THE BROOKINGS INSTITUTION

HACKTIVISM, VIGILANTISM AND COLLECTIVE ACTION IN A DIGITAL AGE

Washington, D.C.

Friday, December 9, 2011

PARTICIPANTS:

Introduction and Moderator:

ALLAN A. FRIEDMAN
Fellow, Governance Studies
The Brookings Instituition

Panelists:

GABRIELLA COLEMAN
Professor
New York University

RICHARD FORNO, PH.D.
Cybersecurity Graduate Program Director
UMBC

PAUL ROSENZWEIG
Principal, Red Branch Consulting
Lecturer in Law, George Washington University

* * * * *

P R O C E E D I N G S

MR. FRIEDMAN: So, I want to thank you all for joining us this Friday morning. I know, in the season of holiday parties, sometimes it can be hard to drag oneself out of bed, but I think we have a very interesting discussion lined up today. It's a topic that is both very popular in the media but, at the same time, doesn't get a lot of very serious discussion. Anonymous and the related phenomena of hacktivism have inspired an incredible amount of fear. I know, inside this particular Institution, there was a decent amount of concern that we might be exposing ourself to some sort of risk because a lot of the media reports are genuinely terrifying. This seems to be this force from out in the ether that can come and prey on anyone at any time. They have visuals that are certainly resident of many popular media themes, a creepy computer voice, and they seem to be everywhere. At the same time, there are many people who are tempted to dismiss some of the phenomena that we see.

Every generation has some sort of antisocial behavior that people decry. Bill Buford's famous book *Among the Thugs* talks about hooliganism and, at the time, everyone in England was afraid that it was going to destroy civic society, and there's a natural reaction among some of the people who have been doing IT for a while that every time the media talks about something new in IT they're going to overreact. See, for example, sexting.

But, there is, I think, quite a bit to talk about and understand in the phenomena of digital hactivism and vigilantism. There is some power on the technical side. The attacks take advantage of social phenomena, of crowd sourcing. They use tools that are shared by others in some cases, denial-of-service service attacks. The model of doxing or releasing massive amounts of public information about individuals is certainly disturbing to many people and many companies.

And as we look at it, several things are apparent. First, much of the power that we see comes from the open nature of the information technology world. We don't regulate how to design a website. We don't enforce clear models of what upstream providers have to do, and private information is easily available about all of us, everywhere. So, this is part of the ecosystem that we live in. Similarly, Anonymous as a phenomenon, I think, really deserves to be studied if for no other reason than it's a fascinating, self-organizing system. Online association and collective action has been something that people have talked about since the beginning of IT, and have talked about the challenges of pseudonymous and Anonymous communication in terms of building a community. This one seems to have accomplished some amount of collective action. And, at the same time, it's also clear that a world with multiple groups who are happy to engage in their own agenda at the expense of law and order, at the expense of other people's private property, at the expense of other people's systems, is not a very stable model that we want to look into. So, as policymakers and as scholars, we need to explore that and understand what the long-term trajectory is going to be.

To do that today, we have a fantastic panel. We'll be starting off with Professor Gabriella Coleman, who's an assistant professor of media, culture, and communication at New York University, soon to move up to McGill University, and she's an anthropologist by training. Her first book, *Coding Freedom* is about the online associations and models inside the free software community and how you have community and cooperation and collective action in that community. She has since been working on, among other aspects, understanding the Anonymous world and has spent a lot of time talking to people involved and studying them as an anthropologist, as an ethnographer, to understand what's going on in that community.

On the technical side to tell us a little bit about some of both the attack models and defense approaches that we can have, we have Richard Forno, who is the director of the graduate program, cybersecurity, at the University of Maryland, Baltimore County, and is the co-founder of Maryland Cyber Challenge and Conference. He's also a visiting scientist at the Software Engineering Institute at CMU. He has a long and storied career in IT and computer security and was one of the first people to seriously study Information Warfare as a new phenomena in the Information Age and has written a book on information, *The Art of Information Warfare* and also *Incident Response*.

Finally, to give us some understanding of the policy side and the law enforcement approach, we have Paul Rosenzweig, who is the founder of Red Branch Law and Consulting. He's also a fellow at the Heritage Foundation and a professional lecturer at George Washington University Law School. He formally served as a deputy assistant secretary for policy in the Department of Homeland Security, and twice as acting assistant secretary for International Affairs, where he was deeply engaged in understanding development of policy and strategic plans in a variety of national security activities, including things related to IT.

So, with that, I'd like to welcome Gabriella Coleman to tell us a little bit about her life among the hackers.

MS. COLEMAN: That was great. Well, thank you so much, Allan, for inviting me here today. It's actually really exciting to be able to talk to a slightly different audience than I normally talk to, which also presented some challenges because I wanted to maybe give you a picture of Anonymous that you may not be getting in the media, for example, but I also just want to cover some basic ground. So, I've kind of compiled a short little presentation that gives some history, but then also gets at some kind of analytical questions that I think are kind of interesting and important as we maybe discuss some policy questions during the panel. So, I'm going to just jump right in.

All right. So, Anonymous is, by nature, as well as design, difficult to define. It's a name employed by dispersed individuals; some, small groups of hackers, technologists, geeks, system administrators, human rights activists -- a cluster of both ideas and ideals adopted by these individuals to organize collective actions, online and in the real world. Some are fearsome, others are trivial pranks. Some interventions have saved lives in the Middle East region.

In recent months, Anonymous has continued to show its face in a range of very unlikely places. From an audacious announcement to take down the seemingly invincible Mexican drug cartels to its constant presence in the Occupy movements. Anonymous seems everywhere, and yet, notoriously difficult to pin down, and they've made my life as an anthropologist very difficult at times. Their actions are alternatively peaceful and legal, illicit and disruptive. Often times, they exist in a moral grey zone, as Anonymous has famously deployed disruptive tactics and illegal ones, such as the distributed denial-of-service attacks, for the sake of making political claims.

Many of these characteristics of Anonymous have much to do with its origins on 4chan, which has become an immensely popular and iconic message board since its launch in 2003. It's been described by one of my colleagues as the single most offensive human artifact in human history. So, I take no responsibility if you decide to go there. You might have to make an appointment with your therapist afterwards. Composed of 50 topic-based forums, ranging from anime to travel, 4chan is widely perceived to be one of the most offensive quarters on the Internet, teaming with pornography. Next to nothing is sacred there. Participants communicating in a language that seems to have reduced English to a bevy of vicious epithets shocking to outsiders, but among insiders taken as the normal state of affairs. Indeed, one of its defining and endearing qualities.

Today, Anonymous is nearly synonymous with a very irreverent brand of activist politics. But before 2008, the monarchy was used exclusively by people from 4chan for staging fearsome pranks -- in Internet parlance, trolling. While trolling has often been the purview of boastful clicks such as the exploits of *weave*, who's a hacker, who's the president of a group called the GNAA, which is an extremely offensive trolling group. On 4chan, trolling is largely crowd source and participants are strongly discouraged from identifying themselves. Because of all the trolling to come rolling out of 4chan, in 2007, Fox news dubbed Anonymous the Internet Hate Machine, which Anonymous embraced, ironically, and then shortly thereafter, in response to this Fox News segment, it released a grim parodic video describing itself as the face of chaos, harbingers of judgment -- those who laugh at the face of tragedy.

Six months after the release of this video, some Anons took this trolling namesake to organize more strident forms of protest. This surprising metamorphosis is what prompted my ethnographic study of Anonymous in 2008, the year they launched what they would describe as an epic win, when they trolled the Church of Scientology. In the course of a few weeks, these events -- these trolling events against the Church of Scientology, which took the form of sending unpaid pizzas, pranking dianetic hotlines, sending nude fax body parts to the church -- these events took a dramatic U-turn and came to include earnest street protests. Anonymous shifted its tactics disseminating incriminating facts about Scientology, forging bonds with an earlier generation of dissidents, and focusing in on issues of censorship and human rights abuses.

