

Congressman Marsha Blackburn

**Remarks To The
Telecommunications Industry
Association's "Inside the Network"
Conference**

**Dallas, Texas
May 18, 2011**

Remarks As Prepared For Delivery

Thank you TIA for inviting me here.

I am so excited to continue our dialogue on something I know you all care about deeply, securing the prosperity of our online world. Many of you attended the State of the Net conference this January, where we first took up this conversation.

I asserted there that, where tech policy is concerned, a Conservative wakeup call is well overdue. For too long, mainstream activists have seen tech issues as a boutique enclave of the policy world, one where reasonable compromise can be reached over unimportant issues. This is not the case.

Today's tech policy debates will determine the prosperity of tomorrow's free markets, the viability of free innovation, and the survival of free speech. They draw the map of 21st century prosperity and determine if the most free and prosperous marketplace, the most dynamic force for freedom can long endure.

This challenge is an important one for obvious reasons. And it is becoming clear we must apply our Conservative principles boldly to protect our virtual world from emerging threats that might disrupt the engine of creative growth.

We saw the first attack in the form of a federal agency's mandate that wrongly imposed strict net neutrality regulations on the Internet. The fight to overturn those regulations is one we will continue to carry, and one which we know we will win.

We've also seen how intellectual property is being threatened online through rogue sites that manipulate and rip off consumers through sales of stolen or fake products. Now we are witnessing the convergence of the proliferation of privacy concerns and online data theft issues.

In the past I have discussed the threat posed by government overreach and the threat posed by theft. Today, I would like to focus my discussion on the rapid monitoring, transfer, and retention of our online information, or what I like to describe the "Virtual You"—your online shopping, personal information, browsing preferences, and social interactions.

The American consumer has been digitized. Government and industry alike- have an obligation to protect her if we are to maintain her confidence in the future marketplace. I fear that the entire supply chain of online stakeholders fails to fully appreciate the challenges we are facing in this information sharing age.

I want to be very clear here, consumer trust in online information collection and management has eroded and we will soon reach a tipping point, leading to greater uncertainty that could suffocate the growth and innovation we all have come to expect

online. But you have within your power the means to come to voluntary self regulatory solution that will restore that trust.

You must recognize two things. One, though you dazzle consumers with your ends, you also frighten us with your means. Two, self-regulation offers the only path to a palatable solution.

Compounding consumer privacy concerns is the disturbing proliferation of data theft that knows no boundaries and has led to greater anxiety over how much of our personal data, the aggregate of which represents the Virtual You, is at risk of being lost to criminals and hackers.

The lifecycle of recent data breaches and the lag time in appropriate consumer notification is a trend that I fear perpetuates industry's "culture of damage control". It further strains consumer confidence. Understand that consumers are forgiving when criminals steal data from you. What disturbs them is how much data you were holding in the first place.

If we fail to lead on this issue, bureaucracy and Big Government will rush in with all its corrosive potential. Indeed, many have already begun to lay out their plans.

Government solutions to privacy concerns will evolve either from the left, in the form of hyper-regulation from a menu of agencies, or from a classical liberalism perspective that defines private information as property. Either way, the solution will be spurred to action by shrewd activists and morning headlines -- not by careful consideration of the facts.

The FCC's net neutrality decision is a hyper-reactive, counterproductive, and predictive example of what happens when Government finds a problem they feel the urgent need to fix.

If interested participants fail to soon define and voluntarily enter into a credible structure of self-governance, the FCC and the FTC will in all likelihood broadly define one out of thin air.

It is possible, even likely, that no safe harbor provisions will exist under this regime. No entity doing business online will avoid the frustration, layers of unanticipated bureaucracy and heavy costs generally associated with new regulations.

I admit I am sympathetic to arguments others would make, aggressively defining private information as an extension of private property. What follows is a strict opt-in approach to privacy where no information can be used or interpreted without explicit authorization.

European regulators have already gone down this road and devastated innovation. We can't let the 300 billion dollars the ad-supported Internet contributed to the US economy in 2009 – not to mention 3.1 million domestic jobs- meet that same end.

Compromise between the individual's desire to control his own information and the economy's drive toward greater efficiency is possible, but not if industry and Washington's only solution is to ignore the problem and build firewalls between the individual and the marketplace.

