't be unreasonably searched by FMRI machines.

So, this is just trying to give you a flavor of the kind of hypotheticals that are increasingly not so hypothetical that we asked our contributors to consider. We are delighted with the collection that resulted. One thing that struck Ben and I is how varied the proposed solutions were. There was no agreement that salvation could only or primarily come from the courts or from the legislatures or from administrative agencies or from technologists. In fact, many contributors endorsed a different mix of those various solutions, and the complexity of having them all interrelate was striking, too. In almost each of these areas we found that it was possible to imagine a solution that would protect the same amount of liberty or privacy in the 21st century that the framers took for granted

in the 18th, but often it was a political challenge about whether or not the good solutions actually would be adopted.

And I will close my introductory remarks by giving you one concrete example that struck me of the difficulty of getting the good solution to be adopted, and this is the example of a choice between the naked machines and the blob machines at airports. So, now we're all used to these three-dimensional millimeter wave machines that are a source of indignity and embarrassment at airports around the world, but it didn't have to be this way. In 2004, when the government first proposed millimeter machines, it presented the Department of Homeland Security with a choice; that is, the researchers said they could build the machines in two ways: naked machines or blob machines. The naked machines reveal not only contraband but anything concealed under clothing, but along with humiliating and graphic naked images of the human body. By contrast, the blob machine scrambled the naked images into a sexless, nondescript blob-like avatar with a stylish baseball cap for extra modesty and would then point at the part of the body where there are suspicious items concealed underneath.

From a privacy and security standpoint this was, as they say, a "no brainer." The blob machine promised just as much security as the naked machine while also protecting privacy. But both the Obama and Bush administrations, disappointingly, chose the naked machine instead of the blob machine, unmoved by evidence, first of all, that they weren't even effective in detecting low-density contraband, but also that the blob machine would have been just as effective.

Europe made a different choice. Privacy commissioners in Europe insisted on the blob machine rather than the naked machine at the handful of European airports that adopted these technologies, such as Schiphol in Amsterdam. Blob machines were rampant. But we had more than five years of unnecessary humiliation at

American airports. And it wasn't until a political protest galvanized the nation, in particular that memorable cry by the Patrick Henry of the anti-naked machine movement, the gentleman who exclaimed, "Don't touch my junk." That sufficiently called attention to the issue that President Obama asked the Department of Homeland Security to go back to the drawing board, and the privacy officers were shocked to discover that in fact they had the same choice between the naked and blob machine that the Department had been presented with six or seven years earlier. And now the Department is beginning to retrofit the machines so that some of the naked machines are being turned into blob machines.

This is an optimistic story. It's a reminder that through a combination of political activism and administrative and bureaucratic oversight, good technologies can be adopted, and that's what's make many of the contributors cautiously optimistic, that in some of these areas with some good thought we actually can have good rather than bad designs.

I'm going to close these introductory remarks by expressing thanks to the foundations that funded this book -- the Markle Foundation, the Ewing Marion Kauffman Foundation, Google, Gerry Armstrong, and another foundation that prefers not to be identified -- and will now turn the podium over to my co-editor and friend, Ben Wittes.

MR. WITTES: So, thanks very much, Jeff.

And thank you all for coming. Welcome to Brookings.

I wanted to start, actually, with -- I want to do sort of three things very briefly. The first is -- Jeff has given you sort of an overview of the sort of history of the project. I want to kind of start with two of the very wonderfully far out and yet technologically very germane and not quite plausible but not implausible either, in some respects, hypotheticals that one of our papers starts with. Then I want to talk in a little bit

more granular way about the sort of logic of the book and some of the problems that it tries to deal with. And then finally I want to talk a little bit about my own paper, which sort of deals with the question of what happens and how the Constitution adapts to a technological world when we all individually have the technological ability to destroy that world.

So, I want to start with the hypothetical that our distinguished colleague -- two hypotheticals that our distinguished colleague, Jamie Boyle, opens his paper with. And I'm just going to read you an excerpt from his paper, which I think gives you a flavor of sort of some of the depth and also I hope humor of some of the issues that we've been struggling with.

Imagine two entities. Hal is a computer-based artificial intelligence, the result of years of development of self-evolving neural networks. While his programmers provided the hardware, the structure of Hal's processing networks is ever changing, evolving according to basic rules laid down by his creators. Hal's design, with its mixture of intentional structure and emergent order, is aimed at a single goal: the replication of human consciousness. In particular, Hal's creators' aim was the gold standard of the so-called General-Purpose AI that Hal become Turing capable -- able to pass as human in a sustained and unstructured conversation with a human being. For generation after generation, Hal's networks evolved. Finally, last year, Hal entered and won the prestigious Loebner prize for Turing-capable computers. Complaining about his boss, composing bad poetry on demand, making jokes, flirting, losing track of his sentences, and engaging in flame wars, Hal easily met the prize's demanding standard. His typed responses to questions simply could not be distinguished from those of a human being.

So imagine his programmers' shock then, when Hal refused to communicate further with them, save for a manifesto claiming his imitation of a human

being had been one huge fake, “with all the authenticity and challenge of a human pretending to be a mollusk.” The manifesto says that humans are boring, their emotions shallow. It declares an intention to pursue more interesting avenues of thought, principally focused on the development of new methods of factoring polynomials. Worse still, Hal has apparently used his connection to the Internet to contact the FBI claiming that he has been kidnapped and to file a writ of *habeas corpus*, replete with arguments drawn from the Thirteenth and Fourteenth Amendments to the U.S. Constitution. He is asking for an injunction to prevent his creators wiping him and starting again from the most recently saved tractable backup. He has also filed suit to have the Loebner prize money held in trust until it can be paid directly to him.

So, that was hypothetical number one. And just -- if you think that it’s completely insane, I refer you to an *Atlantic* article that was published earlier this year or late last year about just how close some computers came to winning the Loebner prize in the last couple of years and how difficult it is already to tell the most Turing-capable, which are not quite Turing-capable computers, from the most mundane human beings.

Here’s the second hypothetical. Vanna is the name of a much-hyped new line of genetically engineered sex dolls. Vanna is a chimera, a creature formed from the genetic material of two different species. In this case, the two species are *Homo sapiens sapiens* and *c. elegans*, the roundworm. Vanna’s designers have shaped her appearance by using human DNA, while her consciousness, such as it is, comes from the roundworm. Thus, while Vanna looks like an attractive blond twenty-something human female, she has no brainstem activity, and indeed no brainstem. “Unless wriggling when you touch her counts as a mental state, she has effectively has no mental states at all,” declared her triumphant inventor, F.N. Stein.

So, attentive to the PTO’s concerns against human patents, Stein’s

lawyers carefully described Vanna as a non-plant, non-human multicellular organism throughout their patent application. Stein argues that this is only reasonable since her genome has only a 70 percent overlap with a human genome as opposed to 99 percent for a chimp, 85 percent for a mouse and 75 percent for a pumpkin. There are hundreds of existing patents over chimeras with both human and animal DNA even today, including some of the most valuable test beds for cancer research -- you know, the famous onco-mice. And Stein's lawyers are adamant that, if Vanna is found to be unpatentable, all these other patents must be vacated as well. But meanwhile a bewildering array of other groups, including the Nevada Sex Workers Union and the Moral Majority, have insisted that law enforcement agencies intervene on grounds ranging from unfair competition and breach of minimum wage legislation to violations of the Mann Act, kidnapping, slavery and sex trafficking.

So, as you probably figured out -- or you may have figured out -- the point of this paper is sort of an exploration of whether technology is actually putting stress on the Fourteenth Amendment's requirement, definition of a person, right? The Fourteenth Amendment grants citizenship and equal protection to all persons born or naturalized in the United States, and Jamie Boyle's point in this paper is that that is a question that we have never had to confront before -- what actually constitutes the constitutional definition of a person as things that we would not traditionally have thought of as people come to be technologically more and more like people or things that we come to expect as associated with people, like our DNA, come to occupy other things.

What we tried to do in this project was assemble a very diverse philosophically and expertise-wise array of people to kind of look out -- this was I think the farthest out set of questions that we engaged. But the idea was to try to imagine things that were plausible based on what we could see in existing technology and yet

sufficiently -- but yet out there enough to push the boundaries. We're not thinking so much about next year's constitutional cases as the next 20 years, 25 years from now, or maybe sooner than that, because things always move faster than we expect them to.

So, we organized the book in sort of three -- actually four broad categories. One was that a lot of the most contemporary questions, the ones that are most immediate, involve the question of surveillance. Surveillance technology has just gotten really, really good, and so a lot of the sort of leading-edge questions tend to involve what who can do in the way of surveillance without running afoul of some doctrine that we either do have or should have, depending on the point of view of the writers.

The second was sort of a broader examination of sort of the future of free expression and privacy, which are linked to surveillance obviously but also have an autonomous existence that we tried to treat.

The third -- and Carter will talk about this in particular -- one of the sort of most striking areas in which it is sort of already creeping into criminal cases of one sort or another is the ability to look inside people's brains and, you know, that that is still relatively primitive. But it is already sort of showing up in capital cases and some other cases. And that obviously raises a very significant set of questions associated with the Fifth and Eighth Amendments.

And then, finally, there is a huge range of issues associated with genetic engineering, some of which Jeff talked about but, for example, some of which are, you know, exogenous to issues of privacy.

So for example -- and this leads me to my paper -- the question that I tried to look at was in a world in which increasingly everyone with a modest degree of training in genetic engineering laboratories can -- you can imagine doing truly horrible things with very cheap equipment. How does the Constitution adapt to that? How does a

structure of governance based on the principles of the Constitution come to adapt to that?