A spout of trolling had thus given birth to an activist endeavor, by the name of Project Tunology, and is really interesting because this shift occurred quite accidentally. And you see this all the time with Anonymous, people had released a video; one of the videos by the name of "Hello Leaders of Scientology" was just done for the fun of it. It was not a kind of serious video. It was a call to arms to dismantle the Church of Scientology, but it prompted a discussion on Internet chat rooms, where people ask, "Huh, maybe we should, in fact, protest the Church in earnest."

So, the video was made for what's called, "the lulz," L-U-L-Z. These four letters are a bastardization and pluralization of laugh out loud, and it denotes the pleasures derived from generating things like, Internet memes, which might be very playful cats with insensible captions to more fearsome pranks.

So, so-compelling was this video that they decided to organize street demonstrations, and on February 10th, 2008, thousands of Anons and supporters hit the streets in cities across North America, Europe, and Australia for a worldwide day of action against Scientology. Six months after being labeled the Internet Hate Machine by Fox News, Anonymous had legions of followers in the real world, not just geeks and hackers typing at their keyboards who are seizing on the group's name, its ethic of anonymity and iconography.

Project Tunology, thus, marked the genesis of a distinct political sensibility, one that cannot be reduced either to just their trolling nor their ardent free speech commitments. It's important to note at the time that project tunology took off; the name was still being used by people on 4chan to troll. Two years later, Anonymous became even more widely known and came to be more widely thought of as an activist entity, as a result of a different network, by the name of Anon Op. So, this is a whole different group of people on a different Irish Sea network, who coordinated what you may have heard Operation Payback, also known as Operation Avenge Assange, which was launched to paralyze the Web site of the financial institutions refusing to transfer funds to WikiLeaks from donors.

In the ensuing months, I became shackled to my computer -- that was in December 2010. And, thankfully, I was on sabbatical, as this germinal operation gave rise to dozens and dozens of additional Anon Ops political endeavors, from Op Malaysia, which enabled citizens to bypass government filtering, to providing daily technology assistance to activists in the Middle East and African Revolutions. Those operations, in particular, were dubbed the Freedom Operations.

Then, in February 2011, came one of their most famous operations, Operation HBGary. Aaron Barr, the CEO of the security firm, claimed to have poned Anonymous -- claimed to have uncovered the identity of key operatives. In response, and in 48 hours, Anons hacked Barra's Twitter account and spewed the most kind of offensive racial slurs possible in 140-character limits. They had him follow the Holy Trinity of Hitler, Gay Pride, and Justin Bieber. They hacked HBGary's servers. They downloaded 70,000 emails, gutted the files. Then, they wiped out his iPad and iPhone for good measure. They published the company's data, alongside Barr's private communications, and this was done purely for the sake of trolling, for retaliation, but during the process, they uncovered a document -- the WikiLeaks Threat -- which outlined how HBGary Federal and other security companies might undermine WikiLeaks by submitting fake documents to their site. There was also evidence of plans to ruin the careers of supporters of WikiLeaks -- among them, Glenn Greenwald from Salon.com.

It was only a small crew of hackers within Anon Ops who had started this kind of retaliatory trolling event and ended up exposing what was a kind of COINTELPRO-like proposal. And, basically, what happened -- and again, this happened so much with Anonymous -- they do something, they discover something, and all of a sudden they decide to go forward with a new type of intervention because previous to this, Anonymous had rarely hacked to expose security flaws and access politically sensitive information, preferring to deface and disable Web sites, along with their legal human rights tech activism.

The success of HBGary, and especially the kind of colossal media attention it received, launched new wings of Anonymous dedicated to disclosure of documents, dedicated to exposing security flaws, by doing illegal hacking.

Okay, so that's a little bit of a sort of overview of where they came from and just I want to finish off by making a few kind of more conceptual points. There's still a lot more that I didn't obviously cover. So don't take that as, you know, the only thing Anonymous has done.

So, as a result of the actions just described, Anonymous has been generally misunderstood, described by news reports, alternatively as kind of freedom fighters, online activists, or vigilantes. Given what I just told you, the nature of this confusion is not hard to understand because beyond a foundational commitment to anonymity and the free flow of information, Anonymous has no consistent philosophy or political program. Though Anonymous has increasingly devoted its energies over time towards digital descent and direct action, marshaled in the service of political causes, it has no definite trajectory and its political sensibilities are still drawn by the collective will towards pranking, transgression, and mischief.

Even as Anonymous has moved away from pure trolling and 4chan, the underlying character of Anonymous is still intimately connected to kind of lulz joking and mischievous pranking, common to the culture of online message boards, and some of their kind of political actions are still motivated by this kind of prankish sensibility. Thus, if one term embodies the paradoxical and contradictory character of Anonymous, which is now made up of committed activists and agents of mischief, or mischievous activists, it is the lulz. The spirit of the lulz, however, is not particular to Anonymous, the Internet trolling, nor our times.

There have been other groups in the past, such as the Dadaists, the yippies, and the yes men, who have shared a kind of similar rowdy disposition where you fuse pranksterism with activism. But these groups, as opposed to Anonymous, were conceived from the start as radical, political enterprises, who were also quite vanguardist in their composition. They weren't, you know, allowing kind of hoards of people to join up. Thus, what sets Anonymous apart is its fluid membership and structure, and its organic political evolution. And so, within the activist expressions of Anonymous, you have order, disorder. You have serious protests in the lulz. You have legal and illegal tactics. And they kind of coexist to ensure a kind of fiery storm of interventions that will make some people inspire to follow suit, others smile, some cry, and leave many wondering who and what lies beneath the mask, which is to say that Anonymous follows a logic of its own.

Partly because of its maverick image and lulz antics, the group has secured constant media attention, along with a considerable number of participants, as well as a wealth of sympathizers who may not spend hours in chat rooms, but will heed commands to their operations, contribute to DDoS attacks or circulate messages unfurled on popular Anonymous Twitter accounts. They've developed a loose structure with technical resources, such as Internet relay chat being run and controlled by a few elites. But, these technical elites have erected no formal barriers to membership, such as initiation guidelines or screening processes. Ethical norms tend to be established consensually and enforced by all. The hacking operations are much smaller, much more covert, and far less participatory, but all political operations often come together haphazardly.

It's like Anonymous has its finger on the pulse of world events and exploits ones that they think they can intervene in. Despite its unpredictability and the tendency of Anonymous to act in ways that are irreverent, even destructive, vindictive, often times disdainful of the law, Anonymous has seemed to capture a certain prominent Zeitgeist. Today, the image in iconography has deeply resonated with many outside of the purview of Anonymous. The icon most associated with them, the guy fox mask, has come to stand in for a new form of identity, individualism, the promise of human flourishing, embitterment, and the absence of leaders, and moreover, in the absence for the need for individual recognition and fame, and it's become one of the most prominent sort of symbols in the Occupy movements.

Across its various faces, Anonymous is configured as E Pluribus Unum, one out of many. The singularity premise on a celebrity anti-leader ethic, participants chastising those who seek credit, recognition and especially celebrity and fame for the labor they put into the collective pot. And so here, I'm just giving a little bit of a sense of how they do have some shared ethics and norms across the different kind of faces and networks.

The most dramatic example of the importance that Anonymous puts on its kind of anti-celebrity ethic came in real-time on IRC when I had posted on one of the channels, an article from actually a newspaper that comes out of D.C. that was on Anonymous. And after reading the piece, many participants were just simply indignant that the featured Anon had revealed details about his personal life to the reporter and, in fraction, made only worse by the fact that this person hadn't really contributed much to some of the political operations.

One of the very respected IRC operators who tend to be more prominent assessed the situation in one biting sentence. She said, "Attempting to use all the work that so many have done for your personal promotion is not something I will tolerate."

