THE FREE STATE FOUNDATION

A Free Market Think Tank for Maryland.....Because Ideas Matter

# The Free State Foundation's
# Fourth Annual Telecom Policy Conference

## *"The Internet World: Will It Remain Free From Public Utility Regulation?"*


**Closing Keynote Address**

**Danny Weitzner**
**Deputy Chief Technology Officer for Internet Policy,**
**The White House Office of Science and Technology Policy**

**March 20, 2012**
**National Press Club, Washington, DC**

**MODERATOR:**

**RANDOLPH J. MAY**, President, The Free State Foundation

**CLOSING KEYNOTE SPEAKER:**

**DANNY WEITZNER**, Deputy Chief Technology Officer for Internet Policy, The White House Office of Science and Technology Policy

---

* This transcript has been edited for purposes of correcting obvious syntax, grammar, and punctuation errors, and eliminating redundancy. None of the meaning was changed in doing so.

MR. MAY: Now, Danny Weitzner is going to give closing remarks. The important thing to say is that Danny is now Deputy Chief Technology Officer for Internet Policy at the White House Office of Science & Technology Policy. You have the rest of his bio.

I first met Danny back in the early 1980's, I think. I was representing CompuServe, if that name means anything to anyone.

(Laughing.)

And that's back when you actually couldn't have user names. My number was something like 14666. And they never got around to letting you have a user name until very late in the game.

Anyway, that's when I first met Danny. He was at the Electronic Frontier Foundation. We were talking about things like bulletin boards and access charges.

It was a pretty small circle of us who were doing that before Al Gore invented the Internet.

And Danny was always the smartest guy in the room. I could tell then that he knew more than the rest of us. His career went on and he continued to demonstrate that.

So I'm really honored and pleased that you're here

with us today.

(Applause.)

MR. WEITZNER: Thank you so much, Randy.

It's a great pleasure to be here with you. And it is true, Randy, you added about ten years onto our respective lives. Because I think that that was probably 1990 or '91, lest I appear any older than I actually am.

Age seems to be a theme here. Why is that?

(Laughing.)

But it's actually a wonderful moment from which to start my remarks here. Randy was doing what was absolutely cutting-edge legal work, trying to understand how to address these very odd ducks called electronic bulletin board systems, BBS's.

CompuServe had a real going business. It was available in many places around the world, around the country. It was right up there with MCI mail and AT&T. What was AT&T's service

called, Easy Net or something? Words like that.

And CompuServe was, importantly, one of the first services, (a) that was really addressed to individual users, to individual consumers; and (b) that actually let users speak. It let them do stuff. It was a platform on which all kinds of small little publishing businesses were

built.

And that was a really extraordinary thing. It was before AOL did that. Sorry, Steve. CompuServe was really the first service to do that.

Amazingly, some people thought the center of the Internet was going to be Dayton and Columbus, Ohio, because Mead Data Central was there. There was a lot of data and a lot of phone lines coming in and out of there, and everyone thought that was going to be Silicon Valley. But it ended up not being, unfortunately.

I remember really learning from my working with Randy and a couple of other lawyers who were involved with that issue. At the time I was an intern. So internships are really important because you get to learn from people like Randy.

I was working at the ACLU on First Amendment issues related to new media. And the question about what matters about the First Amendment in these new communications platforms was a very hard to figure out. I remember working on this with Jim, too.

At the end of the day, it's probably the best lesson about unintended consequences that I have learned in my life. Now these are actually positive unintended consequences.

So a small group of us set out to really address the problem that had been raised by CompuServe.

CompuServe was a platform for lots of small publishing businesses. One of the publishers got sued in a defamation suit. And the plaintiff tried to join CompuServe in the suit, saying that CompuServe was the equivalent of a publisher of this defamatory material.

CompuServe tried to say, "No, no, wait a minute, we're more-or-less the carrier, we're just the platform."

In the end there was an important district court decision that found that CompuServe was more like a public library or lending library than it was a publisher.