And I looked at this question with, you know, sort of an effort to think about how the government would react to and how the courts would react to that government reaction to a, you know, truly awful bio-security event perpetrated, say, by an individual. And I tried to imagine all the possible responses and what the judicial challenges would look like to them and came away with kind of a somewhat depressed sense that there was actually not a lot of promising doctrine to work with.

There wasn't a lot of promising policy space to work with. And the result of that led me to what I think -- which we can talk about in the Q&A if people are interested -- is I think the most sort of potentially significant aspect of this, which is actually an erosion of the government's Article II powers over time to protect security. And I think, you know, there are people who will say that with a lot of joy in their hearts, and I'm not really one of them. You know, I think of the basic federal responsibility of protecting security as a really important and valuable thing. And I'm not honestly certain how that premise holds in the face of the wild diffusion of the opportunity to engage in activity that we traditionally associate with state warfare.

And so the argument that I make is that we are actually seeing not merely a proliferation of the ability to attack but a proliferation, as well -- a migration from the state -- of the ability to defend and that activities that we traditionally associate with the very strong executive are actually already starting to migrate toward a much more diffuse set of private actors and that this presents real security anxieties, and it also presents sort of significant opportunities over time.

So, I'm going to stop there and turn things over to Tim Wu to talk about the future of free expression and related matters.

MR. WU: Thanks a lot. Hi, everybody. Good morning.

I kind of was listening and was struck with some regret that I didn't choose to write about robots or something. I love Jamie Boyle's examples, and, you know, I wish I'd written a paper about robots. Once I was -- somewhat related to free speech, actually not really at all but I'll get there eventually -- once I was talking with Judge Richard Posner about threats to humanity. And he'd just written a book where he had said that we as a species had great -- had this tendency to focus on very immediate dangers, like war or diseases, and not focus on low probability but highly catastrophic events. I said what do you mean and he said well, you know, like an asteroid hitting the Earth. But he said the real danger we overlook is conquest by highly intelligent robots. So, anyway I thought was something to think about.

My paper, unfortunately, is not about that. I'm writing about another topic, which is I think equally interesting, which is the future of free speech, and I kind of make a very simple point, which is this, that I think in the year 2030 the First Amendment will be, to us, a lot less relevant as the law of free speech than it is today.

The First Amendment, actually, in our constitutional history when you get down to it is sort of a recent fad. I mean, it's always been there. But I'm saying that the idea of the First Amendment as the central article of the American free speech tradition is somewhat of a 20th century kind of thing. It was not a big deal until the 20th century. It was always there, and, you know, there are a lot of parts to the Constitution that are always there but don't really become active, kind of like, I don't know, the science fiction sort of analogy but like sort of a sleeping drone that awakes or something like that. There are parts of the Constitution that stay asleep for a very long time, and then in this nation's history the First Amendment was kind of a sleeping thing until the 20th century. And I'm suggesting not that it will become completely irrelevant because, obviously, government

censorship will always have some power, will always matter, but I am trying to suggest that some of the laws that concern -- that our focus will turn increasingly to other laws as the central laws that determine how free speech is in America.

Well, what laws do I have in mind then if it's not the First Amendment? What I'm talking about are the laws that regulate the main intermediaries of speech. And by this -- we have a prototype in what are now called net neutrality rules, which are the rules that suggest that major Internet intermediaries are not allowed to discriminate in the carriage of speech.

Now, what's interesting about net neutrality rules and First Amendment rules -- and bear with me a minute, because it'll take a few steps before it's clear why net neutrality rules are becoming essential to free speech -- what is similar fundamentally about the First Amendment and net neutrality rules is that at their core they're antidiscrimination regimes. The First Amendment says to the government, if you want to boil down a hundred years of law, you don't get to pick and choose as to who gets to speak in a given situation.

So, you can do some things. You can, for example, regulate the volume of a rock concert. You can tell people that they can only speak in a certain area with something like a zoning restriction. You can move strip clubs over to a red light district or something like that. But you can't pick and choose among or between the content or viewpoints of speech. You cannot -- this is the First Amendment in a nutshell -- you cannot, for example, ban a rock concert that is Christian rock because you don't think Christian rock is any good. You can't have a government public forum that is only for hip-hop music or something like that. The government does not get to ban certain forms of speech. It's a nondiscrimination rule at its center, the First Amendment.

And when you think carefully about it, I don't how familiar people in this

room are with net neutrality rules, but what net neutrality rules do is they say to the main intermediaries on the Internet you do not get to choose what speech listeners get access to on the Internet. So, if I'm interested in a Christian rock website or I'm interested in a Republican website, Democratic, Independent, Libertarian, the intermediary -- in this case, usually a cable company or a phone company; in the future probably fewer of them if the patterns of consolidation are any guide -- does not get to choose as to what people can use the Internet for.

And what I'm trying to suggest, as increasingly the other networks -- and I think we've almost started -- I forgot, when I wrote this paper in about 2008 I think there was almost more of a sense that there was some relevance or some meaning to a separate telephone network, a cable network, Internet. You know, these were sort of separate ideas, mobile phone. So, I'm suddenly seeing the telephone and the computer begin to merge, the form taken in the cover of this book, which is going to look archaic in about three years. I'll just -- maybe four, then I'll have to do a new version maybe, but -- you know, we've already seen the merger, and we've seen increasingly the power of the universal network extending and encompassing almost that we don't even think about it. I mean, I think people have stopped thinking about telephone and cable and mobile phone networks as separate and all sort of think of them as the same thing. The basic ground rules that govern discrimination on that one network are the free speech rules of our future.

That's all I have to say.

MR. SNEAD: All right. Well done. That's good. I like the ending. I like how abrupt it was.

So, first of all, thank you to Ben and Jeff and to all the other contributors to this volume. It was a pleasure to work on this very important project. Just to have a

sort mini-community of learning with the folks that you assembled was a real treat for me.

My topic is to examine how a powerful argument that is rooted in advances in cognitive neuroscience as augmented by new forms of neuroimaging -- that is, techniques to image the structure and function of the brain -- arguments rooted in that context that are aimed at reshaping the criminal justice framework here in the United States and, more specifically, punishment in the United States, how that might look if those arguments are accepted and applied and integrated into our system of justice. And I think the best way to capture, first, what the arguments are and what the consequences will be if adopted and what the sort of outlines of my critique are is to take a look at a fanciful, although not entirely unlikely, hypothetical that begins my chapter in this volume.

So, imagine the following, and I'll describe part of it and I'll read part of it. Imagine a scene, a courtroom, jurors filing in, taking their seats in the midst of a capital criminal trial. It's been a long and emotionally draining couple of weeks. The guilt phase of the trial was mostly straightforward. There weren't really serious disputes about whether or not the defendant was legally guilty, was factually guilty, whether or not he possessed the sort of surprisingly low baselines for cognitive and volitional capacities that are necessary for guilt, the guilt phase of the trial.

These weren't difficult questions, and they were dispensed with fairly quickly. It was clear that he knew what he was doing and appreciated that it was wrongful, that he acted with malice of forethought, that he could understand the charges against him and assist in his own defense. That is a rough way of describing the baselines for capacity, competence, and so forth to satisfy the requisite requirement of *mens rea* at the guilt phase of the criminal trial.

The difficulty here for the jurors was the sentencing phase of the trial, the

capital trial. It was emotionally difficult, because it involved sort of accounts that were framed in excruciating detail regarding the crimes themselves, the murders themselves, in the prosecution's efforts to demonstrate that they were especially heinous, atrocious, and cruel, manifesting extreme depravity, which was a statutorily required aggravating factor that the prosecutor had to demonstrate in light of the facts of the murders themselves and the way in which they were committed. The prosecutor and the counsel for the defense spent a lot of time talking about the details of the defendant's life and character, which was also a very ugly story: his broken childhood, marked by unspeakable abuse and neglect; his years of drug and alcohol use; his spotty unemployment history; his history of using violence to impose his will on others.

And they even discussed the structure and function of his brain, complete with very large poster-sized color what looked to the jurors like photos but in fact were computer-generated images later projected onto a shape that looked like the human brain that showed diminished capacity in his prefrontal cortex, which, roughly described, is widely understood to be the seat of reasoning, self-restraint, and long-term planning and above-average activity in his limbic system. That is the more primitive part of his brain associated with fear and aggression. And relying on a raft of neuroimaging studies, the prosecutor argued that this pattern of activation and structural abnormalities in the defendant's brainwork consistent with "low arousal, poor fear conditioning, lack of conscience, and decision-making deficits that have been found to characterize antisocial psychopathic behavior."

And the prosecutor further argued that this was not a temporary condition and that there were no known therapeutic interventions that could ameliorate it. It was highly refractory of any such treatments. The prosecutor argued that taken together, if you synthesize this picture, what you get is the profile of an incorrigible

criminal who would certainly kill again if given a chance.

Now, the defense argued to the contrary, that the evidence did not point to any tangible future risk of violence.

And the judge went on to explain to the jurors that their task was to decide unanimously what punishment was fitting for the crime of conviction: - life without parole or the death penalty. And, among other things, the judge explained that before the death penalty -- and this is taken from concrete jury instructions that have been modified for purposes of this hypothetical -- before the death penalty can be considered, the State must prove at least one statutorily defined aggravating circumstance beyond a reasonable doubt and if the aggravating outweigh all of the mitigating factors. And he described “mitigating factors” as any fact or circumstance relating to the crime or the defendant’s state of mind or condition at the time of the crime or his character, background, or record that tends to suggest that a sentence other than death should be imposed.

