than material wealth. The lure of K Street never touched Tom Faletti. Instead of cashing in on his time in the Senate and his amazing experience on Capitol Hill, Tom is actually leaving the Senate to take a pay cut and teach in an inner-city high school. Those of us who know and love him are not surprised.

He will be teaching government and political science to 11th graders and a religion class on social justice—his great passion.

Tom said above the chalkboard in his classroom he will hang a sign that reads: ''You can change your world.'' Tom has proven he can change the world because he has changed America. He wants to show his students how they, too, can reach that goal in their lives.

Tom will not need a textbook for that lesson. He can teach from his own experience because that is what Tom has done for 24 years as a dedicated staff member in the House of Representatives and the Senate. I was always proud to be Tom's friend and to learn so much from this good man.

I thank Tom for his service, and I thank his wife Sonia and their children, Timothy, Joanna, and Luke, for sharing him with us for all these years. I wish him the best of luck, and I say to the students at Archbishop Carroll: Listen carefully to Tom. I have for 24 years, and it has worked out pretty well.

I yield the floor.

The ACTING PRESIDENT pro tempore. The Senator from Rhode Island is recognized.

Mr. WHITEHOUSE. Madam President, I ask unanimous consent to speak as in morning business for up to 15 minutes.

The ACTING PRESIDENT pro tempore. Without objection, it is so ordered.

CYBERSECURITY

Mr. WHITEHOUSE. Madam President, I will speak about a topic that is central to our national security and economic prosperity and which gets far too little notice and attention; that is, the vulnerability of America's network information systems, and the economic danger and national security risks we face from cyber-theft, cyber-piracy, and cyber-attack.

We live in a wired society. If we sever those wires and the social, economic, and communications linkages that make our way of life possible, we will cease to function. I am gravely concerned that we are not taking the necessary steps to guard against this threat, which I believe is the greatest unmet national security need facing the United States.

Earlier this month, the Intelligence Committee Cyber Task Force submitted a classified final report to the chair and vice chair of the Intelligence Committee. It was an honor to chair this bipartisan initiative and to serve with my distinguished colleagues, Senator MIKULSKI and Senator SNOWE. I thank them for their diligence, their leadership, and their important contributions to this effort. They were excellent and we made a good team.

We spent 6 months investigating cybersecurity threats and our current posture for countering those threats, with a particular focus on the intelligence community. It was a very sobering experience.

There is a concerted and systematic effort underway by nation states to steal our cutting edge technologies. At the same time, criminal hacker communities are conspiring to penetrate financial industry networks, rob consumers of their personal data, and transform our personal computers into botnet zombies that can spread malware and chaos.

It is difficult to put a precise dollar figure on the damage and loss these malicious activities are causing, but it is safe to say it numbers in the many tens of billions of dollars—perhaps as high as $1 trillion.

I believe we are suffering what is probably the biggest transfer of wealth through theft and piracy in the history of mankind.

In addition, we face the risk of attacks—attacks designed to disable critical infrastructure, with grave potential harm to our national security and to our financial, communications, utility, and transportation sectors.

The intelligence community is keenly aware of the threat and is doing all it can within existing laws and authorities to counter it. The bad news is the rest of our country—including the rest of the Federal Government—is not keeping pace with the threat.

I am encouraged by the growing interest in Congress, where there are now more than 40 bills pertaining to cyber. I want to commend Senator ROCKEFELLER and Senator SNOWE, in particular, for being at the leading edge of the Senate's efforts. They have spent more than a year fine-tuning their legislation, which speaks of their commitment to protecting the country and their recognition that we cannot reduce our vulnerabilities without careful study and thoughtful engagement.

Much of the current debate on cybersecurity in the Congress focuses on executive branch organization dealing with this threat. This is obviously an important issue, and it is one that we must resolve sooner rather than later. But the question of how this all gets organized within the executive branch is merely one of the many problem areas we saw during the course of the work of the task force.

What are these other areas? Well, first of all, an overarching issue, we must raise the public's awareness about cyber-threats; otherwise, we face an uphill battle trying to legislate in this challenging and sensitive policy sphere.