A number of Anons then called this person into a different channel, asked him to justify his actions. Unsatisfied with his answers, they eventually killed him off by banning him on this particular server.

But it's not simply that, within Anonymous, individualities eradicated in favor of a well-defined group goal. Part of the reason that Anonymous looks the way it does, operations blooming like crazy as a rhizome or as a hydra is because individuality flourishes among Anons. It is part of the reason for with Anonymous is also driven by strife intentions, especially between the different networks.

Few of the Anons in projectionology who continue to protest the Church of Scientology were fans of the distributed denial-of-service attacks that Anonops had launched in support of WikiLeaks, for example.

The Anonops network thinks that the projectionology operations are too small and narrow to be effective. The hacking-to-leak operations brought other tensions to surface due to the fact that these hacking endeavors by necessity had to be conducted secretly on a network that values open participation.

But even if Anons don’t always agree about what's being carried out under the rubric of Anonymous, and they do argue a lot about it, they tend to respect the fact that anyone can assume the moniker. That’s really what they really value.

To conclude, Anonymous sits at the cusp of spectacular visibility, thanks to the media and intense individual invisibility. They’re rootless, evasive, shifty and nomadic. Their visibility is secured by the lows for better or for worse via pranks, via these hacks, and the lows securing some of the most audacious irreverent and scary interventions.

The symbolism of anonymity and their anti-leader ethic has circulated far and wide, and seemed to have kind of captured the imagination of other activists around the world.

However, in many other respects, they are invisible, intractable; they're spectral. Anons camouflage their identity, although to different degrees and for different purposes. Since some Anons engage in illegal actions, they use it tactically for defensive purposes. Most all Anons, even those that engage in only legal and peaceful protests also conceal identity for ethical reasons, as I discussed. As a whole, they shun individual celebrity and fame. Thus, at the very same time, they've been made into Cause Celeb by the media; and by this, I mean a kind of very controversial topic. They, themselves, are disdainful of the culture of celebrity.

To be Anonymous is to be many things from prankster to hacker to human right activist to fusions of these. However, they sublimate signs and markers of their individuality that otherwise are so commonly offered in every way, place and form in today's highly networked world of social media where one is supposed to reveal a constant stream of information about yourself.

Whatever we might think of their individual campaigns, Anonymous has thus secured a small oasis of anonymity in this desert of constant bottom-up self-revelation and top-down turbulence. So hopefully that'll give you a little bit of a picture of what they look like from the vantage point of an anthropologist who has spent way too much time on internet chat with them over the last year. Thank you.

(Applause)

MR. ROSENZWEIG: As we go through our talks this morning, if there are any members of Anonymous here and hear us make a mistake, would you raise your hand and correct us, please? We want to make sure we're giving accurate information. Are there any members of Anonymous here?

MALE SPEAKER: That means we're all members; nobody raised their hand.

MR. ROSENZWEIG: Any members up here? So we heard about the conceptual underpinnings of Anonymous; you know, who they are, what are their motivations. I'm going to spend a little bit of time talking about how they do it and what we might consider doing about it at an operational level.

Your terms like denial of service, spot-nets, IRC; how do these all come together and what does it mean for Anonymous and online activism or online vigilantism? Well, denial-of-service attack is simply as the name applies; it knocks another server or network off the internet. It shuts it down. It denies that service. You can do it one against one or many against one.

In the case of Anonymous, their preferred method of attack, if you will, is many Anons targeting one given target, and then you essentially overload this target with a lot of information, a lot of network noise, and ultimately that target crumbles.

Part of the allure of denial-of-service attacks is the fact that you can acquire large constellations of cyber armies consisting of controlled PCs very cheaply. So, for example; if I'm a member of Anonymous or any non-Government group, a terrorist group or any sort of non-Government entity, and I want to cause mischief on the internet for spamming purposes or to make a political statement, I can rent -- yes, rent for a 24-hour period a constellation, an army of let's say 100,000 computers that have been compromised by others. And for that 24-hour period, I can use this constellation of computers that I don’t own to do my bidding. And the going rate is pretty cheap; anywhere from $500 to a couple of thousand. And you get this cyber army at your command for the next 24 hours. Pretty impressive, especially when you can harness all these powerful PCs and laptops to target a given website like the Church of Scientology or, you know, Master Card or Visa.

But at the same time, there are also tools available individually that users, we can download and use to launch our own denial-of-service attacks or participate in one to show our support. One of the most commonly known tools that's made the rounds of the media over the past year or so is a tool with a name of Low Orbit Ion Cannon. It sounds very star warsy, doesn't it? And this is a free tool; LOIC. You can download it. It's a Windows-based tool. And from this tool, you simply say, "I want to attack this target. I want to send this message," and tweak a couple of settings and click go, and you now turn your computer into a direct weapon sending network traffic against your target of choice.

Now, imagine tens or hundreds of thousands of people doing the same thing, same effect, a denial-of-service? So that’s what a denial-of-service is and that’s generally been the tool of choice, if you will, in many of these Anonymous and online vigilante type of events to raise publicity about a given issue, about a given topic.

What's the goal though? What's the goal of using these tools? What's the operational goal? Well, first off, to draw attention to the cause, as Gabriel said, we want to make a political statement. We're protesting the Church of Scientology, their policy on internet censorship, their policies on whatever. We're protesting Master Card and Visa's policy of withholding payments to the WikiLeaks' defense fund. We're making a political statement.

You can trace a type of online activism back to the mid-90s with the electronic liberation front and the Mexican Zapatista who did early types of denial-of-service and website defacements to draw attention to their cause, whatever that might be; in the 90s was mostly political.

Online activism essentially jumped the shark from traditional real world activism. Instead of vandalizing a polling station, they would vandalize a website, a political website and replace the homepage with another message, a political message.

So you see how activism moves from the physical world to the online world in the 90s. And now, with the collective nature of Anonymous and the nature of internet in general, we take it to a much more distributed level of impact and influence.

So you have denial-of-service attacks as probably the most common form of online activism or protest to make a point. You also have website defacements; the goal being, we're going to attack a given website and replace the homepage with something else, our message.

So, for example, if Anonymous wanted to take on -- I don’t know -- Whitehouse.gov, you go to the White House website one day and you see a Guy Fawkes mask. That’s a defacement. That’s a political statement. Maybe there is a movie or a message of some sort there, a taunting or teasing or something. That’s a message. That’s website defacement; again, in furtherance of a political or social cultural goal.

But we also see cases where groups like Anonymous target intellectual property, personal information, corporate information, proprietary data, and that raises a whole different set of questions. And while we hear discussions about -- I forget the term Allan use -- doxing -- I've heard it before; I just drew a blank; doxing. Most people don’t equate doxing with Anonymous or online activism. They equate denial-of-service attacks with online activism, but doxing is also a form of online activism. But how does this occur?

And for me, one of my challenges in talking with media and those who don’t necessarily understand the nature of online activism is that denial-of-service attacks aren't the same as stealing private information. Okay? Denial-of-service attacks generally take place only from the outside.

And every opportunity I raise a point that, theft of proprietary information from within a company or government organization suggest to me that there is probably an insider helping them out. That’s not a simple case of somebody in their hotel room or their door room hacking in and stealing something. Not unheard of; it does happen. But the vast majority of these incidents, I believe, occur with the help from someone on the inside who may or may not be a supporter of Anonymous or a given online collective.

If indeed a given incident of online activism, whatever involves theft of data that then raises a question of, "Well, what can we do about it?" I mean, if a website goes offline, yes, it's annoying. It's a nuisance but we can deal with that, generally. But how do we put the genie back in the bottom with information that’s been extracted, been stolen from our private networks? Can we do it? Not really. It's very difficult to un-ring that bell, so to speak.