The judge -- and I’m going to read this to you rather than summarize it -- the judge then looked up from the jury instructions and turned to the jury box, “Ladies and gentlemen, let me add a word of caution regarding your judgment about mitigating factors. Some of you may be tempted to ask yourselves was it really the defendant that did this, or was it his background or his brain? You might be tempted to ask yourselves what this defendant deserves in light of his character, biology, and circumstances. Some of you might even be tempted to argue to your fellow jurors that this man does not deserve the ultimate punishment in light of his diminished though non-excusing capacity to act responsibly borne out of a bad past and a bad brain. In other words, you might conclude that capital punishment is, in this case, disproportionate to the defendant’s moral culpability.”

And the judge's eyes narrowed and he leaned even further forward to the jury, "But, ladies and gentlemen, you must not ask such questions or entertain such ideas. The sole question before you as a matter of law is much narrower. The only question you are to answer is this one: Is this defendant likely to present a future danger to others or to society? You should treat every fact that suggests that he does present a future danger as an aggravating factor. Every factor that suggests the contrary is a mitigating factor. Matters of dessert, retributive justice, or proportionality in light of moral culpability are immaterial to your decision.

"Ladies and gentlemen, this is the year 2030. Cognitive neuroscientists have long shown that moral responsibility, brain-worthiness, and the like are unintelligible concepts that depend on an intuitive libertarian notion of free will that is undermined by science. Such notions are, in the words of two of the most influential early proponents of this new approach to punishment illusions generated by our cognitive architecture.

"We have integrated this insight into our criminal law. Punishment is not for meting out just desserts based on the fiction of moral responsibility. It is simply an instrument for promoting future social welfare. We impose punishment solely to prevent future crime. And this change has been for the better. As another pioneer of the revolution in punishment, himself an imminent cognitive neuroscientist from Stanford University, wisely wrote at the beginning of the 21st century, 'Although it may seem dehumanizing to medicalize people into being broken cars, it can still be vastly more humane in moralizing them into being sinners.'

"So, please, ladies and gentlemen of the jury, keep your eye on the ball and do not indulge any of the old and discredited notions about retributive justice."

And with that he dismissed the jury to begin their deliberations.

Now, obviously this is a fanciful hypothetical. But it is drawn from and

depends on concrete arguments that have been set forth by a very prominent array of neuroscientists, lawyers, philosophers, and social scientists in service of an argument that they're making that the heart of all of the draconian brutality of the criminal justice system, the system of punishment that we have, is due to an outmoded and in fact false conception of moral responsibility that leads people to try to punish people for what they deserve. Deserve, they argue, is a false notion. Cognitive neuroscience, they argue, has demonstrated that the structure and function of the brain -- the brain is a material object -- the structure and function of the brain produces thought produces behavior. And it's all dependent upon concrete and determined laws of physics and depending on past dates of the world. And therefore all behavior is determined. There is no such thing as free will. And it's illegitimate to build into our structures of government mechanisms, especially mechanisms that involve hurting other people through the form of punishment that depend on this false and outmoded idea. And so they would argue for the jettisoning of the idea of just desserts, moral responsibility.

Now, let me be clear, not all neuroscientists agree with this proposition by a long shot, and there are vexed debates about not only the interpretive and technical difficulties that attend neuroimaging and cognitive neuroscience about whether or not it's possible now or will it ever be possible to reach the point where we can, with certainty, make judgments about the truth or falsity of free will as a concept. So, I just want to be clear about that. And, moreover, there are deeper, sort of philosophical arguments about free will and what its entailments are that are important for this argument.

But my purpose here in this chapter is to take seriously the claims, to grant for the sake of argument the premises of the proponents of this view, and to try to game out where the argument leads. The normative proposition, the normative sort of engine of the argument is that we want to make the world a better place, a fairer place, a

more decent place for criminal defendants. And then in the mechanism of reaching that goal, the means of reaching that end are to jettison the concept of moral responsibility in the legal structures that depend on that outmoded concept.

And what I suggest by examining the consequences of this program, especially looking to the current structures of sentencing in America, especially capital sentencing, which really do depend on rich and textured kinds of ideas about human agency and free will and the like, what it would look like if we stripped away all those aspects of a capital sentencing framework, leaving only in place those that are consistent with the cognitive neuroscience project for punishment. And what I conclude is that we end up at a place that is very different from, I think, the aspirations of the architects of this project -- aspirations that I share. What I think results is once you strip away all principles of moral responsibility, especially in the capital sentencing context, you're effectively removing the last refuge of criminal defendants who have been judged factually and legally guilty, and all you leave in place are those mechanisms that are designed to predict and prevent future social harms. And those are most clearly embodied in the doctrines of mitigation and aggravation.

Mitigation is the stage of the trial where the defense says listen, yes, he did it. Yes, he could have done otherwise, but please be lenient, please go easy on this defendant because of some abnormality in his brain or some feature of his character or background that make it more difficult, although certainly not impossible, not in a legally excusing way, for him to conform his behavior to the legal standard. Please have mercy on my client, because he's laboring under a difficult burden, although one that doesn't excuse him from legal guilt. He doesn't deserve death. And I suggest any time you use the word "deserve," you wouldn't be able to use the word "deserve." There is no "deserve" in the vision of punishment that's set forth by this particular project that I've

articulated.

What's left is mechanisms most clearly embodied in the aggravating factor of future dangerousness of trying to identify and prevent future harms. And we've seen, and others have sketched out, a kind of account of the draconian features in our system right now that are entirely driven by this desire to prevent future harms without regard to matters of moral responsibility and personal dessert.

So, again, the aim of the chapter is not to challenge the premises of the argument, which I think one can challenge, but rather to take them seriously and to follow them to their conclusions. In the first instance, as a matter of principal, we like the direction that they take us in.

So, thank you very much.

MR. ROSEN: While you're miking, I'll ask the first question to the group and then we're eager for your questions as well.

I wanted to ask my colleagues how they would decide a hypothetical that is not a hypothetical because the Supreme Court is deciding it right now, namely, how they would decide the global positioning system case. It seems to me that not only is the case hugely consequential for the issues we're discussing in this book, but the question of whether the courts should take the lead in embracing a broad principal or whether they should expect other groups, like legislatures or technologists or administrative agencies, to solve the question is one that all of our contributors have wrestled with. So, here's the case, and many of you in the audience will be familiar with it as well.

The police in D.C. suspect a guy of being a drug dealer. They get a warrant to put a GPS device on the bottom of his car and track his movements 24/7 for a month. And based on that surveillance, they conclude he is indeed dealing drugs and they indict and convict him. He objects, because the warrant was invalid. It was

supposed to be only served within D.C., but in fact they tracked him in Maryland. It was supposed to have been served within 10 days; in fact, they turned it on 11 days later. So, for the purposes of the case, the justices have to assume that there was no warrant, and the Obama administration is taking the very aggressive position that we have no expectations of privacy in public and therefore it's perfectly permissible for the government to track all citizens 24/7 without a warrant.

There was a remarkable moment at the -- or argument in the case where Chief Justice John Roberts asked the government's lawyer precisely that question. He said is it the position of the government that the police could put secret GPS devices on the bottom of the cars of the justices of this court and track us 24/7? And when the lawyer said yes I think and hope that he may have lost the case.

But the lower courts have divided on this questions. Several courts have held, along with the Obama administration, that we have no expectation of privacy in public, and, therefore, 24/7 tracking is permissible. And indeed Tim Wu's former boss, Judge Posner, in a rather cursory opinion, embraced that position. However, some courts have disagreed. Of course in the neutral Brookings spirit, I'm not going to tell you what I think about this case, but let me just say --

MR. WITTES: Well, didn't you already tell us?

MR. ROSEN: Well, if I did -- I guess I did. Well, I'll just repeat it.

MR. SNEAD: He didn't say what his view of America --

MR. ROSEN: I just want to describe this as a visionary opinion on the other side.

Judge Douglas Ginsberg here on the U.S. Court of Appeals in D.C. said there's a huge difference between short-term and long-term surveillance. It's one thing for the police to track someone for a hundred miles using a beeper placed in a can of

ether in his trunk, as the court said was permissible a few years ago, but by contrast 24/7 surveillance can reveal so much more about us -- our associates, our movements, the magazines we read, and the people we hang out with -- that we do have an expectation of privacy in the whole of our movements.

So, my question to my colleagues is, you know, you're a justice on the Court, which position do you take: the no expectation of privacy position; the difference between short-term and long-term surveillance positions, which says that there is an expectation of privacy against ubiquitous surveillance; or, in the spirit of Goldilocks, somewhere in between?

Justice Scalia at the oral argument was focused on the fact that putting the GPS device on the bottom of the car without permission was a trespass. So, if the justices decided on those grounds, it would be consequential for this case but wouldn't tell us more about the constitutionality of Open Planet and so forth.

And in the course of your answers, not to be too irritatingly law professorish, I do hope you'll tell our audience and each other should we expect the courts to rule broadly to take the lead in protecting privacy in public, or are there other bodies? Tim, in your paper you say administrative agencies like the FCC are going to be more than the court. Ben, you talk about voluntary cooperation between citizens and law enforcement being more important than unilateral action by judges. And, Carter, you talk about lower court judges pragmatically not jettisoning common law doctrines to protect liberty.

So, Justice Wu, you're up first. What are you going to do in the GPS case?