What is the problem? Well, threat information affecting the dot.gov and dot.mil domains is largely classified—often very highly classified—and entities in the dot.com, dot.net, and dot.org domains often consider threat information to be proprietary and disclosing it could be a risk to their business. So the result overall is that the public knows very little about the size and scope of the threat their Nation faces.

If the public knew the stakes—knew the cyber-criminals, for example, have pulled off bank heists that would make Willie Sutton, Bonnie and Clyde, and the James Gang look like a bunch of petty thieves, they would demand swift action. If they knew the extent of the cyber-piracy against our intellectual property, and the economic loss that has resulted, the public would demand swift action. If they knew how vulnerable America's critical infrastructure is and the national security risk that has resulted, they would demand action. It is hard to legislate in a democracy when the public has been denied so much of the relevant information.

The first key point is public awareness. We have to share more information with the public about what is going on out there.

Second, we need to establish basic rules of the road. One of the signal features of our cybersecurity risk profile is that the overwhelming majority of malicious cyber-activity could be prevented if some computer users installed simple antivirus protections and allowed automatic updates of their software.

If we followed basic rules of the road, there would be a national security advantage: The Federal Government could focus its cybersecurity efforts on that narrower subset of threats that can evade commercial, off-the-shelf technology. There would be economic advantage from the potentially massive reduction in cyber-crimes, such as identity theft and credit card fraud.

Third, we need to empower the private sector to adopt a more proactive stance against cyber-threats. I am from Rhode Island. My State was founded as a sea trading State. When our traders were attacked by pirates, they got out their guns and fought back. Under current law, companies under cyber-attack can do little more than batten down the hatches. We need to look for more ways to help American companies better defend themselves.

Our courts provide one option. Creative technical experts and smart lawyers at Microsoft were able to mount a very impressive counterattack against the Waledac botnet by obtaining a Federal court order requiring that VeriSign, the domain name registrar, cut off domains associated with the botnet. This disrupted the botnet's command-and-control function, and it highlights an important possible role for our judicial branch.

Additionally, we need to establish lawful and effective means for industry sectors to band together with one another and engage with each other in

common defense strategies and information sharing where appropriate with the government. There are some early examples, such as the defense industrial base, that merit commendation, which we should encourage. But it is still pretty primitive.

Fourth, we must ensure that the Federal Government has the authorities and capabilities necessary to protect our American critical infrastructure against cyber-attack. If a bank, for instance, runs into a solvency problem, there is an established and widely accepted procedure for Federal intervention to protect the bank depositors, stand the bank back up, get it back on its feet, and move back out again.

There is no similar procedure if that bank or American critical infrastructure, such as an electric utility, is failing due to an ongoing cyber-attack. There needs to be clear, lawful processes for the private sector to request technical assistance and clear authority for the government to act when a cyber-incident raises significant risk to American lives and property.

It gets a little bit more complicated than that because you cannot just call 911, such as when there is a fire, and have the government come and put out the fire when it is a cyber-attack. Cyber-attacks happen literally at the speed of light.

The best defense against cyber-threats, particularly the most dangerous cyber-threats, requires speed-of-light awareness and response. For this reason, it is worth considering whether some defensive capabilities should be prepositioned in order to better protect the Nation's most critical private infrastructure.

During medieval times, critical infrastructure, such as water wells and graineries, were inside the castle walls, protected as a precaution against enemy raiders. Can certain critical private infrastructure networks be protected now within virtual castle walls in secure domains where those prepositioned offenses could be both lawful and effective?

This would, obviously, have to be done in a transparent manner, subject to very strict oversight. But with the risks as grave as they are, this question cannot be overlooked.

Fifth, we need to put more cyber-criminals behind bars. Law enforcement engagement against cyber-crime needs to be considerably enhanced at multiple levels, reporting, resources, prosecution strategies, and priority. A lot more folks need to go to jail.

Finally, we must more clearly define the rules of engagement for covert action by our country against cyber-threats. This is an especially sensitive subject and highly classified. But for here, let me simply say that the intelligence community and the Department of Defense must be in a position to provide the President with as many lawful options as possible to counter cyber-threats, and the executive branch must have the appropriate authorities, policies, and procedures for covert cyber-activities, including how to react in real time when the attack comes at the speed of light. This all, of course, must be subject to very vigilant congressional oversight.