What this taught the very tiny number of us who were trying to figure these issues out was that it was really important to sort out what we now call intermediary liability. I can't remember what we really called it then.

And that led to, along with the passage of the Communications Decency Act, this funny little Section 230, which has had a second life in the last decade.

But when we were working on this, it was the oddest little backwater issue. You couldn't explain it to anyone. It was even more obscure than the communications law that you guys do. It was really out there.

And somehow, now-Senator Wyden, then-

Representative Wyden, and Representative Chris Cox, picked this up as an issue that they decided was important. I think Tom Tauke was in Congress then.

They fixed the problem as it was defined. It felt like a little narrow problem of defamation and First Amendment law.

And it ended up being the provision that enabled the creation of Facebook, the creation of most of the Google services, the creation of YouTube, Ebay, and all these services that you can imagine, all these platform services that are now the basis of tens of billions of dollars of productive activity on the Internet.

Now I would love to be able to stand here and claim credit for having the foresight. Maybe Randy did. But I know that most of us didn't.

The challenge that we have now, the challenge that we feel in this administration, is to make sure that we retain the extraordinary innovative potential that the Internet has. That is, to make sure that we didn't just have a cool 15 years and then it all goes flat, but that we can keep going with this kind of innovative activity.

At the same time, we have to address what are clearly a real set of public policy concerns that we have to take seriously in a way that we didn't back in the '90s,

when this all started.

A friend of mine likes to say that in the '90s the Internet was a cool side show; now it's main show. It's clearly an essential platform for economic activity, for political activity, for educational and scientific activity.

So we have to attend to the issues, such as privacy, cyber security, copyright protection, that this platform has created.

And we have to do it in a way that takes those issues seriously, without stifling the innovation that we really want to see continue to develop.

Since we're short on time, and you all are staying up past our schedule, which I appreciate, I want to talk very quickly about one example of how we've looked at these issues in our work on consumer privacy issues, and extrapolate just very briefly to how we think that provides a model for dealing with Internet policy issues broadly, that keeps in mind the lessons that we learned in the mid-90's about preserving the openness of Internet platforms.

We took on a series of Internet policy issues at the beginning of this administration, focused on consumer privacy, cyber security, online copyright protection, and the global free flow of information, looking at the

trade-related issues in global Internet policy and making sure that we have a global platform for innovation.

I'll spare you the gory details of how we got here, though many of you contributed quite a bit. Here's where we came out on privacy.

At the end of last month, we released the Consumer Privacy Bill of Rights. It's the Administration's blueprint for protecting consumer privacy in the online environment.

I'm not going to talk about it in detail because I'm sure you've downloaded this report and read it all. It's one of the most popular reports on the White House website.

That's actually not true.

(Laughter.)

But it is available on WhiteHouse.gov. You can all read it.

There are two key aspects of the Administration's framework for protecting consumer privacy that I want to emphasize: Number one, we begin with a set of principles. There are seven principles that are drawn from the history of privacy protection. Notwithstanding my friend, Adam Thierer, these are American principles about privacy protection.

They are principles that we actually developed here in the United States in the early '70s and have been the basis of privacy protection laws in the U.S. and all around the world.

We would like to see those principles enacted in legislation, because we think it's important to close the gaps that exist in U.S. law.

We have lots of great privacy laws in the U.S. for health privacy, for financial privacy, for video privacy. We have lots of coverage of privacy issues. But we have a significant gap in the area of general commercial interactions.

We'd like to close that gap, but we have a very particular view about *how* to close that gap.

To begin with, we would like to see stakeholders take these principles and implement them in what we call "enforceable codes of conduct." It's a strategy that Tom Tauke alluded to earlier. Most businesses today, large and small, on the web, have privacy policies.

There are seven principles that we think guide any sensible, thoughtful, responsible privacy policy. We've put out these principles in order to set a baseline of expectations about what privacy policies ought to entail.