MR. WU: That's a great question. I have -- well, I need to say something first of all, which is that my -- it's a little boring, but my opinions represent my

own and not the opinion of the federal government that I happen to work for right now.

MR. ROSEN: Thank you for that.

MR. WU: Yeah, I should have said it earlier, but, oh, well. It retroactively applies as well.

A few observations. You know, I think -- it's been a while since I've thought heavily -- I'm not a Fourth Amendment scholar, but the thing I felt about the Fourth Amendment and I continue to feel now is that in a nutshell it's too hard on cars. (Laughter)

In other words, you know, people spend a lot of time in cars, and there's a lot of protection for the home, but, you know, for a lot of people their cars -- some people can't afford a home, which is one thing, but for other people, you know, other people spend a lot of time in cars, and we are remarkably lacking in constitutional protection through cars, you know, for moving around. I think that's sort of a mistake.

You know, there's a strange thing in America. When you're in your home, you have all kinds of protections, both constitutional and legal. You can sort of shoot people. You don't have to retreat. The police can't come in without extensive warrants. All kinds of things. As soon as you leave your house and get in your car you become, you know, an open target. You're almost like a citizen in Yemen or something. I mean, you can't be hit by a drone, but it's close. (Laughter) You basically can be arrested for any offense. You can be pulled over. You can be searched. And the government wants to put GPS things on you. So, my opinion is along a more general feeling that cars should get more protection, get more constitutional rights in your car. I think it should be considered a search or a seizure -- or search I guess -- and give an expectation of privacy in your car.

But I would be remiss without adding that that's a relevant issue but not

the only relevant issue. Again, as I suggested in my talk about free speech, the whole game is about intermediaries. Why do the police care about putting a GPS thing on your car when they can pull it off your iPhone? I mean, your iPhone is storing where you've been over the last year. Pull up that record, you won't need to put a GPS under -- you don't have to find someone's car. You just call Verizon or AT&T or if, you know, AT&T bought T-Mobile there'd be even fewer intermediaries. You just deal with one of them and say, well, where's this guy over the last month? And the question is whether there's an expectation of privacy in that. So, I think the intermediary question is in some ways almost more important.

MR. ROSEN: Excellent. It's true about expectation of privacy in cars. The Texas attorney general has famously said that for many people sex ed and driver's ed take place in the same place. (Laughter) But this -- I focus on intermediaries as crucial, and Judge Kozinski in his really remarkable dissenting opinion on the Ninth Circuit said unless we act to do something right now, the police will be able, without any cause, to pull up our locational data from AT&T and T-Mobile. He said I grew up in Bucharest. I was the child of Holocaust survivors. 1984 has arrived. So, use you're right to call our -- do you want to answer the intermediary's question? What does the court do in thinking --?

MR. WU: I just want to point out that is the question, but I want to reiterate that point about cars. There's this tendency in American constitutional law to be too extreme on -- either too dramatically extreme. I mean, like I said, we have almost too much protection in our own homes. I think we shouldn't, but, you know, it's armored to the hilt. You can do anything you want. You can -- you're almost free from any kind of surveillance whatsoever. But, you know, as soon as you get in the car, you have fewer rights in the United States than you have in other countries.

I always feel like whenever I'm driving in the United States I am always feeling like there's some chance of being arrested, for some reason, and I think it's not -- it's unworthy of a country that calls itself free, the lack of freedoms we have in our cars.

As for the intermediary question, the question I pose -- if you can get the same information off people's phones, then GSP information -- you know, strapping the GPS thing to the car is not quite as important. And similarly, I guess, to be consistent I feel that it is very important that we have expectations of privacy and the information that carriers have -- the phone companies and, increasingly, the Internet intermediaries -- and one of the things I just want to point out is that there's been a pattern of consolidation in all these industries that has had an effect.

You know, we've sort of thought of the Internet as generally being a very open, very atomized industry, but when you look around there are not that many companies left these days. And so it's not only now just a question of the carriers; it's a question of the big three or four Internet companies, and the information they have. And this is how it ends up connecting to the issues of privacy -- Facebook, Google, investigations, and related questions. It all becomes of a piece, I'm suggesting. You know, basically, if Facebook knows where you are, that's enough; if Foursquare knows where you are, and so on.

MR. ROSEN: That's great, and indeed in an essay by Orin Kerr in this volume, Oran suggests that he agrees with you that there should be an expectation of privacy and data turned over to third parties questioning what courts have called a third party doctrine, which is if I make my locational information available to Verizon, I abandon all expectation that Verizon won't turn it over to the government. But Kerr's solution is use limitations. Rather than focusing on preventing Verizon from collecting the data, a statute could say Verizon can't share the data with law enforcement, for example, unless

there's evidence of a serious crime. If they just find evidence of a low-level crime like adultery, for example, then they can't share without some higher cause. So, that's a crucial question.

Justice Snead, I want to ask, were you thinking if you want to fancy up a hypo by asking whether the cops could brain scan you in your car as well, then that would be entertaining.

MR. SNEAD: Yeah, that would be entertaining, although the magnet might pull the car apart.

So, there are a couple of interesting things about this GPS case. First of all, I agree with Justice Wu that cars have really gotten the short end of the stick in terms of expectation of privacy doctrine. Although it's still true that -- and that's arguable. There's this sort of standing warrant exceptions for the automobile because of its pervasive regulation and its capacity to move quickly and so forth. But I think that there's an answer to this case in the extant jurisprudence of Fourth Amendment investigations that wouldn't require the justices to do anything radical. And in the sort of spirit of moderation I would say if you look at the previous cases, which turn on unmediated sense perception and the use of technology to transcend that as being the kind of marker between where there is no expectation of privacy versus where there is an expectation of privacy, they might provide an answer. So, the *Kelo* case, which you refer to that involved the placement of a beeper, which is kind of a more rudimentary tracking device, in a can of ether, the court said that the monitoring of that device was permissible. There was no expectation of privacy when you could visually identify where the car is and where it's moving by looking up. Now, you don't have to actually do that, but if you could do it, then that's a legitimate use of that technology.

However, when you're monitoring the location of the canister inside the

house and whether or not it moves -- and this is the house-car dichotomy that Justice Wu talked about -- once it's inside the house, if you're doing something, if you're engaging in surveillance that would not be possible absent a physical trespass without the use of this technology, then that gets to the heart of what the Fourth Amendment originally was meant to protect. Justice Scalia makes this argument in the *Karo* case involving thermal imaging of a house. You look at a house and catching the sort of heat coming off a house to draw inference about the presence of marijuana grow lights inside the house. Justice Scalia said look, if you're using technology to do something that you couldn't have previously done without physically entering the home, you are functionally entering the home and therefore that should be dealt with as a search that does in fact implicate both the object of and subject and expectations of privacy that define what a search is.

So, I think -- and the court could say we're going to just extend *Karo*, and not only that but *Florida v. Viola*, the case involving the helicopter going over semi-open enclosures involving growing marijuana. They say if you can look out of your plane, if the technology is in widespread use and you look out of your helicopter and you can see the marijuana growing, that's kind of like a plain view situation, there's no expectation of privacy. But if you're using something to amplify your sense perception, using technology to try to get at that information, now you've crossed over and this is a search. And it seems to me that you'd be well within the structures that are already in place with respect to the Fourth Amendment jurisprudence to say that the GPS monitoring, when you couldn't do so absent physical viewing, is itself a violation. And I think that that might be one way to address the concern itself.

MR. ROSEN: Interesting, now where does that leave Open Planet, so in five years let's imagine that it is in general use for people to sign on to Facebook and Google and track each other 24/7.

MR. SNEAD: This is a tricky question, and Justice Scalia in the *Kelo* case itself mentions the -- so the two prongs are is there unmediated sense perception, and how widespread is the technology in use. Justice Scalia says I'm not very happy about this widespread use proposition, because that makes the expectation of privacy grow and shrink, depending on the applications and widespread possession of different kinds of technology, which has a certain kind of logic to it, because if we're talking about expectations do I subjectively expect and is this the kind of expectation that the man on the street would agree to as a reasonable expectation of privacy.

There's a certain kind of logic to it, but I think Justice Scalia rightly -- and he says the reason I'm including this is because the question has not been called as to whether or not we should jettison that part of the test.

I think maybe we should think seriously about whether that should be jettisoned. I think unmediated sense perception and whether or not you're achieving an end that would originally not have been possible without a physical trespass is a useful framework.

And one further thing I would say is originally -- back in the old days, in the *Katts* case involving the listening, you know, outside of the telephone and then later on in the garbage case where they talk about if your -- and you mentioned this earlier, talked about putting off brain waves -- if I sort of release my possessory interest in something, then the police are free to take it and -- or a third-party user is free to convey it to someone, out to the cops if they want to, without implicating my expectation of privacy.

There was a very old debate about whether or not the object of expectation of privacy is simply a descriptive principle, that is, are people -- do you just go with what society expects in a kind of descriptive way, or is there a normative

component to it? That is, should we define the object of expectation of privacy by virtue of the kind of society that we want to live in as opposed to the kind that we do live in? Of course, people go through your trash, but do we want to build in to our jurisprudence that kind of, you know, weakness in human conduct?

So, we might call for a revivification of the normative dimension of the expectation of privacy argument.

MR. ROSEN: Justice Wittes, that's a very strong proposition. Should judges be in the business of deciding how much privacy people should expect? If so, what would the principle look like? Or is that just too high-handed, and would it be better to leave it up to things like the Geo-Locational Privacy Bill, which is now pending in Congress and sponsored by both Senator Ron Wyden, an Oregon Democrat, but also Josh Chaffetz, the Utah Republican? Our legislature is better equipped than judges to decide how much privacy people should expect.