So this raises the question in my mind of, "Well, where is the vulnerability here? What happened? How did this online collective group manage to steal this information?" Well, point one; there is possibly an insider involved. But whether there's an inside involved or not, it raises a question of internal security controls and risk management; in other words, good cyber-security. That’s my concern.

I then wonder, is this incident of proprietary information leaving a company the result of incompetence or complacency; and I point the fingers and the IT staff. Well, we could talk about that in the Q&A.

So what can we do about it? We have two different types of attacks; two different modalities. We've got externally oriented, denial-of-service type of attacks, and we have theft of intellectual property, theft of personal information from machines on the inside of our networks. What do we do about them? Well, in the case of externally oriented denial-of-service attacks, the answers haven't changed for the past 12 or 13 years.

Back in 1999 when denial-of-service first came on the internet security scene, I was part of a team that looked into "What do we do about it? This is going to be really bad."

Some old-timers here might remember words like trinew and stockeldrot or tribe flood net. These were early examples of denial-of-service attacks and they scared us back in the late '90s: you know, could this shut down the internet, and in some parts, it did.

So we developed a list of countermeasures to deal with denial-of-service attacks coming from the outside from groups like Anonymous or other online activist groups. Things like ensuring we have enough bandwidth available to give our legitimate internet traffic a chance to get through. If I'm Amazon.com, my bread and butter is the customer data coming into my web servers.

If I can expand that internet pipe and add more capability, that may mean we get more bad stuff coming into us during attack, but it also gives the good traffic a chance to get in. And if I'm an e-commerce site, I'd rather have 20 percent of the revenue still coming in during an attack than no revenue coming in.

So things like increasing your capacity, filtering, identifying traffic that’s going in and out of your network to see does it match a given pattern of a known attack tool of a known denial-of-service tool, and then blocking or working with internet providers upstream of you to disrupt and track these attacks; these kind of measures haven't changed.

Strong internal controls in the case of intellectual property being extracted from an organization, and the best example of that is the Bradley Manning/WikiLeaks scenario. How could one person in a tent around the world get access to this, what they call the treasure trove of data; one person? What risk controls were not in place or circumvented that allowed this insider to steal all this data? Internal controls, which really comes back to good risk management and good security planning and operations, security competence.

One of the things that challenges security folks in dealing with online activist type of events -- denial-of-service or (inaudible) filtration of data -- is the fact that these groups, as we just heard, are very resilient. And it's very difficult to block or prevent everything coming at us from these groups.

When I was a child -- and you go to a birthday party as a kid -- you go to those arcades and they had the game Whack-A-Mole -- you know the game where you hit the mole, mole pops up, you hit it, and then another mole pops up and you hit that one and another mole -- right? That’s what we're doing here as defenders; we're playing Whac-A-Mole.

If you want to block every attackers coming at you, you’re never going to win. You'll be playing a perpetual game of Whac-A-Mole, which illustrates the resiliency of these attack networks and their ability to survive even in the face of a strong defense. And it really becomes an order of scalability and capability; very difficult to trade blows one for one with these types of distributed attacks around the world.

You block this IP address from Russia and it's replaced by another one from China or one from Russia or one from France. You're not going to win in a one-on-one bout with them. So the challenge for defenders is the pure technical resiliency of these online groups, let alone the social resiliency, the anonymity factors that Gabriel talked about. Okay?

You have these characteristics of the social aspect also applying to the technical aspects, makes it much more challenging for us as the defenders to be effective.

So why do we care? Well, if we are the victim of an online activism attack, we're involved -- as a victim, we are perhaps embarrassed. "I run a great company and our website was defaced in support of the protest of the Church of Scientology. Well, we have egg on our face for a day. We know somebody report it to the media; there's some bad press about us: okay." A nuisance but not insurmountable. But we might care about that intangible reputation value. And if Anonymous could deface our website, could somebody else do something more devastating. That raises all kinds of follow-on questions.

There might be political ramifications. Again, you look at protest and support or against the Arab Spring or, you know, Bradley Manning, WikiLeaks, or even just, more recently -- and I'm drawing a blank -- the recent Russian elections. Okay?

In the past 36 hours, people noticed that folks on Twitter posting questions about the legitimacy of the recent Russian elections or any sort of misconduct, those tweets were suddenly swamped by tons of other tweets coming in and burying it in the Twitter universe; a form of online activism being used to stifle descending opinion about political real world physical social change, social elections. Okay?

So we care about that because, what does this mean for stifling political expression; if not freedom of expression, more generally, so there are political ramifications for the leadership and as society and, of course, loss of information.

If you’re running a company and you have intellectual property or war plans or cables that are extracted from your private networks, you have a loss of credibility. It raises questions that it might make you a bigger target for another type of adversary because they realize if this one group was able to compromise and steal data, who else could? How good is your security really? And I won't go into too many examples, but it's more of a concern than I think we care to admit to ourselves.

Finally, I'd like to just leave one comment: understanding the structure and the organization of groups like Anonymous is useful, as is understanding the technical way in which these groups operate and what we can do to defend ourselves or mitigate the consequences of any sort of incident arising from their existence in the world.

But I also wonder if more attention should be given to their motivations for action. And rather than look outwards at them and blame them, whoever they might be, we also take a minute and look inwards to see well, what are we doing that motivates and inspires these groups to action.

If you look at the moral gray area that Gabriel talked about, a lot of things Anonymous has done in their doxing over the years I think is kind of cool, me personally. It's interesting to see things and get a different glimpse of the world, but that’s a whole huge gray area. And we have to really wonder, well, why is this being kept secret to begin with? Again, I'll go back to the Bradley Manning example.

A cable was classified, made the front page of the New York Times that said, "Canada is a strong ally of the United States; a classified cable. You could find that going to the CIA world fact book, Wikipedia; take your pick, okay? People saw that and they go, "Why is this classified?" We phrase questions that maybe those in charge don’t want asked; you know, "Do we over classify too much information. Information may not want to be free but are we restricting too much of it?" All kinds of corollary issues get raised as a result of this fusion of social activism and technical capabilities that allows information to be disclosed and flow to make a political statement.

So, I close by simply wondering if not just looking outwards at the adversary, but we also look inwards to see what are we doing that enables them in their day-to-day operations. Thank you.

(Applause)

MR. FORNO: I too want to join in thanking Allen for inviting me to come and speak with you here at Brookings. It's always a pleasure to come over here.

I want to start by saying that I hope that I at least, and everybody who considers, this would approach this topic with a sense of great humility, which is to say that it's very, very difficult to talk about what to do about a problem when there's a huge arc of technological change going on.

It's extremely difficult to think about the policies to approach a problem when there's a massive social change going on. It's doubly hard in a situation like the discussion we're having today about Anonymous and other hacktivist groups to make good judgments about what the right course of action is when the phenomenon that we're talking about is a product of a confluence of both massive technological changes on the internet and massive social changes that it enables.

So I offer the comments with some degree of trepidation and with a great deal of uncertainty about the right way to think about Anonymous generally. I love the title of this panel. You know, hacktivism, vigilantism and collective action, because it spans the gamut of possible ways of thinking about groups like Anonymous. And the true answer is, is that, in some instances, it's hacktivism of a vicious sort, or vigilantism of an even more vicious sort. And then in some instances, it embodies collective action that has been a traditional core part of what we in America think of as free speech and political activity.

I think one of the things that I start with in thinking about how to think about Anonymous is to think that, in some ways, groups like this are an inevitable consequence of the internet. The internet is this borderless domain that exists across sovereign borders in ways that are new and different and fundamental. It has built into its structure essentially an inherent bias towards anonymity.

You can identify people within the domain of the internet, but as a first-cut matter, that’s not what the internet is about, and so we tend to favor the ability to be Anonymous on the internet as an architectural matter; not as a political matter, but in the nature of the way that the internet protocols operate and the switching system is built. It tends to enable action at a distance, right?