But we very specifically do *not* want to empower

any particular regulatory agency with rulemaking authority to go and write rules, as we would normally do, as we would do in a traditional telecommunications context. We don't want to send an agency off with this set of seven principles and say, "Go figure out the rules." We think that process is not adequately flexible, and we think that process is not adequately timely for the Internet environment.

Our very distinguished Chair of the FCC, Julius Genachowski, said about a year ago that the average cycle time for a rulemaking process at the Commission is six years.

Now you all would have more experience with that than I. I note that that's the average, some probably take a little longer. And there are good reasons for that.

But take what we know about the Internet environment. Six years ago, there was no Facebook at all. Six years before that, there was no Google. And six years before that, it was just me and Randy, goofin' around.

(Laughter.)

MR. WEITZNER: So we really have to take the need for speed very seriously in this environment. That's as important for consumers as it is for businesses.

In many cases, we look at the privacy rules that

are on the books now, in statute or in regulation, and they frankly don't meet the needs that people have or the realities of the online environment.

We want to make sure that we have a privacy framework that can keep up with the changes in technology, without having to slow down the evolution of technology.

So we've put out this Consumer Privacy Bill of Rights. The Commerce Department is right now beginning a process of convening stakeholders. It is a process for companies that handle personal information, privacy advocates, regulators, and academic experts to take these principles and implement them in specific cases.

We expect to see a whole range of codes of conduct to address specific privacy issues, specific industry sectors, and specific contexts. And we then expect that those codes of conduct will be adopted by companies and be enforceable at the Federal Trade Commission.

One of the points that we make in our report is that we think the FTC has done an outstanding job of privacy protection in the United States over the last 15 years, amazingly enough with no specific privacy jurisdiction whatsoever. No offense to those of you from the FCC.

The FTC has Section 5 jurisdiction for unfair and

deceptive trade practices. They've used that jurisdiction very strategically, partly through the raised-eyebrow process, to make sure the companies adopt privacy policies, and then to make sure that they're enforceable.

This is just an aside: We got a kind of a bum rap around the world for not taking privacy seriously.

First of all, we just had a very senior delegation of European Commission and European Parliament Officials in town this week. They put out a statement that acknowledged how important this policy statement is, and acknowledged that while our approach to privacy is different from theirs, it is a real approach.

And we are going to be working with them very carefully to make sure that we have a process by which U.S. companies that are doing business in Europe have a coherent way for complying with new European privacy laws.

But while Europe has clearly a more comprehensive set of privacy protection laws, there can be no doubt that the U.S. is a world leader in enforcement of privacy laws.

If you look at the Federal Trade Commission's actions over the last year in their consent decrees with just Google and Facebook alone, that's more than a billion users who are now covered by FTC supervision.

And there's quite a bit of scrutiny, as Google is

now discovering, of their subsequent practices.

That's a billion users. As far as I know, we don't have a billion people in the United States. So we must be doing some protecting for people outside the United States, too.

It's our responsibility. It's the right thing to do. But it shows that we are going to have an increasingly interconnected and overlapping set of privacy jurisdictions around the world.

The reason that we think the model that we've laid out for privacy is important for the Internet, overall, is it addresses exactly this global phenomenon.

The principles that we've agreed to are more-or-less globally recognized principles. The specific rules that we'll be enforcing through these codes of conduct may well be local rules. They'll be specific to a particular industry.

If we have to tell, say, the mobile apps providers or location-based services or social networking companies, to go into some global policy process and figure out what rules they ought to follow, we all understand quite well that that process would be a non-terminating process. It would, at least in our lifetimes, leave consumers unprotected. And it would leave businesses with a great

sense of uncertainty.

So we need to find a way to build from these broad principles, and then recognize between countries that compliance with codes of conduct that satisfy those principles ought to constitute compliance with national laws, whatever they are around the world, provided they are based on a common set of principles.

So there's going to be a delicate dance here of making sure that we can arrive, increasingly on a global basis, at a common set of policy principles, that can then be implemented locally, but enforced in a coordinated fashion, all around the world.

This is the only way we'll ever get to an open and evolving global Internet marketplace.