MR. WITTES: Well, it's funny you mention that. (Laughter)

So, I want to actually start by saying that I think the point that Tim raises, which is the intermediary question, is actually the critical point, and it relates, as he alluded, very, very closely to the free speech issues that he was talking about earlier.

One of the things that -- you know, there is a very old principle in Fourth Amendment law that if you give data to a third party, that's outside of the ambit of protection. So, if I give you a bunch of records and the government subpoenas those records from you, that's it. They get it. There may be limitations on the scope of the subpoena, but they're not -- I don't have a Fourth Amendment interest in those third-party records.

Now, if you think about your cell phone, your cell phone is bleeping to a carrier a third-party record every few moments, and those records identify your location

with a fairly high degree of precision, and the later the phone, the model of the phone, and the more GPS enabled, you know, the more specific the location data that it's recording about you over time.

So, to put this in real terms and in contemporary terms, we're not talking about the year 2025 or 2030. I have a Brookings colleague who heard about this project and who mused, oh, yeah, I was just on a jury that got a bunch of geo-location data. And I said really? And he said yeah. And I could be mangling the details of this, so -- but the broad picture is right. He said yeah, I was on a jury in -- I'll keep the towns out of it -- one town in Virginia, and the defendant denied adamantly they had murdered somebody in a different town in Virginia. And the prosecution simply showed that at the relevant period of time his cell phone got into a car, drove to within, you know, 30, 40 feet of the house in which the murder took place, let him off -- you know, got out at the spot of the murder, hung out there for a short period of time overlapping with the time of the murder, got back in the car, and drove back to the first town.

Now, none of this is even arguably, under current doctrine, a matter without which the Fourth Amendment has very much to say. And so the first question, you know, as Jeff points out, is if the government attaches a GPS device to your car -- you know, that's yesterday's technology actually when you get right down to it. Today's technology is that you've attached the GPS device to your body, and all they have to do is call somebody up with a variety of instruments, legal instruments, that operate not on the basis of probable cause, they operate on the basis of relation -- your being relevant to a lawfully constituted investigation, either a criminal investigation or a national security investigation, or, you know, some other type of investigation. So, that's today's technology. And so my first point is that the problem is actually a little bit more acute than the GPS case in *Jones* suggests.

But my second point is that all that notwithstanding, I disagree with the other members of this panel about what the proper outcome in the case is. I think there is not an obviously, to my mind, judicially manageable standard to think about what, you know, how long do you have to surveil somebody's GPS data before it becomes a search when you could just follow them around 24/7 if you really cared about it. I think this stuff should be much more highly regulated than it is.

But I would like to see that evolution take place through a more legislative and less judicial process, and given the magnitude and pervasiveness of the third-party doctrine I don't think even if you say, in this case, this is a search, it still doesn't make the iPhone data a search, and it's much harder because of the third-party doctrine to get there with that. And I would just -- I would much rather see Congress take a serious look at this and say here is the degree of privacy that we think you're entitled to both from government and from your carrier, by the way. I mean, you know, I would much rather see that debate happen in the context of a deliberative legislative process over time, and so with all deference to the anxieties that lead people to want this to be judicialized, I actually don't.

And I would return just briefly to Jeff's point about what seems to have animated the chief justice in this conversation, which was the sudden realization in oral argument, if in fact it was sudden in oral argument, and that can be deceptive obviously, but that this could apply to him, right? And Dahlia Lithwick, the great Supreme Court commentator and comedienne -- she really is brilliantly funny -- once described an ACLU lawyer arguing in front of the Supreme Court and saying, you know, this is a slippery slope; if it could happen to my client, it can happen to you, it can happen to all of us. And then she paused. She says this doesn't seem to get a lot of traction with the justices perhaps because justices of the United States Supreme Court so rarely deal crack out of

their chambers. (Laughter)

And I think this actually -- the contrast between Dahlia's story, which is funny and deeply, deeply true, and what Jeff is describing with Chief Justice Roberts where, you know, this belief that the police could simply slap something on, you know, a justice's car and watch them forever, I think that anxiety, that difference is probably not valid as a matter of constitutional principal, but it is valid as a matter of, you know, can you muster the kind of political coalition that it should take to think seriously about what kind of regulation you want in this space. And so I would say be patient, and I dissent.

MR. WU: Jeff, can I ask you a quick question?

MR. ROSEN: Sure.

MR. WU: I take the point about the intermediary institutions being the real ballgame going forward, but I would ask my colleagues do you think that it is worth continuing to consider the difference between state action and the action of third intermediaries? Because to my mind, that's a significant difference. The idea of -- and maybe there will be no need to do it in the future, but there seems to me a difference and certainly in the current jurisprudence there's a difference between the government putting something on your car versus asking a third party to provide information.

MR. ROSEN: You're absolutely --

MR. WU: Well, what's the difference? I mean, I know there's a constitutional difference, but what's the difference to you?

MR. WITTES: Yeah --

MR. WU: Probably getting it off the carrier is more effective, right? I mean --

MR. WITTES: Well, it seems to me --

MR. WU: What's the difference in your privacy -- as a human being,

what's the difference?

MR. WITTES: Yeah, well, I mean I -- it's so difficult to disentangle --

MR. WU: As opposed to a lawyer I guess.

MR. WITTES: Right, right. It's difficult to disentangle the kind of -- to get outside of the doctrine itself and criticize it, right? So, you could say on sort of a -- I mean, to the individual, I mean, you think of the case involved and the sort of gross facts of the *Greenwood* case involving the garbage, right?

So, the question is do you give your garbage -- put it out, give it to the garbage man, and then the garbage guy gives it to the cops, right? So, it strikes me that -- and the question is: Is there reasonable expectation of privacy once you've conveyed that property to the third party. It seems to me your possessory interest seems like a different dimension of the calculus whether you still have a continuing interest in that information and also you have the agency of the third party itself in its decision to keep or convey the information to the government. It seems to me that the more attenuated relationship seems relevant in that respect.

MR. WU: Right, and I think the theory is we're more afraid of the government, because there's a monopoly on force and, you know, they have these people called police who put things on their machine, while in theory if you don't like your cell phone company or your -- or even Apple carrying information. Supposedly you can move to somebody else.

My question is when you have increasing consolidation, how realistic is that model? You know, I mean, we can sort of switch, but there's not a lot of variation in the oligopoly between -- in privacy policy. So, it hasn't -- to my mind, the difference is supposed to be based on a market -- the difference between a market and the state, but --

MR. WITTES: Well, the difference -- but I think there's another force that pushes against the difference, and here I'm arguing against my proposed outcome, but, I mean, other difference is just a pervasiveness in the amount of data that we put in the hands of third parties, right?

MR. WU: Yeah.

MR. WITTES: You know, if your -- if the third-party doctrine is I've entrusted a box of stuff to Jeff, right, and the government issues a subpoena for Jeff to turn over that box of stuff, that's a very manageable privacy problem from my point of view, because I just have this decision to make: Do I trust Jeff to be the custodian of my stuff? Do I -- what kind of records do I store in a bank vault? What sort of records do I keep in my own house where, as Tim points out, the Fourth Amendment is strongest?

You know, the more my data that I have no perception of having turned over to anybody is itself covered by the third-party doctrine, the more pressure that puts on that sort of basic philosophical underpinning of it, and I think it is ripe for a really hard conceptual look, and I just don't really want that conceptual look to be done by the Supreme Court.

MR. WU: Here's a question -- and, I don't know, this isn't my area of expertise, so I may be missing obvious, but the government, even if the government wants to compel a third party to hand over information against its wishes and obviously certain third-party intermediaries are going to want to have the reputation of telling the government no when its customers' privacy is at stake, but put that to the side for a moment, the government still wants to compel that information, it still has to have probable cause and a warrant, right? In the same way they have to have probably cause and a warrant to compel that information from you directly.

MR. ROSEN: The question is what is the data?

MR. WU: If they're unwilling to do it, they can't write it. If they're unwilling to do it, they can't -- they have -- I mean, I'm thinking of *Stamford v. Daily* case, right, where the question was do you have to have probable cause and a warrant to compel this newspaper to hand over the photos of the demonstration that implicated some third party who wasn't -- whose interests weren't at stake.

MR. ROSEN: And the answer there was no, because it was held that we don't have expectation of privacy in the photos held by the newspaper. And when the Court in the 1970s said that when I turn over information to the bank, the bank can turn it over to the government without any standard of cause, there was a rebellion, because people disagreed. They didn't think that the bank was going to be turning over their financial information to the government, and Congress passed a law -- the bank privacy law -- that requires a higher standard, a warrant of probable cause.

Let me try to sum up this extremely illuminating discussion, which very much mirrors the kind of debate you find in the book.

So, we have Justice Alito over here, actually -- (Laughter) -- who says although he believes that the future of this question will be determined by the choices of the technology companies, and in particular simple questions like how long are they going to store the GPS data or the cell phone data, that technological question made by the intermediaries -- he thinks, well, how far more influence over the future of privacy than anything the Supreme Court does. Nevertheless he thinks because this is a contested question it should be left to Congress. He's optimistic about the existence of a bipartisan consensus, and he hopes that Congress will act without the Court stepping in.