I mean, most of what we consider to be activity that we regulate in human nature is action in person, this speech. We have seen steadily the arc of technology permit action at a distance; television, radio sorts of things, and the internet just is a quantum leap forward, a step function forward in the ability to act at a distance.

It allows asymmetric action, right? In a world of conflict, it used to be, yo, who had the bigger guns wins the conflict, or who had the bigger voice wins the debate, wins the shouting match. In a world where every human being on the internet, all two billion of them, can download the low ion cannon and become a cyber warrior in -- what's the download take; about 32 seconds, something like that? Yo; that changes the dynamic of what power means in the context of the internet.

And the final thing that really makes Anonymous a challenge and what makes it almost impossible to distinguish between hacktivism, vigilantism and collective action is that on the internet, the information flows are indistinct. It's all ones and zeros, right? It would be as if, in air power, we couldn’t tell the difference between commercial planes, spy planes and missiles that were coming across our aviation borders.

Yet, on the internet, by and large, it is difficult, it not impossible, to distinguish between normal commercial traffic coming to Amazon and as denial-of-service attack. You can, again, with difficulty, but those sorts of factors enabled an Anonymous indistinct at-a-distance collective action attack of a sort that is completely different than anything we've seen. So, in some ways, I tend to think of this type of group or these types of groups as an inevitable consequence of the very fundamental architecture of the internet.

And then when you ask yourself what should one do about it, at least the first order approximation is, "Should we do anything?" Right? Or is this just kind of the natural churn of this amazing borderless open communication system that has produced so much in the way of positive value to society. It enables Wal-Mart and Amazon and banking online and getting the Guardian front page on your computer right now.

I mean, there are all these sorts of things that are necessary portions of the internet that go under the rubric of internet freedom or internet commerce, any one of which is systematically at risk the more we tend to tamp down on communications because we fear the consequences of them.

So one possible approach to this is to think that there's nothing that really need to be done. We can do good hygiene on our own end and, you know, just like everybody should get their flu vaccines, everybody should have a firewall program and an anti-intrusion program on their computer. But it may very well be that there is nothing that, systemically, a government ought to do about that.

On the other hand -- well, and if you buy that, then I can just sit down and we can stop this. I actually think that there's more to it than that. But for policymakers, at least those with some degree of humility, I would say before we enable a large set of massive changes of governmental policy and restructuring of the internet, we sort of think about whether or not that’s truly necessary, because I think the candid answer is that though Anonymous generates a great deal of fear and a great deal of media attention, the true scope of the harm that it has actually caused is relatively modest; certainly not existential, at least not yet. And perhaps you fear that they might become an existential threat down the road, but at least, as a first approximation right now, it's kind of like crime, right? You can't eradicate it; you just kind of worry about it. You try and reduce it a little, but we're never going to reach a world in which there are zero murders. And I suspect that absent massive change, we'll never reach a world in which there are zero Anonymouses; period, full stop. So maybe we just live with it.

What you decide to do about it though depends upon really which of these three bucks, hacktivism, vigilantism or collective action you think is the predominant value, and which approach you should take.

If you think this is a hacktivist group, kind of one that acts in a illegal manner as a way of either making a political point towards stealing personal property, then to me, that assimilates sort of to an insurgency of some sort, right?

It's not a criminal group so much as a group motivated by a philosophy, a philosophy of anonymity and I would say also internet freedom and keeping sovereign control off of the internet. That looks a lot like, you know, Mau in China, looks a lot like, you know, the Viet Cong.

If that's how you think of these types of groups, then the right approach is a good counterinsurgency strategy, right? It's not going out and burning down the hamlets and villages -- we know that part of it doesn't work -- but it's something like good intelligence, right? A public relations campaign that tries to diminish their influence and those aspects of their interventions that are criminal, that hurt people, that are hypocritical, whatever their flaws might be, right. It's building capacity amongst people who would be resisting an Anonymous or other hacktivist type attacks by spreading good cybersecurity practices around the globe so that you can't -- I mean the largest number of botnets in the world right now are in Africa they say. Why? Because nobody there can really afford good cybersecurity practices so the computers are really well taken over.

It gives us a broad domain within which to work, but that is one way of thinking about it. If you think that they're vigilantes, right, if you think that they're essentially criminal actors, then the answer is better enforcement of criminal law. That means more cooperation internationally amongst law enforcement authorities and using public relations and diplomatic tools to get other sovereign nations to participate more regularly in counter criminal activity.

The botnets that Anonymous rents are -- a large number of them are, by and large, owned by a group called the Russian Business Network, which is a massive criminal computer enterprise housed in Russia. The fact that Russia has been weak in choosing to go after that group for their own reasons, i.e. because the business network is sometimes at their service as in the war against Georgia, that enables Anonymous by giving it access to a larger network of botnets.

If we think of this as a vigilantism problem, then one of the tools that should be on the plate is diplomatic activity by the United States to get countries like Russia and China and other people who haven't taken strong action against the underlying botnet and illegal server activity that enables groups like Anonymous to act, that's another model.

If, however, you think that this is dominantly a collective action public activism expression of a political viewpoint, then you've got a whole different cattle of fish. Then it's traditional First Amendment activity, right.

I saw just yesterday that Anonymous posted a video opposing passage of the National Defense Authorization Act here in the United States on the ground that it will authorize the detention of American citizens.

Whether you think that’s what the NDAA does or not, that’s classic First Amendment speech and is the sort of thing that ought not to be suppressed in any way, manner, shape or form. And it was with the Guy Fawkes mask and the big computer voice and even cited a friend of ours, a friend of mine as an authority. Then if it’s a First Amendment sort of activity, the only thing you really need to do, the only thing that’s legitimate is, A, police the margin so that it doesn’t trend over into criminal activity, and B, enforce the traditional First Amendment rules, things like preventing a heckler’s veto so that one set of free speech doesn’t drown out other parts of free speech. And that’s a completely different model for activity within the government and portends a completely different sort of policy and legal response to groups like Anonymous.

So as I started at the beginning with some humility, these are, you know, three models of action, and I honestly am not sure which is the right course. I suspect that in the end, it’s a mix of them. For my own self, I tend to see predominant within Anonymous the more adverse parts of the activity. I see less of the political speech and more of the criminality in the interventions and the theft of private information, so I tend to lean in that direction, but I’m certainly willing to acknowledge that I might be wrong.

And that kind of indeterminacy about what the true nature of the threat, if it’s a threat at all, makes it very difficult, possibly impossible for a coherent policy and legal approach to be developed to define what you should do to approach a group like Anonymous and its many co-actors. And with that, I’ll stop and turn over to questions. (Applause)

MR. FRIEDMAN: You may come by to make sure that we’re properly recording, because we’ll be recording this to post an audio version and a transcript on the web site soon. And usually I take the moderator’s prerogative to ask questions, but I think we have a number of hands already shot up in the audience because there’s a lot of provocative comments here. So I think we'll start with Ben over in the corner. And there are mics passed around.

Just a quick note on questions, please, if you feel comfortably, identify yourself and where you're from, and, as always, questions are relatively short and defined by the interrogative -- question mark at the end of the line.

MR. WITTES: So I'll actually stay Anonymous. No, I'm kidding. Ben Wittes from the Brookings Institution.

So as Paul alluded to yesterday's video or the video that I became aware of yesterday about the NDAA, which I actually think raises some issues that I'd love to hear all of the panelists talk about, but -- so one of the -- when you're thinking about which basket to group this in, this sort of activity, and one of the things that has to be salient to that is the way they present themselves, right, and the use of the Guy Fawkes mask and the symbolism, so in this video, which has speech by the guy in the Guy Fawkes mask that promises at the end some sort of action against the senate on Guy Fawkes Day of next year. So Guy Fawkes, of course, is at the end of the day a guy who wanted to blow up the British Parliament, and so he's a terrorist, right. And you have a presentation that talks about some unspecified action against the legislative body on the anniversary of the execution of or capture or failure of the terrorist plot to build up a different Parliament building by somebody proudly wearing a mask. So a nefarious read of that would say, well, it sort of kind of looks like, you know, a group -- a guy with an Osama bin Laden mask talking about a September 11th action involving the Pentagon.