We had an early recognition of the value of this kind of approach to Internet policymaking. It's a combination of broad principles with flexible implementation through enforceable codes of conduct through the OECD's Internet policymaking principles.

At the OECD, 34 countries got together last year and adopted a set of Internet policymaking principles as a recommendation.

That means that the members of the OECD are taking on themselves a voluntary commitment to approach Internet

policy, using exactly this framework.

We're very encouraged that we were able to have that kind of support from our allies.

Obviously, those 34 countries are an important part of the world. They make up a substantial part of the Internet economy today. But where Internet growth is going to be in the future really is in the next 34 or the next 50 countries down the line.

The next challenge is that many countries are mistakenly relying on the International Telecommunications Union to take on a regulatory role in the Internet environment, both as to the operation of the infrastructure and as to important questions, such as privacy and security, that really are not appropriate for the ITU to handle.

We think there are a lot of important things for the ITU to do on an ongoing basis. Telecommunications technology standards continue to be very important, as does the spectrum allocation work and the development work that the ITU does.

But the temptation by a number of countries is to look at these difficult questions of Internet policy and say we need single centralized, globalized solutions. And we don't think that's the right way to go.

Over the next couple years, there will be a number of debates at the ITU on just this topic. And we're going to be very engaged in those debates.

I want to wrap up and just very quickly say that the messy process that Randy and I found ourselves in when trying to deal with these questions about who was liable for what when something gets published on BBS's remain with us.

There is an ongoing debate about the responsibility of Internet intermediaries. We saw that with the piracy debate that went on last year and the beginning of this year.

And the central question there was: What kind of obligations ought the various Internet intermediaries, the various platform providers, have in order to police or somehow control online copyright infringement?

We have a substantial and active commitment to developing new strategies to combat intellectual property infringement. It's critical for our global economic competitiveness and the success of our economy domestically.

But we also want to make sure that we're not thwarting innovation in the Internet environment in the course of doing that.

We put out a pretty carefully-worded statement on this. And our answer really is to use, as much as possible, voluntary but enforceable codes of conduct.

We've been very encouraged that in the intellectual property area some of the Internet service providers have gotten together with rightsholders to develop voluntary mechanisms to address infringement on their networks. We think that was a very positive result.

We've seen the same kind of efforts in efforts to police counterfeit pharmaceuticals online, which present a very similar kind of challenge.

You have global sources of contraband material. We don't have the kind of border where you can just put a lot of customs agents there and check all the crates as they come in.

So we have a new set of challenges here in the Internet environment. But we are firmly of the belief that this voluntary cooperative model is an important part of addressing the issue, provided it comes with an underlying set of principles that have legal enforceability to them.

I was lucky enough to see the Internet in its early days. Technologically and from a public policy perspective, it was then very much a work in progress. It was very much evolving.

And if we're lucky, it will stay that way. If we're lucky, the Internet will remain a work in progress. We have to get better and better at addressing these public policy issues.

There are lots of companies in this room, there are lots of civil society organizations in this room, that have made major contributions to that process, whether it's in the area of child protection or privacy protection.

We will be able to retain the flexibility of the Internet policy model, only based on the strength of engagement from companies like yours, from civil society groups like yours.

Because fundamentally, the challenge that we've put out to the Internet community, that the private sector in many ways has responded to very positively, is to say: We have a fork in the road here. We can increase our voluntary engagement to address these issues with appropriate legal foundations, or we can turn this into a process that has a much more heavyweight top-down regulatory framework.

That top-down process would never be our choice, as an administration. But there is clearly a demand in the U.S. government, and I think in governments all around the world, that we have to have a serious strategy about how we

protect our citizens from the real threats that are developing in this environment.

So that's the challenge. Back to Randy, who will have the answers, once again.

Thanks a lot.

(Applause.)

MR. MAY: Having Danny here certainly made me feel young again.

So just in line with our tradition, if we have one great question, I know Danny will take it. Then I know we'll be out of time.

So we always like to have good provocative questions. I thought that might come from Adam. Adam will do it.