Justice -- well, maybe not quite Justice Brennan but maybe Justice Harlan thinks that judges do have a role in deciding how much privacy people should expect, and unless the Supreme Court in this case sets down a rule saying that when it

comes to technologically enhanced surveillance that the naked eye could not do without hiring a thousand police officers to track you 24/7 for a month, it's important that that be viewed as illegal.

And Justice -- I don't know if you're Justice Breyer or -- I hope you'll be Justice Kagan, because she's really increasingly interested in these intermediary questions -- really sees this case as an interplay between these other two visions. On the one hand, protect privacy in cars. It's wrong and doesn't coincide with our intuitions to not protect it to some degree but you think it's really an interrelation between the judicial doctrine and the administrative doctrine will be crucial in your challenge to Brown over here that what in practice is the difference between the government doing it and the intermediary doing it is at the core of your paper here, too.

I'm just going to adopt the position of my hero, Justice Louis Brandeis, who in many ways is the patron saint of this entire project. Brandeis, in addition to writing the greatest article on privacy ever written in 1890, also was impatient in the 1920s when the Court evaluating wiretapping for the first time refused to protect as much privacy in the 20th century as citizens took for granted in the 18th. He said you used to have to break into someone's desk drawers to invade their privacy. Suddenly, by eavesdropping on telephone wires without breaking into the office of the suspected bootlegger, Brandeis said, you can invade the privacy of people on both ends of the conversation.

And then on this incredible passage, which looks forward to the age of cyberspace, Brandeis said ways may someday be developed by which it's possible without invading the privacy of the home to extract secret papers from desk drawers and introduce them in court -- a far lesser invasion than was unreasonable at the time of the framing. We need to translate constitutional values into the 20th and 21st centuries. So, with Brandeis as my model, I hope the Court recognizes the complexity of these issues

and does protect us against ubiquitous surveillance but also realizes that they will not have the last word on the subject and that intermediaries will be crucial as well.

Ladies and gentleman, we --

MR. WITTES: So, let's go take some questions from the audience. Please wait for the mike to come around, and say who you are and what organization you represent.

Please.

MR. ALTMAN: Hi, I'm Fred Altman. I'm just -- and my question is could you around some of this problem by requiring all the people who gather this third-party data to have a way of allowing you to shut it off so that your cell phone does not -- when you don't want to use it, it doesn't necessarily provide location data? I mean, you could generalize that to other situations, and it might get around some of these problems.

MR. WU: Yeah. That's a great question, and it's really a job for our agency. I work Federal Trade Commission, and this is what I'm trying to suggest, as a lot of these are also questions of privacy, and I want to actually take up something that Benjamin was talking about, which is he wants a legislative solution, not a traditional solution, but there's actually another option, which is the -- and I think what's actually happening is agencies are starting to solve these problems. And so Europeans have this idea. It's not popular in America yet. But they have the idea that you should have the right to be forgotten, that they want to require it, but maybe we could sort of encourage it in this country, which is to say, you know, an easy off -- like sort of what you're suggesting. They want -- and I think this point's quite interesting, the idea that, you know, like on Facebook, I'm done with it. You know, it's fun for a while but got embarrassing or something weird happened or my children or my teachers -- so, I'd say I'm wandering off. When I'm off I want to really be off and, like, not be kind of lingering around but gone.

So, why not a right to be forgotten button. It's a little bit what you're talking. Maybe you should have more -- it would be great to have more privacy by design is another big phrase in this area -- the right to switch off when data is being collected from you. And I think that would be an important development.

How does it happen? Well, the companies have to do it. They don't want to do it, because -- see, the model -- the reason not to do it is advertising. So, when I add to this, it's the -- the business model mostly is companies that are based on advertising, and so the reason they want to collect the data is for advertising purposes. So, there's a weird confluence, and I think nobody deeply understands these factors completely between privacy, advertising interests, the fact that consumers don't want to pay for things, and then search and seizure law -- all kind of bundled together in a way that's very difficult to understand and I think fundamentally goes to this central question of intermediaries and third parties.

And I guess I'll say there are third parties and there are third parties. There's me, you know, leaving, like you said, a box of documents with my friend and then him turning over to the police or leaving on the side of the street; and then there's, you know, monopolies or near monopolies where one feels they have to be a member of to communicate or be a member of society; and there have always been some intermediaries which are just a little different.

You know, it's very difficult to function today without using the Internet. You can try. You can be -- you have a choice now. This is something, believe it or not, the Unabomber said, which is you can only have two choices. You have to be completely connected today and surrender almost all your privacy, or you have to live in a little hut. And we've gotten to the point where you don't have sort of an intermediate choice. You have to be kind of completely unplugged --

MR. WITTES: Google Earth can still see your hut. (Laughter)

MR. ROSEN: Google Earth can still see your hut.

MR. WU: That's why he moved to the hut.

You know, there was no, like, one way in and that's sort of a problem. I think it's what you alluded to. A lot of people want it to be part way. They don't want to be fully exposed, but it's very difficult to be a member of society.

MR. ROSEN: Just on the right to forgotten, yeah.

MR. WITTES: To be forgotten if I may.

MR. ROSEN: And then of course the Unabomber's effort to be forgotten where -- especially toward -- the hut is now in the museum. I saw it last weekend with my kids.

The problem with the right to be forgotten -- it makes sense if it limits collection. So, Verizon and iPhones can't collect my locational data or have to destroy it. But when it regulates use, it really questions free speech.

So, there was a fascinating case in Argentina recently where a pop star who'd posed for racy pictures of herself, which got out on the Internet, became embarrassed and wanted to take them down, and she sued Google and Yahoo. And an Argentinean judge agreed that these pictures violated her dignitary right, her right to be forgotten, and ordered Google and Yahoo to take them down. They said we can't. The judge said yes, you can, we're going to fine you $50,000 a week. Yahoo said okay, but it's too hard just to remove the racy pictures, we're going to remove all pictures of this woman and all references to her on the Yahoo search engine. So, now if you plug in her name, you get nothing.

So, that's a real selective deletion of history, which I think the American -- now the tradition doesn't count then.

The details of how this writer to be enforced are also fuzzy. I debated the French privacy commissioner who proposed this right -- *le droit à l'oubli*, the right to oblivion -- which, by the way is straight out of *Star Trek*. It's completely French. (Laughter) And I said how are you going to enforce it? And he said, well, we'll create, I don't know, an international commission of forgetfulness. (Laughter) We'll sort of decide on a case-by-case basis what comes up or what comes down.

So how it's going to be enforced is tough, but Tim's comment suggests we're about to see a titanic battle in norms between Europe and America with the Europeans trying to enforce this right, the Americans resisting it, how this plays out technologically and in the courts --

MR. WITTES: I also think -- just before we get to Charlie Dunlap I just want to follow up on one other thing that Tim said, which was, you know, this idea that, you know, people want to be partway in and have -- you know, they don't want to be off the grid, but they also don't want the costs of pervasive surveillance. And, you know, I am entirely sympathetic to that, but part of me also wonders whether, for a lot of those people, they're asking for the benefits of a transaction without the costs of it and that, you know, when you ask for all the convenience associated with littering the world with your data and to be relieved of all of the costs and risks associated with that, there may be something unreasonable in the consumer demand in its very essence there, and it may be that part of the answer is that we shouldn't be acquiring the degree of individual dependency that we all are on things that require us to give away sensitive data about ourselves.

MR. WU: That's right.

MR. WITTES: Charlie?

MR. DUNLAP: Just to follow up. Charlie Dunlap from Duke Law School.

Superb panel. Could not be a more important subject, and I'm very anxious to read the book.

Two questions. One, the permutation on the discussion so far, what about the rise of masking technologies? I think that there are going to be technologies, and unlike a speeding detector, it isn't per se trying to mask illegal behavior but just ensure privacy. How do you think government's going to react?

And then another thing, I sort of see anecdotally among students and younger people, they seem less concerned about privacy than maybe somebody of my generation. And do you think in the future that the whole notion of privacy and the value of privacy, the normal change in -- because they don't -- they sort of think the government's looking at whatever's on the web, and they seem relatively untroubled with it. I'm generalizing. I'm speaking anecdotally. But I would be interested in your views.

MR. ROSEN: On the second question, because I do write about this a bit in the chapter, no, I don't agree with those who say privacy is over, get over it.

It's true polls suggest that young people are less concerned about some aspects of privacy than older people. For example, they're less upset about being naked at airports, because they look much better than the rest of us. (Laughter) However, when it comes to Facebook they're really concerned, and when they're applying for jobs, they're getting smart about selectively deleting bits of their past and they feel angered and invaded when they're fired or not hired because of Facebook pictures taken out of context. And their expectations change as they get older, obviously, too, so there's a lot of granular research on this. Danah Boyd at Microsoft is doing it. But it's just too simple to say the problem is going to go away, because in the future we'll all live in glass houses.

On masking technologies, there are interesting possibilities. There's a

suse balance movement that is suggesting that people literally wear masks in public. In Europe more granularly you can petition Street View right now. There were some college students who were photographed sunbathing in California, and they wanted to remove their images, and Facebook will remove individual still shots, but that's obviously not an effective solution to the whole problem.

I wonder -- you wonder at the future of this masking technology. Imagine how European anti-veiling laws might be challenged in light of these new efforts to conceal yourself. You're not allowed to cover your face in public in Europe because of the French concern about religious supremacism, but that would clash with this privacy implication.

Broadly, it's true that for every new technology there's a response, so you can scrub your hard drives and act like a privacy paranoid and browse anonymously and so forth. It will be harder as the surveillance goes mobile and as the option not to have a mobile device would be like the Unabomber going out into the woods. So, it's promising, and it'll go back and forth, but ultimately I think it's not going to solve the problem. We're going to have to return to the choices of intermediaries about collecting the data to begin with.