Now, I don't actually read it that way, but I do think it raises the question of what the symbolism that the group is projecting about itself and what they're trying to say about themselves in relation to these various forms of action that Paul is sort of musing about. And so I'd be interested in all of your sense of, you know, how does their self-presentation affect the way they are and the way they should be understood by the larger public. Are they basically presenting themselves as speakers or are they basically presenting themselves as sort of something more nefarious than that?

MR. FRIEDMAN: Do you want to start with the history of the --

MS. COLEMAN: Yeah. So I'll give a little bit of background on why they use the mask, too, because it's just kind of interesting, and it goes back to this whole sort of way in which the contingent and the accidental creep into this world, and then speak a little bit to, you know, the message they're trying to convey.

So unfortunately, a lot of means are created. These are kind of capped phrases or images that are not simply viral. They're always under constant modification. And there's one mean called epic fail guy, he's a failure. And one day he put on the mask. And so, unfortunately, everyone knew about this mask because he put on the Guy Fawkes mask because, you know, of the popularity of the comic and movie.

And then when they had decided to, you know, fast forward, that was I think in 2006. Fast forward to 2008, when they decide to protest the Church of Scientology sort of in earnest. They knew very well, which is actually a fact, that Scientology goes after its critics, and they're like we must protect ourselves, and then they're like, well, where can we get cheap, accessible masks? And already the Guy Fawkes mask had been sort of in the air. And then they're like ah, the Guy Fawkes mask, right, and then all of a sudden, you know, thousands of orders replay.

And then it kind of stuck, in part because, you know, the very day of the protest they circulated images and videos like almost at the moment they were happening, and both because it is already a popular icon because of the movie, right, it has a cultural kind of currency, as well as the fact that it was practical, as well as the fact that I think more than the kind of terrorists association, it signifies that importance of anonymity just because the culture of Fortran is one in which you really are sublimating the individual in favor of, you know, the meme or the act. That, I would say, is one of the reasons why it stuck.

So then in terms of what message they're trying to convey, I'll just be very brief. For every video that may be kind of sinister and scary, you can find a video which really seems to be -- which not really seems to be, but is kind of parlaying, you know, a message of human rights activism and please help the people in Syria.

That's actually the point and I think that's why your presentation was so interesting, was like which basket do we put it in? And the problem is you can't even separate the individuals. Some individuals may be engaging in all those different actions, some don't. And then on one network, these multiple things are going on at once, and that's why it's such a kind of tough nut to crack.

MR. FRIEDMAN: Want to join in briefly?

SPEAKER: I'll just say, you know, from the operational perspective, if you have a public presence on the Internet, the senate.gov, the webmaster, the U.S. Senate, the U.S. House, whomever, if you're a public figure, celebrity, you expect to be a target of some sort, whether it's the paparazzi in L.A., or, you know, an online activism group looking to deface your website if you come out in favor of something they're against, and that really comes down to, you know, you expect it.

I mean, the Secret Service expects there to be attacks or threats made against the President and the Vice President. They're on guard for that, that's part of their job. They track down every lead and they follow them up. But there's a security bubble that work, a protective shield that works and in place.

If I was an operations person at the Senate, I would say, okay, let's be on guard for any suspicious network activity, any change in our baseline of normal operations that might be a clue that something is going to happen. I would do a lot more sharing of information with my colleagues, my Internet providers to try to see if there's anything out of the ordinary, but I would treat that as the noise of being on the Internet in that role that we are today.

MR. FRIEDMAN: Chris, in the front here.

MR. SOGHOIAN: Hi, my name is Chris Soghoian. I'm a fellow at the Open Society Foundations. So for the past few years, some simple minded politicians would say that, you know, terrorists in the Middle East are coming after us because they hate our freedom, which is, of course, stupid, although this line was trumpeted by our former President. But when you delve into the issues a little bit, you find out that they are legitimate beefs that they have, you know, stationing of troops in Saudi Arabia or our actions in Israel. I mean, we can disagree over whether they're legitimate or not, but there are deeper reasons why people may want to try and blow up bombs here.

I think Anonymous is the same. In many ways Anonymous is either the soul or the conscience of the Internet, and several of the things -- the actions that Anonymous has taken over the past few years have really struck a chord within me. And I'm going to say I sympathize with what Anonymous has done, but not the way in which they've done it.

When Visa and Mastercard cut off donations to WikiLeaks, when Sony went after independent security researchers for revealing flaws in their system that Sony had long ignored, there have been similar like this where Anonymous has really done something that no one else has done. Anonymous has stepped up because there was no one else to go and go after these activities. You know, whether or not you believe what Bradley Manning did was a good thing; I think many people are upset with what's been done since. And so, you know, Paul mentioned the idea of treating this as a counterinsurgency, and one of the techniques that you use when you want to stabilize things is, you know, you have this hearts and minds campaign, you go in and you build schools and libraries, and you provide free health care and candy bars. And the hearts and minds campaign against Anonymous would be to stop doing stupid things to the Internet.

So if we really want Anonymous -- and I will wrap up and actually end in a question mark -- but if we really want Anonymous to stop engaging in these kind of antics, wouldn't stopping things like SOPA be a good idea? Wouldn't stopping things like removing the power of the copyright lobby and, in fact, stopping the harassment of WikiLeaks seem to be a really good start? Thank you.

MR. FRIEDMAN: Paul.

MR. ROSENZWEIG: First, it's great to finally have a face to go with the name. We've been on the Internet before and now I know what you look like. I think you're right, in part. Here's the only piece of it that makes me a little skeptical of that story.

I see Anonymous and groups like that going after the easy target in the west, where they know that a rule of law prevents really adverse activity against them. I would have a greater confidence that that's the fundamental part of Anonymous if they were trying to break down the great Chinese Firewall and bring Internet freedom to the group of people who have the least amount with too -- did they?

SPEAKER: They were in the ground in the Middle East.

MS. COLEMAN: In the Middle East.

MR. ROSENZWEIG: In the Middle East, yeah. In the Middle East, they've been active, though, of course, their other action when they -- their act against the Mexican Cartel, which would have been I think a great positive example that made that part of the mean they withdrew. So they used their power, and I take most of what you say to heart, but they tend to focus on people who are going to fight back only within this zone of acceptable fight back, where they know -- where they probably know that we're not going to send assassination drones after them, maybe they think they will.

So I would be a little more comfortable with that as the fundamental expression if they were more catholic -- small C catholic -- in their oppositional taste.

MR. FRIEDMAN: And then Rick.

MS. COLEMAN: I just want to make one point, which is we're talking about Anonymous as if it's Anonymous. And then, you know, I sat there, and the mediating factor is the media, as well, who are very responsible, too, for kind of putting a spotlight on certain issues, but then it gains steam. You know what I'm saying?

SPEAKER: Yeah.

MS. COLEMAN: And so we're talking about as if they have intention and then, you know, we're supposed to interpret the intention. First of all, they're very good at kind of making intention hard to read, and then the media oftentimes is what kind of makes or breaks a certain sort of operation.

And then I would say actually, you know, for the whole month of January, the kind of interventions all over the Middle East and North Africa were really astounding, you know, and that's the thing that's really hard to kind of interpret.

But you have like basically a 16-year-old kid who started up Tunisia January 2nd, when the media was not paying any attention. And they were providing tools and helping them circulate videos out and making sure that they could protect themselves from death squads, you know. But, yes, that comes at the hands or right along with using tactics that are, you know, very profoundly discomforting at the same time.