There is a third way.

For the online world to continue to thrive, we need real leadership that answers consumers cry for help, not just a typical ploy that gives off a false sense of security and a free credit report.

We need to find equitable and durable solutions before Big Government finds them for us. I am urging you and warning you here today to empower consumers before government empowers itself.

To me, such a solution has several principles.

First, Washington is foolish and arrogant to assume that we have the power to regulate or even shape, what is a global free marketplace. Those who are active in this marketplace, both on the demand side and the supply side, should design and enforce its future.

Second, government's role here is not to determine what information is or is not, should or should not, be private. Industry must proactively and credibly ensure that individuals know more about what data is being collected about them and how it is being used.

Third, while many speak of what industry owes government, I believe that government owes clarity and predictability to all online stakeholders.

There are three "deliverables" that I actively pursuing.

One, all stake-holders deserve consistent and transparent protection, no matter what technology platforms they might use at any given time.

Consumers' should also be guarded equally across the technology spectrum. Our current dual system of FCC and FTC jurisdiction only serves to blur the lines of protection. As I said in January, it tends to emphasizes the means of transmission over the essence of transaction. This is a serious error.

For example, in a response to a letter several Republican lawmakers sent last month to mobile device operating system developers seeking detailed information on their gathering and storing of location-based data, one developer responded that their carrier "was not subject to Section 222 of the Communications Act because they were not considered a telecommunications carrier."

Another responded that "the plain language of Section 222 in the Communications Act demonstrates that it applies only to providers of telecommunications services." If we "de-fragment" government's jurisdiction in this arena, we can give consumers some clarity, certainty and consistency in how privacy rules and strong self-regulatory structures will be administered and enforced.

The FTC has the experience and expertise in this arena and therefore should have full jurisdiction. The FCC's claim that it knows best how to identify "potential harm" to our competitive market is fatally misguided.

That's not a good foundation for a workable privacy regime. Sections 222 and 631 of the Communications Act are relics and I will shortly file legislation to repeal them.

Second, this year we have seen the FCC take significant steps to hinder a market-based solution to the privacy issue. Net Neutrality orders expressly prohibit the marketplace's most important tool for facilitating consumer choice: discrimination.

Proposals like an online Better Business Bureau or other mechanisms that would alert consumers as to what personal data is used, shared or sold runs afoul of the FCC's vision of a government regulated Internet. Likewise ISPs or other entities are limited in acting on the consumer's behalf to protect them from bad actors. For this reason, and many many many others, repealing the FCC's Net Neutrality order must be a priority.

It is futile to craft a free market solution unless Washington is prepared to accommodate it. Once we successfully shift privacy issues away from the FCC and to the FTC, I support the kind of safe harbor that Congressman Sterns has proposed.

Beginning this spring, and I hope continuing for some time, I will convene a series of tech stakeholder roundtables around the country. My hope is that by bringing stakeholders- including consumers- together with their federal representatives and America's best innovators, we can find some solutions.

I hope to base this solution on resolving the challenges consumers face online, to give them a "credible level of transparency" and at least "a fighting chance" to protect their sensitive data.

We must do this if we hope to sustain a healthy and thriving creative economy. The main questions we'll focus on are: Who can sync into our Virtual presence, to what extent, and for what purposes? What solutions can we prescribe before its too late?

The extent of what information is gathered and tracked online, or how deep one can "data dive" into your virtual space, ought to be based on the importance and "relative sensitivity" of the data.

Does very private data also warrant more consumer choice and control over whether it gets shared and with whom it is shared?

Can we give the consumer the opportunity to explicitly opt-out or even perhaps opt-into easy to read agreements regarding their most personal data?

Once our online terms and conditions are better defined, what are the solutions and boundaries to work within once we have moved data regulation under one roof and to level the privacy playing field for consumers and covered entities?

Those of us in this room represent the creative economy and we lead in providing innovative solutions to the world's biggest tech problems. Online privacy and data security issues stretch beyond time and location.

But a conservative approach that returns to the time tested business adage that the customer is always right, may be prudent in this circumstance.

Instituting a solution that respects all people in the digital space would foster and harmonize our industry for another generation. I urge the leaders of the creative economy to join me as we come together to provide a creative solution.