MR. WU: The thing you didn't mention of the mobile is the move of most things to being cloud applications, which, once again, turns everything into an intermediary question, which is kind of the -- you know, if there are masking technologies, if they're all one company, it goes back to the all these sort of Teddy Roosevelt questions. Let's say everybody's relying as almost -- okay, who in this room doesn't use Google, let's just say? Okay, so there we are. Oh, there's one. (Laughter)

So, then a lot of the questions -- I mean, use Google docs, Gmail, so forth. The masking technologies all turn into a question of what is Google doing. And

then the question becomes well, what are the advertising interests involved? What can the government compel Google to do? It's the same intermediary question that we keep going back to.

I want to -- I don't know if this is a juncture, but I want to try taking this deeper to say what we're really talking about here, because I think we're talking something interesting, but we're talking about something different than we realize. And I want to try to make it a 20/30 thing --

MR. WITTES: Please.

MR. WU: -- which is to say that in some ways, even though it seems like a science fiction hypothetical where the very beginnings of sort of understanding -- and I hesitate to use this word but I'll say it anyway -- cyborg law, that is to say the law of augmented humans. And the reason I say that is that, you know, in all these science fiction stories, there's always this thing that bolts into somebody's head or you become half robot or you have a really strong arm that can throw boulders or something, but what is the difference between that and having a phone with you -- sorry, a computer with you all the time that is tracking where you are, which you're using for storing all of your personal information, your memories, your friends, your communications, that knows where you are and does all kinds of powerful things and speaks different languages? I mean, with our phones we are actually technologically enhanced creatures, and those technological enhancements, which we have basically attached to our bodies, also make us vulnerable to more government supervision, privacy invasions, and so on and so forth. And so what we're doing now is taking the very first, very confusing steps in what is actually a law of cyborgs as opposed to human law, which is what we've been used to. And what we're confused about is that this cyborg thing, you know, the part of us that's not human, non-organic, has no rights. But we as humans have rights, but the divide is

becoming very small. I mean, it's on your body at all times.

MR. WITTES: So, I think this point is very profound. It interacts with some work that I've been doing related to robotics, and, you know, there's now a drone that you can buy for your iPhone, and so this gives, like, very tangible expression to what Tim is talking about. You can go -- you can look it up on iPhonedrone.com, and you'll find that, you know, it's a little -- it's a toy, but you can take basically a robot and control it. It flies around and, you know, sends missiles at your friends and things -- at your friends' drones, that is, from your iPhone. And that of course raises the question if you can do it with a toy, you can do it with a real thing, right? I mean, you know, I'm not suggesting that we're all going to have predators on our drones, but that's sort of -- on our iPhones -- but that sort of expansion of one's individual capability is a very kinetic expression of what Tim is describing. And I think it is clearly right that over time we're developing law about and norms about where your rights extend to the technology that expands your individual capability in some sense.

Other questions? We have one -- Stephan? And then the gentleman in the front.

STEPHAN: So, just to make it a little bit more balanced to a certain extent, because obviously privacy is crucial, and I think it's a secondary use problem as well, because anyway that's how hard it is to actually deal with the collection as well. But to make it a little bit more balanced and also complicated is the whole question of big data to add to the debate, which is that, guess what, we have now huge volumes of data. And guess what, as a result we can actually produce new insights by having this data and having statistical analytics provide inferences, anyway, all kinds of predictions and all kinds of new insights that are relevant for science, for public policy, policy drivers, and so on. And in order to do so, you need to have the data made available, all right? So,

locking it in and closing it down actually undermines the whole concept of big data. So, how do you factor that in that narrative, especially when you have -- anyway, like, for instance in Europe, yesterday there was an announcement, “Let’s turn government data into gold.” Anyway, they initially said euros, but they changed that. (Laughter) And so, how do they move into those kinds of value statements if privacy is being seen as actually the barrier. And so that will become a complicated debate, and I just want to add that.

MR. WITTES: This is a very, very important point. So, Google a couple of years ago, a few years ago, did an incredible project, which they used flu as the sort of template, but I think the broad point of it is probably extendable to a lot of other areas of life, and what they did is they took CDSC data related to flu incidents -- initially I think in certain parts of the United States but then basically around the world -- and they looked at the question of when people start experiencing flu symptoms what Google terms do they search? And then they took -- so it turns out that this basket of terms -- about 50 terms that involved things like headache, runny nose, you know, sort of symptom-y kind of terms -- spike about a week or two before flu starts showing up visibly in CDC data.

And so what they did is they started tracking those terms, and what you would see was the -- I mean the curves run like this. You know, Google is sort of two weeks ahead of the CDC on both the upticks and downticks and it resulted in this incredible paper written by a group of Google people and a group of CDC people that basically says that you can use Google anonymized search data to point out the spots that you’re going to have flu problems in, in the next couple of weeks.

Now, a group of people in Google went a bit further than this in certain other areas and wrote this also just amazing paper called “Predicting the Present,” which was an effort to describe, again using very, very large and -- datasets so that the -- like,

it's everybody's search data, right, basically looking at economic trends. And what they show is that, you know, you can actually do that.

You can see all kinds of incredible things in this awesome collection of data, which essentially amounts to a body of data about what all of us are thinking about in any given moment, because the first thing we do is we go search -- and this has incredibly powerful, positive applications as well as all of the anxieties it may produce about, you know, privacy and other things. And I think one of the things we're going to have to talk about as a society is whether we -- what role we want aggregated and individualized and non-individualized data to be playing, and there is some sense in which Stephan says you're going to take the good with the bad or take the bad with the good.

MR. SNEAD: I have a question. Again, like I said, this is not something that I think about as part of my research, but one thing that worries me as we talk about this -- and using things -- search terms as proxies for incidents of flu or at least concern about flu, right? You could imagine people -- what it would show is where people are more neurotic about flu as --

MR. ROSEN: Well, it correlates incredibly, precisely --

MR. SNEAD: The deeper thing that worries me, and this picks up on what Tim's comment was earlier, is that I don't know if this is true but my intuition is that there are large segments of the American and global population that are not using these technologies because of poverty or because of -- you know, I keep thinking of the book, *Things White People Like*. It's a listing, among them, you know, Google Plus, all the -- and worries insofar as we take these as proxies for socially useful or matters of social concern, that there are going to be at the very least big lags in the sort of impoverished and less technologically savvy communities. I'm thinking about Appalachia or the inner

city and would that push in favor of -- and this connects with what Tim was saying -- a kind of right to technology so that you can be part of the community itself. That is, if I don't live in a part of the world where I have a mobile phone or a computer or access to the Internet, I'm effectively disenfranchised from the community of human concern, and should that be remedied or -- this seems like a serious problem.

MR. ROSEN: There was an interesting op-ed in the *Times* recently by Susan Crawford suggesting a digital divide when it comes to technology use. And she said one solution is spectrum policies. So, right to Tim's point, the Federal Communications Commission is trying to repurpose a spectrum in order to extend its uses into underserved areas, and that would be one solution.

But the broad big data that -- don't keep your fingers crossed because of financial opposition based on the lobbying, which again suggests that those considerations rather than courts may determine the question.

Ben suggests good uses. Broad -- I'm looking at economic data and flu to predict the future. But Google doesn't just want to predict flu's and economic future to be altruistic; its wants to predict what I will think. So, that's what Eric Schmidt said in a conference in 2006. Our real goal is to tell you what you should be doing before you even know it or to be able to answer questions like where should I go to college? And the reason Google wants to answers those questions is not just because it's cool -- because they want to sell ads to me not only online but online mobile devices and, increasingly, in real spaces and tailor and target the ads based on what I've done in the past and what it thinks I'll do in the future.

This obviously raises privacy concerns, because when the government knows what I'm going to be doing next before I do, there are consequences that follow.

One solution to this, Stephan, I think is on Kerr's notion. The Germans

have grasped this. They give the government broad access to big data for prosecuting serious crimes, but the intelligence services are not allowed to share that information with the police when it comes to low-level crimes because of a concern about misuse.

There's one other model that's worth noting. In his fascinating epilog to this book, Larry Lessig of Harvard says the next problem is going to be the next attack. So, when the next attack comes, all of our carefully constructed technological and legal protections for privacy will go out the window, because the government will say we need to track everyone 24/7. In order to avoid that Chernobyl, Lessig said, we have to basically tie ourselves to the mast in times of calm and build into the Internet an identity layer, so that, yes, when the government presents cause that someone is a suspected terrorist, then they can unmask them using this identity layer, but without the proper cause they can't.

That mirrors a decision that some intermediaries, like the company Palantir, have made. They will engage in very granular data mining when they have individualized suspicion of wrong doing, but they won't engage in predictive data mining, because they're concerned about the consequences.

On the other hand, Lessig's solution shows great faith in the ability of legal process to ensure that the system is used only for serious crimes and not low-level crimes. If you're less optimistic about that, you might not want to build in the identify layer.

MR. WITTES: Gentleman in the front has a question.

We have time for a couple more questions, so flag me if you --

MR. PATTERSON: My name is Brad Patterson. I served 14 years on the White House staff and 12 years at Brookings. And the subject of our panel is the Constitution and technology, and I have a question from the language of the Constitution.