SPEAKER: I agree with your take about this being -- possibly be the insurgency. And to your point about the hearts and minds, I think that the actions or antics, depending on your point of view, of groups like Anonymous does strike a cord in the hearts and minds of the public. Where the challenge is, is the public may embrace and support or quietly applaud a lot of their actions and disclosures or things like that, but then the policy-makers and the established figures in society, whether it's, you know, government or companies, they're obviously strongly against it. The media, not to be too conspiratorial, reports to their shareholders and they're part of the power elite. So the hearts and minds I think -- the public is I think in this group's favor. The hearts and minds argument is being won slowly, but not by the folks that actually, you know, swing the pendulum with SOPA and things like that.

MR. FRIEDMAN: So I think we have Michael in the middle of the back and then in the far back corner.

SPEAKER: Just a point on the media while she's getting back there. A prominent security writer declined to join us because he believes that they get too much attention, if we all just ignored them, they'd go away.

SPEAKER: So I have a question for Professor Coleman, sort of a connection question. And I'm afraid I'm going to have to do a bit of a 30-second preview to it. Kicking the Church of Scientology has been sort of the great hobby of the Internet zeitgeist since about 1993. Before there was Scientology, there was Clambake, things of that nature, and this has been going on for a really long time.

So at the same time, in taking a look, Richard mentioned (inaudible) sort of the early DOSbots spots. When you take a look at LOIC, LOIC is, in comparison to, you know, the current generation of malware, almost laughably primitive. It doesn't anonymize, it doesn't spoof, it doesn't do things that we think of as traditional malware type activity. So the thing I'm trying to figure out is sort of Anonymous' connections across time and in organizations. Did they -- when they started Trinology was this an outgrowth of things like Clambake? Whether the older -- you know, were the older grungier people of the Internet involved in that? And at the same time, is there any actual indication of real connections with existing cyber crime organizations, like the RBN or things like that?

It's true that they can rent a botnet, but one of the things that I've seen and speaking from sort of professional paranoid perspective is that a lot of their software is written in sort of the assumption that they're not going to get caught doing anything. And so I'm just curious about the relationships then to e-crime, to the past history, and things of that nature.

MS. COLEMAN: Great. I'm glad you asked, because, you know, it is kind of weird that I look at Anonymous and people want to know why it is and how I got to them. And, you know, I study free software and hackers, and I was quite familiar with the Usenet protest just because I knew people who had engaged in those battles. And then for a year I spent it at the University of Alberta in Edmonton, which happens to have the largest Scientology archives in the world housed in an old Ikea factory, and I felt like maybe Xenu was sending me a message that I should study this. And when I dove into it, I was like, oh, I see why geeks and hackers love to battle the Church of Scientology. It's their evil doppelganger, you know, the perfect nemesis. It's the bizarro comic world, right? It's extremely offensive because it's not simply religion, but one of science and technology that's false.

And so I studied those Usenet era protests, and, man, lo and behold -- and I thought it was sort of a thing of the past, and lo and behold, in 2008, this thing by the name of Anonymous emerges and starts to do it again. And I was like, oh, it confirms my perfect anthropological thesis, this is so wonderful, but it was such a niche kind of phenomena.

And so definitely I used to -- when I gave talks, would situate it in terms of that longer history. And yet what happened with Anonymous, I always thought it would kind of remain as kind of a trolling and a niche political boutique movements against the Church of Scientology. And on the one hand, it came as a great surprise when they started to kind of diversify their tactics politically, right, and so I kind of had to break away from just the scientology dimension. So that's just a little bit of kind of background in terms of how I got there. In terms of that kind of criminal connection, you know, there was one article I was upset at because it portrayed Anonymous as like criminal, and I was like, well, if they're criminal, they would try to stay secret, because that's what criminal do, they don't be like, hey, come look at what I'm doing.

Do they use criminal tactics? Do they turn to the RBN? Absolutely, some of them, you know, that's without a doubt. And some individuals within Anonymous, some really seem to be there just to kind of raise hell because they like to do this, and then others are willing to kind of use criminal connections and tactics for political purposes. So those both do exist in there at the same time.

MR. FRIEDMAN: Paul and then --

MR. ROSENZWEIG: I mean I agree with you. I think in a lot of ways it's a lot like any other protest movement, right. There are a lot of people who are there just peaceful protest occupying space, right. Then there's some who trench upon the criminal law, but aren't true criminals say building a hard structure in the middle of McPherson Square without a permit, which, you know, gets you some real attention.

And then there are people who kind of slipstream inside the group, maybe share its values, but who really like to go out and burn down buildings and break windows. And then there are the next group which come behind them and steal the TVs from outside. So one thing I think is fundamentally correct about what Gabriella said is that this is a multifaceted phenomena, a very diverse group of people. Some of them are just in it for the lulls. Some of them like the lulls, but are, you know, are in it maybe to make some money. Some of them are in it to -- everybody has got a motive, and it's -- the challenge is that we run a risk of trying to pigeonhole them into any one category, and it's not. You know, it's not like China, you know what China is, right, you can figure out who the leader is. You can't figure out who the leader of Anonymous is.

MR. FRIEDMAN: Rick, have you seen anything on when and to the extent which they use sort of malware and botnets?

MR. FORNO: The extent as far as the -- how frequent they use it?

MR. FRIEDMAN: How frequent they use it.

MR. FORNO: I don't know how frequent they use it, but when you look at some of the large-scale events like attacking Visa or Mastercard or Paypal, when you see a web server of that magnitude or a web server or a form of that magnitude get knocked offline, you know it's not two or three people using low LOIC, it's an army of probably zombied computers.

MR. FRIEDMAN: There's a question in the back corner? Then we'll come up front.

MS. WEEDEN: Okay. So my name is Jenn Weeden, I work at a cyber risk management firm. This question is mostly for Dr. Coleman. But I was wondering if you could speak to -- I know it's hard to get into the demographics of the group seeing as it's so fragmented.

SPEAKER: And Anonymous.

MS. WEEDEN: I also have had the misfortune of reading a lot of the IRC chats. And to me, I could never reconcile some of their -- you know, and the (inaudible) Tunisia, whatever, I couldn't reconcile the political ideas behind the rampant misogyny and racism and complete incoherence of some of these actors, so I was wondering if you could speak to that.

And secondly, I would disagree with everyone's characterization of the Russian Business Network. It was a bulletproof hosting provider that hasn't been in operation for a while. It's sort of become the Internet's boogeyman for Russian organized crime. There are certainly actors who are associated with it, we're still doing nasty stuff, but that's a separate issue if you want to talk about it afterwards.

MS. COLEMAN: That's great. So demographics, I often say that I am, you know, walking in a labyrinth or a maze where I see kind of glimmers in the shadows, because I don't try to push Anonymous too, too much to kind of reveal stuff about themselves or unmask themselves in the Anon ops networks. Some people do. I've met some. I, you know, talk to a lot. And what I will say is that on the one hand, you know, there is a kind of discourse among Anons. We are anyone, we are everyone, we're lawyers, we're doctors, we're D.C. policy-makers. And on the one hand, you know, there is a kind of openness and it's kind of surprising like some unusual characters, but I tend to say like they're geeks, you know, they're geeks and they're hackers.

By geeks, you may not be as technically sophisticated, but you have kind of grown up on the Internet, on message boards, gaming, these sorts of things. And yet when you say geeks, often times the problem with using a term like that is that it kind of conjures one image and one image alone, basement, pimples, you know, and thick logical pathology. That is wrong, that is wrong.

The people I have kind of encountered are remarkably diverse, some, you know, people who come from the one percent and are near royalty in Europe to other folks that, you know, are below working class and have extremely unusual backgrounds. And in some ways, the people that have done illegal actions, you know, you could kind of apply Malcolm Gladwell's theory of outliers to them. They just have very unusual backgrounds which may be one of the reasons why they're willing to go where they go, right.