When we're through with this, I would just want to thank Danny again. Then we'll adjourn.

MR. THIERER: You called me out, brother.

MR. WEITZNER: There you are, there you are. I'm ready for it. Come one, come on (laughing).

MR. THIERER: So for the record, I did not say that the principles were not American, or European. They're good principles.

The question is how we enforce these privacy principles. Right?

And the concern that some of us have is that the direction that the White House may be taking us down looks a lot more like what Europe has done, in terms of its top-down data directives and more heavy-handed approach in privacy regulation or co-regulation, as some may call it.

Now maybe that's the not intent. But that's the concern some of us have.

And the secondary concern relates directly to your first point that you so eloquently made about Section 230, and the importance of making sure we don't deputize intermediaries and keeping things fairly self-regulatory and voluntary.

This is the approach we've taken on free-speech issues and First Amendment matters. And it's the approach many of us think that we should still take towards things like privacy.

But again, the concern is that we're changing course a bit, and maybe starting to deputize intermediaries or put the threat of the regulation above their necks, like a Damocles sword.

And so, therefore, Danny Weitzner, why do want to destroy American freedom and innovation on the Internet?

(Laughter.)

MR. WEITZNER: That's a good question (laughing).

Between working on piracy, focusing a certain amount on the intermediary liability question, and then privacy, I have been accused of being a job killer by two major industries. So it's been just delightful.

The concern that we have about the European data protection model is the regulatory process, not so much the principles.

As we have described in our white paper, we intend to have a very different process for implementing these principles.

Just in a sentence, companies would work in a multi-stakeholder process to develop these codes of conduct, and would then seek safe harbor at the FTC, which would determine whether the codes developed by the companies and the other stakeholders is sufficiently compliant with the principles.

So that's a non-regulatory process. We extend no additional rulemaking authority, at least if it becomes our choice, to any regulatory agency.

We rely on the strength of agency enforcement that has guided and helped us to focus on issues on privacy practices that actually cause harm and concern to consumers.

On the intermediary liability question I don't

actually have a simple answer.

In the early '90s, we were dealing with the liability of what were, to a large extent, dumb pipes or platforms. That is, they were either Internet service providers in their simplest form, moving lots of bits around, or they were platform providers such as CompuServe, with a text-based interface that was pretty elementary in terms of its computational power as well as its ability to filter and analyze content and make choices based on that.

As you know better than almost anyone, Adam, one of the purposes of the Section 230 was actually to encourage platform providers to invest in building what we called then family-friendly Internet services, to limit their liability in the event that they wanted to provide a service that was filtered, based on one set of criteria or another.

I think we can say that that worked, because there are all different kinds of options that parents have to make sure that their kids have the Internet experience they want them to have, as opposed to something else. The real challenge for thinking about intermediary liability is that intermediaries today have much more analytic power, and are able to discern content at a level that we never could have imagined.

And the question comes: Should they do something with that power? Should they be legally required to do that?

Even in Section 230, we said there are certain kinds of liability for which the intermediaries are completely absolved.

And then there are other kinds of liability, such as intellectual property infringement liability, which Section 230 didn't touch.

We dealt with that in the DMCA. And what we did there was to define very specific obligations for platform providers, or at least actually provide them safe harbors that would allow them to avoid potential liability.

So this is never a perfectly either-or question.

What I think we learned from the SOPA debate is that the most important thing is to establish certainty for platform providers.

What I think Section 230 stood for, if nothing else, was that platform providers shouldn't be guessing about whether a particular kind of content could result in liability or not, because otherwise they have to self-censor.

So what we need is certainty. We think that the code of conduct and safe harbor process is a way for

companies to get that certainty from the agency that might enforce against them. That's the direction that we've got to go.

It's a great question.

MR. MAY: Okay.

This was definitely terrific. I want you to join me in thanking Danny.

(Applause.)

MR. MAY: And this meeting is adjourned.

(Whereupon, at 2:35 p.m., the meeting was adjourned.)

* * * * *