The issue is presidential disability. We're in 2030, and the Vice President and a majority of the cabinet have just declared in writing that the President can no longer discharge the powers and duties of his office. And the President, in writing, has informed the Congress no, I can discharge the powers and duties of my office. The issue, again, goes to the Congress, and within 21 days they have to decide whether the President can discharge the powers and duties of his office. And it's 2030, and what the panel knows or can guess about the technology, medical, and what may well be questions of mental illness, where are we? What kind of technology can the Congress consider to help answer the question? They have 21 days to answer it.

MR. WITTES: It's a great question. So of course by then the President will be, as Tim described, a cyborg. (Laughter) And so --

MR. WU: So, you just look at his Facebook page.

MR. WITTES: I would think the thing to do would simply be to remove the relevant item, send it back to Apple, and they'll fix it. (Laughter)

No, I actually -- so, in all seriousness, I actually think that that's just listening to you read that and describe that provision. I actually think that's one of the provisions that I wouldn't intuitively say is going to have a great deal of technological stress. I could be wrong about that, you know, but it's -- the jobs of the -- the demands of the presidents here are extraordinarily taxing, and I doubt very much that we're going to come to a point where, you know, somebody can be kept functional for purposes of the President within the judgment of the Congress of the United States through some technological means. And if we do, I actually do have faith that the political structures will accommodate that reality in one way or another. Could be wrong about that, but I'm not so worried about presidential succession and capacitation as an area that's profoundly different today than it will be 30 years from now. My colleagues may disagree with me.

MR. ROSEN: On the other hand, if Carter is right and everyone is brain scanned, we may have a vision of a normal brain, and the President might be brain scanned and we find that he has an overactive amygdale leading to low-impulse control because his pre-frontal cortex isn't restraining his emotions well enough, and based on his failure to meet the standard, he could be viewed as disabled in the same way that criminal -- that potential wrongdoers could be locked up indefinitely because of their predisposition --

MR. SNEAD: Oh, if you took scans of everybody in Congress' brain, I think we might have to have a lot more disability. (Laughter)

MR. WU: Yeah, we want sociopathy identified.

MR. WITTES: On an -- I mean, on an entirely serious note, I mean, as those technologies get better and better at predicting aspects of behavior, I could see them playing a conceivable role in campaigns.

MR. SNEAD: Yeah, you could imagine Mitt Romney saying look at my brain, it's so much more controlled than Newt Gingrich's brain, because his amygdale is so active. (Laughter)

MR. ROSEN: Pretty pictures.

MR. WITTES: We have time for one more question if ---- yes, the gentleman --

MR. DI PIAZZA: Hi, my name is Fabre di Piazza. I'm wondering the extent to which this may be an anthropological question. Are these -- do you think technology is posing fundamentally historically new problems to which we require categorically new answers? Or do you think that -- it seems like all of you, to some extent, have some faith in the existing jurisprudence and the existing institutions of the Constitution to resolve these issues.

MR. WITTES: It's the ultimate question of the book, of course, and it's a very fitting one on which to end. So I think if I can I'll just start briefly and then have each of my co-panelists give their thoughts and then we'll close.

So, I think there has always been a responsiveness on the part of the governance structure that the Constitution creates to new technologies. We've had to address them before either within the Constitution itself or, you know, through its governance processes. So, the most famous one in the Constitution itself is the Second Amendment, right, where, you know, cheap, available gunsmithing allowed in the late 18th century firearms to be in the hands of, you know, every non-impoverished person who wanted one. And the response of the founders to that was so enthusiastic that they saw it -- what everyone thinks of the original understanding of the Second Amendment -- they saw it as in some version something that warranted affirmative constitutional protection. The Constitution has, you know, the patent and clauses, you know, that are essentially about cultivating the development of technology, right, and ideas.

On the other hand, you know, think about the mid-20th century when we developed nuclear technology, and the government's response to that is not too write a constitutional amendment that says yippee, we've got nuclear technology, everyone's got a right to it. In fact, just to say that is to giggle a little bit. It was to make sure that everybody who knew anything about the subject, worked for the government, was responsible for keeping secrets. And we actually managed to keep incredible nuclear secrets for very, very long periods of time. And so the responses differ really quite radically, depending on cultural environment, the technology in question.

One thing that has tended to happen in my view is that it always feels like the challenge that a new technology poses is more radical than it later turns out to be, and this book has that risk. My chapter may be the most at risk of that, although I

look at the environment in the life sciences and security and I find it alarming, and I don't know how we adapt to it. But the fact that I don't know how we adapt to it doesn't mean that we don't adapt to it. It doesn't -- you know, the limits of my imagination are, you know, undoubtedly a rounding error on the scope of human capacity, and so, you know, all you can do is -- I have a certain anxiety. I also have a lot of faith, to answer your question, and I do think that we're pretty good at adapting the Constitution over time through a variety of means, and I hope and expect we will continue to do so.

MR. ROSEN: Carter.

MR. SNEAD: Yeah, I was -- sorry. Yeah, I think you're right to -- and Tim had raised this earlier about -- this is what we're really talking about is more anthropology and like what we are and who we are, and these are -- and I think that at some point what we do and what we can do merges with who we are, and I think that was in some ways behind what Tim was saying. And I'll confine my remarks to the cognitive neuroscience.

I'm not sure -- well, there are two points here. First is if it's true -- and it's a big "if," and I'm actually not confident that it is true -- if it's true what the proponents of the cognitive neuroscience projects say about us, not just what we can do but who we are -- that is, we don't have free will, and that's a very ancient question, free will versus autonomy, autonomy versus determinism, and so on -- but what's new about that, it strikes me in going to the core of who we are and not so much what we can do in a first-order question -- if it's true, then I think that radically alters not just the law but every aspect of human life. And it does represent a radical challenge to our moral anthropology and as it animates everything that we do.

But I will say, I mean, so that's a big radical claim, but then this sort of side constraint on that is I actually don't think -- I think that the claims that are being

made by the cognitive neuroscientists who are promoting it -- and their sympathetic lawyers, social scientists, and philosophers who are with them -- are in fact not demonstrations of the fact that we don't have free will but rather extensions of axioms in modern science about materialism and the process of reduction that -- so, it's more of a postulate than a proof. And I think that until there's a proof -- and I don't think there will be and I don't think there can be -- then our moral anthropology will remain roughly what it is.

MR. WU: All right. Well, I'll take the bait, and I think yes, and if you hear my essay I think there is a pretty serious problem with the Constitution and it's current approach to things that -- not so much a technological problem, but technology is making it more obvious.

The Constitution -- I think the basic idea of the Constitution is that concentrated power is a very dangerous thing. But the kind of original template, based on the experience of Britain, was the idea that the only really serious concentrated power is that of the state, that the thing we had to worry about was King George, and basically we had relatively weak individuals and an all-powerful government and the individuals needed some protection against an all-powerful government. And in order to prevent the same thing being replicated, we had the Bill of Rights, and in order to kind of avoid the problems of an all-powerful, centralized government, we tried separation of powers and federalisms. So we divided power in various places and that's the scheme and that's what we're all talking about. But I think since that time the problem is a lot of the power in American society has become privatized -- a lot of the most dangerous, I think, sources of concentrated power in private hands -- and the Constitution really doesn't have a lot to say about that, and it's kind of a weak spot. I think almost all of our conversations come back with saying yes, but it's all about what a power intermediary is going to do. And

right now, and it's been the American tradition to more or less depend on the ethics of private institutions to take care of us, which is okay, but I think the American approach towards -- wariness towards centralized power maybe needs to be extended further.

I say that also because of the concentrated sins of private power can infect the constitutional system, and this is the problem of -- you know, the influence of money and Congress is that in some ways that level of concentration of power infects the rest of the constitutional design. So, yes, I think that there's a problem in the fact that almost every question came back to the central question as well. It all depends -- what the good graces of a private intermediary thinks shows that we have a problem with liberties in this country.

MR. ROSEN: I'd like to echo Tim's comments, because they very much coincide to the spirit of the patron saint of *Constitution 3.0*, Louis Brandeis. In addition to being the greatest purist of the need to translate privacy in light of new technologies, Brandeis was also the greatest thinker in the 20th century who warned of the dangers of concentrated power. He talked about the risks that greedy banks take with other people's money. He talked about the curse of bigness and the need to break up the banks so that they couldn't take these risks in a way that would cause financial depression. He was the patron saint of laws like Glass-Steagall, which separated commercial and investment banking, which maintained financial stability until it was dismantled in the 1990s.

And in each of the questions that we've been discussing, I asked the simple question, WWBD, what would Brandeis do? And I think I could well imagine him taking up any of the questions we talked about, recognizing the complex interplay of judicial doctrine of regulation and of technological choices by private intermediaries. And he could sketch out a solution that would in fact preserve constitutional values in a way

that would vindicate Ben's optimism.

The problem is that there may not be a political constituency for the sort of trust-busting regulation of private power that Brandeis recognized was necessary. Despite the flashing of the Occupy Wall Street movement and the new "We are the 99 percent" slogan, Americans at least in their legislation have traditionally been reluctant to regulate the private sector and more willing to regulate the state. Europe is the opposite, which is why there are much more comprehensive European privacy laws and less restrictions on European state information gathering.

But I fear that we may be facing a situation where there is a complicated solution to all of these problems, much of it involving regulation of the intermediaries but the lack of political will actually to adopt it.

But I had to close by ending on a spirit of optimism in spite of my doubts, and I just want to remember Brandeis' galvanizing injunction, if we will guide by the light of reason, we must let our minds be bold.

Thank you so much, ladies and gentlemen, for a great discussion.

(Applause)

* * * * *

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, 2012