Uniquely in the world and uniquely in our own history, America's economy and government now depend on networked information technologies for Americans to communicate with each other, keep the trains running on time and the planes flying safely, keep our lights on, and power our daily lives.

The expansion of this powerful new technology across our great country also makes us uniquely vulnerable to cyber-threats. We have to do a lot better as a nation on cybersecurity. I believe we can do better. I know we must do better. Frankly, we cannot afford not to do better.

I hope these remarks and the structure they have provided helps provide assistance to my colleagues as we begin debating and resolving these important issues.

I yield the floor. I see my distinguished colleague from Minnesota prepared to speak.

The ACTING PRESIDENT pro tempore. The Senator from Minnesota.

DISCLOSE ACT

Mr. FRANKEN. Madam President, I rise today to urge my colleagues to allow debate on the DISCLOSE Act, a commonsense measure to fix just some of the problems created by the Citizens United decision.

For a century, Congress has done everything it could to make sure the American public has as much information as possible about the money being spent in our elections. The first Federal campaign finance disclosure law was passed in 1910, which scientists tell us was 100 years ago. It was strengthened in 1925. In the 1970s, it was replaced with an even stronger system as part of the Federal Election Campaign Act. Eight years ago, with McCain-Feingold, it was strengthened yet again. So the Congress has been in the disclosure business for 100 years. And, in fact, at every major step, the Supreme Court has actually affirmed Congress's power to pass these laws.

In 1934, the Court unanimously upheld the disclosure laws that Congress passed a decade earlier. In 1975, they upheld the disclosure provisions of the Federal Election Campaign Act. In 2003, they upheld the disclosure and disclaimer provisions of McCain-Feingold. Just this January in Citizens United—yes, in Citizens United—they voted 8 to 1 to uphold those same disclosure provisions again.

The disclosure provisions of the DISCLOSE Act are well in line with a century's worth of Federal statutes and precedent, at least according to the Burger Court, the Rehnquist Court, the Roberts Court, and the Hughes Court. I bet some of you have not heard of the Hughes Court. That was from 1934. So we can pass this law. We can do it. There should be a will to do it.

Here are some excerpts from a few Members' floor statements from the 107th Congress, the Congress that passed McCain-Feingold:

> Clearly the American public has a right to know who is paying for ads and who is attempting to influence elections. Sunshine is what the political system needs.

Another Member said:

> We can try to regulate ethical behavior by politicians, but the surest way to cleanse the system is to let the Sun shine in.

Here is yet another:

> Disclosure helps everyone equally to know how their money is spent. [. . .] Disclosure is what honesty and fairness in politics is all about. Why would anyone fight against disclosure?

These are actually the statements of friends of mine across the aisle who are still in this body who opposed McCain-Feingold and who opposed it in large part because they said it did not do enough on disclosure. In fact, a lot of them opposed it precisely because it did not do enough to promote disclosure of the independent expenditures of corporations and unions.

As my good friend Senator HATCH said in March of 2001:

> The issue is expenditures, expenditures, expenditures; and [. . .] the real issue, if we really want to do something about campaign finance reform, is disclosure, disclosure, disclosure.

I think he repeated it three times for emphasis.

This is what the minority leader said when he voted against the McCain-Feingold bill, as amended by the House, in March of 2002. This is the minority leader, Senator MCCONNELL from Kentucky:

> Reformers claim this bill will increase disclosure and shine the light on big money and politics. This is, of course, not true. Unions will continue to funnel hundreds of millions of dollars of hard-working union member dues into the political process without ever disclosing one red cent.

The protections my friends were waiting for are in the DISCLOSE Act, and they boil down to this: If someone is spending a lot of money in our elections, American voters will have a right to know whether that person is a corporation, a nonprofit, a union, or a 527.

Before I close, I want to discuss a part of this bill that does not have to do with disclosure, section 102.

Section 102 incorporates critical provisions of a bill I introduced, the American Elections Act. It will make sure that foreign interests—foreign governments, foreign corporations, and individuals—cannot use American subsidiaries that they own or control to influence our elections.

The fact is, after Citizens United, the U.S. subsidiaries of foreign companies will be able to spend as much as they want in our elections, even if they are under foreign control.

The ACTING PRESIDENT pro tempore. The Senator's time has expired.