So geeks, hackers, but still a kind of tremendous diversity within that lot, from Silicon Valley engineers to those that are, you know, at the bottom of the barrel at some level. When it comes to that kind of world of misogyny, racism that is part and parcel of FORTRAN, Encyclopedia Germattica, not alone to Anonymous, it's an extremely kind of complicated question. I don't think it's just straight forward racism or not racism, it's kind of both at the same time, where they kind of parading existing stereotypes and magnifying them. And the purpose is to kind of shock it.

It's a little bit of equal opportunity shock, not entirely, and it doesn't always map onto reality. So just to give one last exam, and there's a really amazing piece coming out in triple canopy, this journal that's all on what is Anonymous culture, not the political wings, but on that kind of crazy world as irony and shock, really look at it, it's the best thing I've seen.

But a non-ops where Tunisia happened, all these places, had a huge kind of queer community, you know. Like at a certain point I was like, oh, you guys are not joking about wanting each other's whatever, you know. And it took me a while because I was just like, oh, they're just being offensive.

So it's not always what you think it is. Does that mean that we should just kind of embrace it? Not necessarily. But it's not just straight forward kind of racism and homophobia on these domains either.

MR. FRIEDMAN: We have time for one or two very quick questions. So

Marcus in the front here?

MR. RASH: Mark Rash, CSC. I have a quick question. When we talk about concerted activity that leads to criminality, whether the activity itself is criminal or not, it raises the question, how do we deal with that from a legal perspective? We’re used to the idea of a conspiracy, where people get together, they agree to commit a crime, and then they go ahead and assign roles and people do it. But it seems to me that with Anonymous and other hacktivist groups or other types of loosely distributed in groups, it's impossible to hold one person responsible for the actions of another, as well as impossible to hold the whole group responsible for the actions of a group. And I'm reminded of a time in Nixon's second inaugural when they had the National Flush-In. When he took the oath of office, everyone was supposed to flush their toilet at the same time, which would cause a dramatic drop in water pressure and all of the this destruction and havoc. One could argue that Nixon did that himself, causing destruction and havoc. But -- so how do we hold individuals responsible for the actions of the collective? How do we hold the collective responsible for the actions of individuals?

SPEAKER: Two minutes.

SPEAKER: That's a great legal question. It's one of the many horrible legal questions that attend. I would say, look, there are a couple of doctrines of law out there that we have used in the past that might apply thinking about. One is the doctrine of conscience parallelism. It comes from the antitrust field. It's where people coordinate their action, not by actually talking to each other and making an agreement, but you see it, and some people think illegally, in airline prices. You know, Southwest lowers its price and then they wait to see if people will parallel them. If they do -- I mean raise its price, the price sticks. If they don't, you know, they quickly drop their price. So there's a doctrine of conscious parallelism. Extremely difficult to prove, very hard to use in criminal context in particular, where in America proof beyond a reasonable doubt.

The other one is we have a reasonable, foreseeable, doctrine. It's called the Pinkerton Doctrine, an old, famous case in which you are liable for the things that are reasonably foreseeable as a consequence of the actions you've taken. At this juncture, I think that our understanding of what is reasonably foreseeable within the context of a group like Anonymous is far too indefinite for us to actually be able to apply that doctrine.

But I also think that things like what Gabriella is doing, and our general experience over the next 10 years, may well get us to a point where we can say with a degree of confidence that's good enough for our legal system that that destruction of that website was a reasonably foreseeable consequence of your participating in this IRSE chat or something of that nature.

We're a long way from there. Right now, I mean, it's (inaudible).

SPEAKER: As you were asking your question I was thinking, material support and questions about, well, if your computer was used from home in the conduct of defacing a website or part of (inaudible) service attack in support of Anonymous and the IP address is traced back to you, you had no idea, did you? Did you not? So I wonder how long before we start seeing legislative language that talks about material support wittingly or otherwise in the support of Anonymous and online activism.

MR. FRIEDMAN: So one very quick question, if there is one in the audience. Ryan?

MR. BEITISH: My name's Ryan Beitish and I'm a fellow at the Berkman Center at Harvard. And perhaps maybe to try to end on a positive note, I was wondering whether there was any lessons that can be drawn from Anonymous, but in the sense that what they're doing is really impressive in some ways, in that it's an Anonymous body that's coordinating action to accomplish certain tasks.

And so I was wondering whether there are lessons about how that could be channeled in, whether lessons about the structure, of how it's set up, and that could be applied to other systems in such ways that that same kind of behavior could be used in other groups to accomplish positive things, or whether you believe that it's something inherent in the system that that behavior will always sort of fall into all three of those buckets that you've been discussing or whether there's a mechanism for channeling it into the more productive of the buckets.

SPEAKER: What can the tea party learn from Anonymous?

MS. COLEMAN: I mean, on the one hand you can say something like FORTRAN has created amazing cultural artifacts. They're not offensive, you know, they're Internet means, and so that's kind of a positive element to it. But it is definitely the case that I do think -- I really like to compare Debbie and the largest free software project in the world, which I study very, very closely, which is, again, a kind of perfect inversion, though meeting at the middle there of Anonymous. Because they have a social contract, a constitution, uber transparency, you have to sign each other's encryption keys. And so in some ways for them to kind of collectively organize and scale to the degree that they have, you have to put in kind of procedures, and policies, and norms that Anonymous does not want to go there.

And so, I do think that part of the kind of flexibility and open-endedness and decentralized nature of Anonymous will always then make it so that it becomes very difficult to fully, morally control what's going on at some level.

MR. FRIEDMAN: Paul?

MR. ROSENZWEIG: I think that one of the things that we've learned from Anonymous, which is really fascinating to me, is that there is this possibility of self-organizing groups. There's a theory about this by a Swedish economist named Einhorn

I'm going to write, and her theory is that these self-organizing groups can be sustained only over a limited amount of time, space, and distance, a cohesive group.

The classic example of this is lobstermen in Maine, who without any need for any rules or regulations, allocate the catch out of lobster pots, even though it's a common resource that they all could exploit to heck. But because they're a tight-knit social group, they've all lived there for 3,000 years, you know, then your reputation's everything. They don't.

She takes that and generalizes it to the fact that it can't be too much expanded beyond a group like that. I look at Anonymous, I see both that it started trying to do that, that it's had its breakups and groups of dissent, groups breaking off and going away, and then some of them even fighting with the original groups, and lots of conflicts.

And I think that what we learned from them is that her theory is probably right, that it's a limiting factor. But one of the things it portends is the possibility that the internet may make it bigger and easier to do and, you know, will have a larger time and space limit. I don't think it will ever get to be like, the grand Internet democracy that everybody participates from everywhere all the time. I don't think it'll work for, what's that third way, Politics America thing that they're trying to do?

SPEAKER: Americans Elect.

MR. ROSENZWEIG: Americans Elect, that's it. Because I think that's probably too big, but it's a great social -- I mean, leaving aside everything about whether what they do is good or bad, you know, it's a great experiment in social organization that's really fun to watch.

SPEAKER: The book is still being written on Anonymous. And I think if you look at Anonymous, as Paul said, it was born of the Internet age, it reflects social activism in the modern information-based society. Ten years from now, we'll have a lot more lessons learned about how activism has evolved and jumped into the online world, and 20 years from now, we'll look back and can see a definitive history of activism of the '60s, in the physical world, the '70s, into the cyber world of the '90s, and where we're at now. So give it time. But I think it shows that -- how information technologies plus social activism concepts, you know, it's opening a new chapter for us, so I think it's going to be a very exciting couple of years ahead.

MR. FRIEDMAN: We need more anthropologists. So before thanking the panel, just a quick plug for those of you who are interested more in the specific question of botnets, next Friday we'll be having an event with the Department of Commerce and Department of Homeland Security on the ISP role in botnet notification and take down.

But this was a fantastic discussion and I think probably one of the more nuance discussions on this phenomenon that Washington has seen. So I really want to thank Paul, Rick, and Bill, and I hope you’ll join me. (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